

Cyber Security Monitoring and Logging Guide

Version 1

Published by:

CREST

Tel: 0845 686-5542

Email: **admin@crest-approved.org**

Web: **http://www.crest-approved.org**



Principal Author

Jason Creasey,

Managing Director, Jerakano Limited



Principal reviewer

Ian Glover, President,

CREST

DTP notes

For ease of reference, the following DTP devices have been used throughout the Guide.

Acknowledgements

CREST would like to extend its special thanks to those CREST member organisations and third parties who took part in interviews, participated in the workshop and completed questionnaires.

Warning

This Guide has been produced with care and to the best of our ability. However, CREST accepts no responsibility for any problems or incidents arising from its use.



A Good Tip



A Timely Warning

Quotes are presented in a box like this.

© Copyright 2015. All rights reserved. CREST (GB).

Contents

Part 1 - Introduction and overview

- About this Guide 6
- Audience 6
- Purpose and scope 7
- A practical solution 7
- Rationale 8
- Requirements survey 9
- Standards and guidelines 9

Part 2 – Setting the scene

- Overview 10
- Defining a cyber security incident 10
- Typical phases in a cyber security attack 11
- Main cyber security monitoring and logging challenges 13
- Standards and guidelines 14
- The need for support from third party experts 15

Part 3 – Cyber security log management

- Requirements 16
- Logging challenges 17
- Configuring cyber security event logs 18
- Centralised log management 19
- Prioritising log use 20
- Targeted log identification 22
- Analysing logs and alerts 23
- Using log management tools 24

Part 4 – Cyber security monitoring process

- The essentials of cyber security monitoring 25
- Monitoring purpose and scope 25
- Cyber security monitoring challenges 26
- Prerequisites for cyber security monitoring 26
- Key phases in the monitoring process 28
- Indicators of compromise 29
- Cyber security threat intelligence 31
- Links to cyber security incident response 34
- The need for collaboration 36

Contents

Part 5 – Security operations centres

- Overview 37
- People, process, technology and information 38
- People 40
- Process 42
- Technology 44
- Information 45
- SOC qualifications 45

Part 6 – Choosing a suitable supplier

- Cyber security monitoring and logging approaches 46
- The supplier selection process 46
- Understand the benefits of using third party experts 48
- Determine what activities should be outsourced 49
- Types of service available 50
- Define supplier selection criteria 50
- Appoint selected supplier(s) 51
- Make the appointment 52

Part 7 – Cyber security monitoring and logging capability in practice

- Summary of key findings 53
- Implementing a cyber security monitoring and logging capability 53
  1. Develop a cyber security monitoring and logging plan 53
  2. Carry out prerequisites for cyber security monitoring and logging 54
  3. Identify sources of potential indicators of compromise 55
  4. Design your cyber security monitoring and logging capability 55
  5. Build or buy suitable cyber security monitoring and logging services 56
  6. Integrate the capability into your cyber security framework 58
  7. Maintain the cyber security monitoring and logging capability 58

About this Guide

This Guide presents details about how to monitor and log cyber security events, some of which are potential indicators of compromise (IOC) that can lead to cyber security incidents if not addressed quickly and effectively. The Guide provides you with practical advice on how to manage logs effectively, deal with suspicious events, use cyber security intelligence and address challenges. It is designed to enable you to prioritise and manage myriad event logs; build an effective cyber security monitoring process and learn about where and how you can get help.

The Guide provides advice and guidance on how to:

- Identify potential indicators of compromise (IOC) at an early stage;
- Investigate them effectively; and
- Take appropriate action to reduce the frequency and impact of cyber security incidents.

The focus of the Guide is on the overall cyber security monitoring process, supported by analysis of cyber security-related events (typically generated from one or more logs) and cyber threat intelligence, bringing context to the process, as shown in *Figure 1* below.

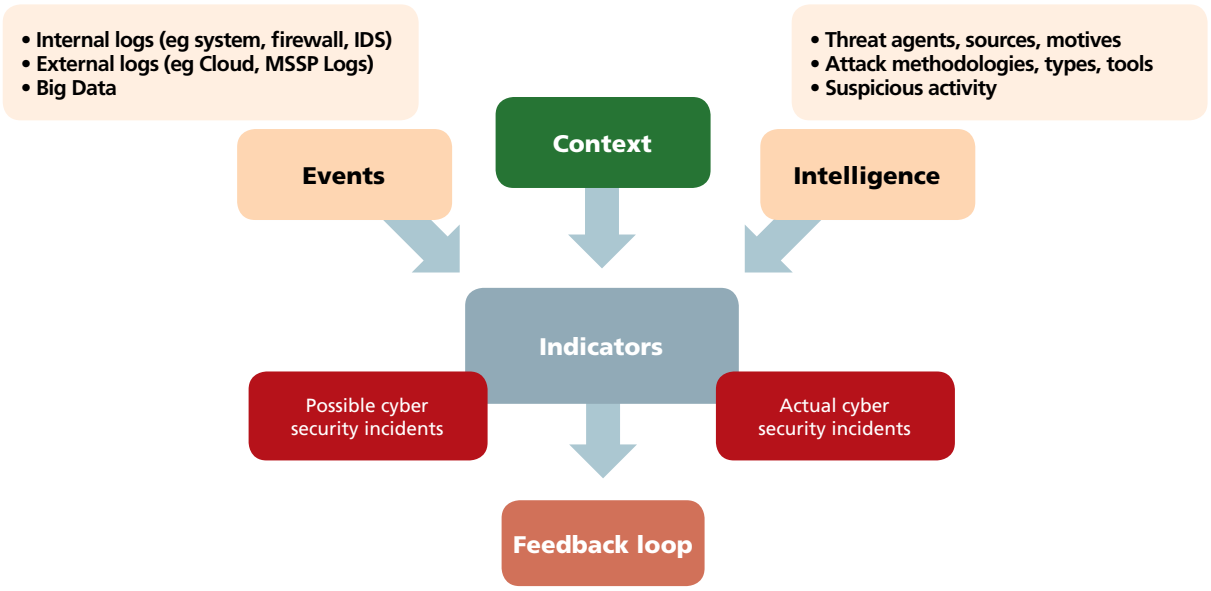


Figure 1: The cyber security monitoring process

The Guide then explores the benefits of using cyber security experts from commercial suppliers and run Security Operations Centres – a key emerging trend. It also introduces a systematic, structured process that can help you select an appropriate supplier(s) to meet your requirements.

Throughout the Guide you will find a set of tips, warnings and quotes provided by a diverse set of contributors, including expert suppliers (such as many CREST members), consumer organisations, government bodies and academia. These bring real-world, practical experience to the Guide, allowing you to get a better feel for the types of action that are most likely to apply to your organisation.

Audience

The CREST Cyber Security Monitoring and Logging Guide is aimed at organisations in both the private and public sector. Project research has revealed that the main audience for reading this Guide is the IT or information security managers and cyber security specialists, but it should also be of interest to business managers, risk managers, procurement specialists and IT auditors.

Purpose and scope

The purpose of this Guide is to help you to meet a range of different requirements identified by a wide variety of organisations wanting to know how to best carry out appropriate cyber security monitoring and logging activities.

The Guide outlines ***Best Practice*** to help you capture important cyber security events, monitor them effectively and take appropriate actions, dependent on your business requirements and level of cyber security maturity.

The main requirements are laid out in the table below, together with the part of this Guide where more detail can be found.

Requirement	Detail
Discover the background to cyber security monitoring and logging, whilst learning about the main challenges faced.	Part 2
Learn how to overcome the difficulties with logging cyber security-related events, configuring logs, fusing them together effectively (eg. using a SIEM), and analysing possible indicators of compromise.	Parts 3
Understand the cyber security monitoring process integrating input from both log management and cyber security intelligence sources, putting them into context (eg. by using situational awareness).	Part 4
Appreciate how an effective security operations centre (SOC) should work, considering the implications of people, process, technology and information (PPTI).	Part 5
Select suitable third party experts to support you, be it for some or all of the cyber security monitoring process or just specialised areas like log management (and analysis); cyber security intelligence; situational awareness; and technical/forensic investigations.	Parts 6
Build or buy your own cyber security monitoring and logging capability.	Part 7

The scope of this Guide could be very large and unwieldy, so it has been refined to focus on key areas, thereby excluding some important cyber security topics (but certainly not all), such as:

- Cyber security incident response, which is covered in a separate CREST guide
- In-depth analysis of fields in event logs, as these are well covered in the CPNI/Context report entitled *Effective Cyber Security Log Management*
- Deep technical analytical tools and techniques, typically used by commercial cyber security monitoring and logging experts
- Cyber security insurance.

The material in this Guide will provide valuable input to each of these topics, any of which could be the subject of a future research project.

A practical solution

This Guide will provide you with a good understanding of the most important elements of cyber security monitoring and logging, highlighting the main challenges and describing ways in which they can be overcome.

However, building, reviewing or improving your own cyber security monitoring and logging capability in practice – or outsourcing it - is not easy. Consequently, a seven stage process has been deigned to help you do this more effectively, which is outlined in *Figure 2* on page 8.



Figure 2: Implementing a cyber security incident management capability in practice

Each step of the process for implementing a cyber security monitoring and logging capability is described in more detail in ***Part 7 Cyber security monitoring and logging*** in practice.

Rationale

This Guide is based on the findings of a research project - ***conducted by Jerakano Limited on behalf of CREST*** – which looked at the requirements organisations have to help them monitor and log events that could lead to cyber security incidents.

Exponential growth in the number of users and devices connected to the Internet has led to an unprecedented expansion in the attack surface that can be exploited by ever more sophisticated cyber security attackers, such as state-sponsored attacks, organised cybercrime and extremist groups.

Monitoring such an extensive battlefield can be an uphill battle in itself – and it is often easier to attack than defend.

The objectives of the cyber security monitoring and logging project were to help organisations:

- Become more difficult for cyber security adversaries to attack
- Reduce the frequency and impact of cyber security incidents
- Meet compliance requirements
- Identify and respond to cyber security incidents at an early stage, doing so quickly and effectively
- Procure the right cyber security monitoring and logging services from the right suppliers.

There were high requirements from organisations who responded to the project survey for a cyber security monitoring and logging Guide to help them in a variety of areas, with the top five responses being to:

- Bring all aspects of cyber security monitoring and logging together in one framework
- Gain senior management support for a cyber security monitoring and logging capability
- Understand what a good Security Operations Centre (SOC) looks like.

- Learn how to carry out cyber security logging and monitoring in a more effective manner – leveraging industry best practice
- Understand the key concepts of cyber security monitoring and logging (eg. drivers, definitions, approaches).

This guide builds on a similar report produced by CREST to help organisations prepare for cyber security incidents, respond to them effectively and follow them up in an appropriate manner. That report, together with a summary of CREST activities can be found at: http://www.crest-approved.org

Project research

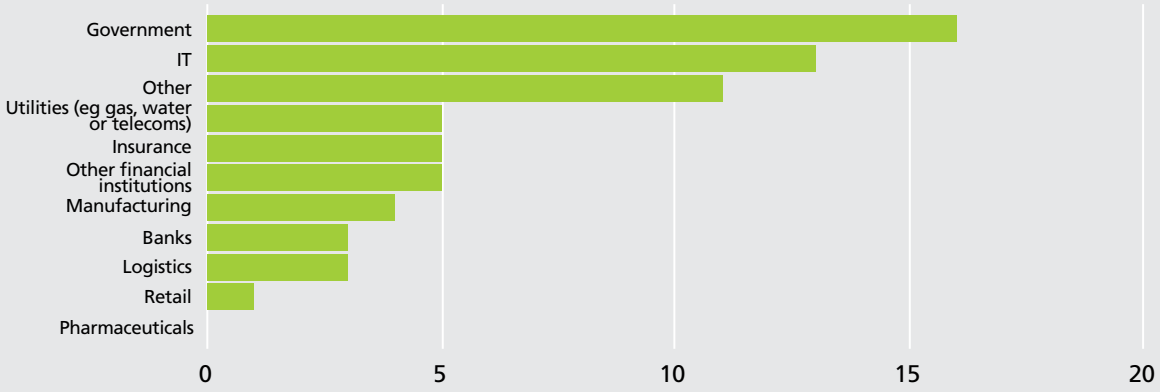
The research project included:

- Performing desktop research on many different sources of information
- Conducting telephone interviews with key stakeholders, such as CREST members and clients
- Undertaking site visits to expert organisations running Security Operation Centres (SOC) on behalf of their clients
- Analysing results from 66 organisations to a detailed project questionnaire
- Running 2 large workshops where experts in cyber security response services from more than 30 organisations determined the scope of the project, validated the findings of this Guide and provided additional specialist material
- Working with the authors of the Effective Log Management report produced by the CPNI and Context.

Profile of respondents to requirements survey

A survey was conducted, primarily aimed at consumer organisations, to help determine project requirements. 66 responses were received in total, from a wide range of types and sizes of organisation, as shown in the chart below.

In which of the following market sectors does this part of your organisation operate?



High level analysis of the profile of respondents revealed that:

- Over half of them were either large or very large
- The number of gateways (eg. web or email) into organisations was well spread from less than 5 to more than 500, 40% having between 11 and 100
- One third of them had over 100 servers, another third over a thousand
- More than 40% had over 5,000 client computers
- Nearly 45% had over 1,000 smart phones/tablets, with nearly 20% having more than 5,000.

Key: Respondents gave an answer to most questions (some were free format text), with responses ranging from 1 (Very Low) to 5 (Very High). Results are presented as charts or tables throughout this Guide, typically showing the average rating across all respondents (eg. 3.29 out of 5).

Overview

Creative, talented and aggressive attackers continue to drive the threat world into new areas. The cyber security threat landscape continues to evolve, with new and innovative attack methods being able to adapt to their chosen target environment(s).

Cyber security incidents – including sophisticated cyber security attacks - can and do occur in many different ways. The risks to your organisation from cyber security incidents are real, with cyber security attacks now regularly causing significant damage to the performance and reputation of many different organisations.

One of the main ways you can deal with suspected or actual cyber security incidents is to record cyber security-related events, monitor them on a continual basis, and investigate suspected cyber security breaches thoroughly, remediating any issues.

However, many organisations have vastly insufficient logging, archiving, correlation and simulation capabilities. This is often because of a range of significant challenges face them when it comes to implementing an appropriate cyber security monitoring and logging capability. Your organisation may therefore need practical guidance to help with monitoring the relevant events on your systems and networks for signs of a cyber security attack.

Defining a cyber security incident

There are many types of incident that could be classified as a cyber security incident, ranging from serious cyber security attacks and major organised cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction.

However, project research has revealed that there is no one common definition of a cyber security incident. The two most common (and somewhat polarised) sets of understanding – as shown in *Figure 3* below - are either that cyber security incidents are no different from traditional information (or IT) security incidents – or that they are solely cyber security ***attacks***.



Figure 3: Different types of cyber security incidents

The main difference between the myriad types of cyber security incident appears to lie in the ***source*** of the incident (eg. a minor criminal compared to a major organised crime syndicate), rather than the ***type*** of incident (eg. hacking, malware or social engineering). Therefore, it may be useful to define cyber security incidents based on the type of attacker, their capability and intent.

At one end of the spectrum come basic cyber security incidents, such as minor crime, localised disruption and theft. At the other end we can see major organised crime, widespread disruption, critical damage to national infrastructure and even warfare.

Capability and intent is what makes both detecting and responding to attacks from well-resourced organised crime/state-sponsored attackers different and more difficult than 'traditional' incidents.

The main focus of this Guide is to help you monitor indicators of possible cyber security attacks, but it will also be useful for monitoring traditional information (or IT) security incidents.

Details about how to prepare for, respond to and follow up cyber security incidents can be found in the CREST Cyber Security Incident Response Guide, available from CREST at http:// www.crest-approved.org

Typical phases in a cyber security attack

Cyber criminals innovate just as business does and the potential rewards for them grow as business use of cyberspace grows. They have access to powerful, evolving capabilities which they use to identify, attack and exploit carefully chosen targets. They also have well-developed marketplaces for buying and selling tools and expertise to execute sophisticated attacks.

Well-resourced attackers, sufficiently motivated by their target, will often innovate and evolve their methods during a single attack, trying different techniques until something works. Evolution and innovation in 'traditional' attacks happens more slowly, with new techniques evolving over time between waves of attack.

For example, in traditional attacks, new variants of malware are released within weeks/months (after many systems have been patched/AV protected). In contrast, in some state-sponsored attacks, the attackers re-compile their malware several times a day to overcome responsive actions taken.

When looking at a cyber security attack in more detail there are often a number of phases that attackers will undertake, which can sometimes take place over a long period of time. An example of the basic components of such a phased approach is outlined in ***Figure 4*** on the following page, together with some of the common countermeasures for each phase.

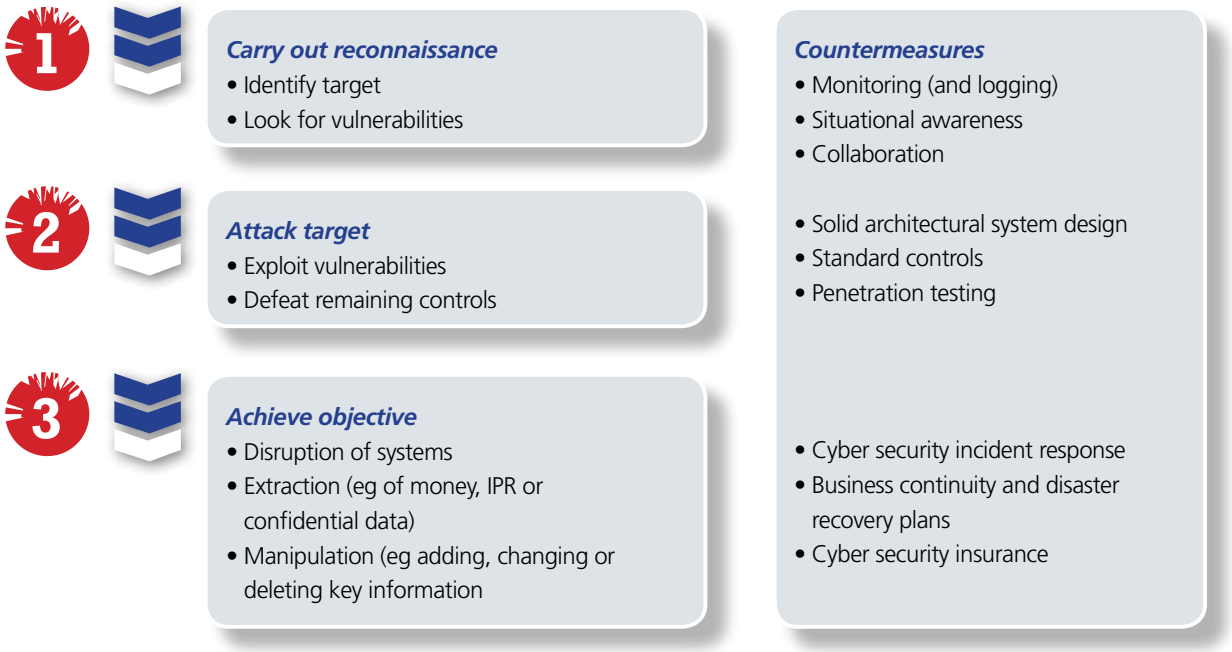


Figure 4: Typical phases in a cyber security attack

When dealing with a sophisticated cyber security attack, it is important to address all stages carried out by an attacker, be they cybercriminals, extremists or state-sponsored agents. However, many organisations do little or nothing before phase 2 (or even phase 3) of an attack, often because they do not have the awareness, resources or technical skills to tackle issues during the reconnaissance stage.

A great deal of monitoring and logging activity is not undertaken until phase 2 or even phase 3 of an attack. Furthermore, phase 2 is often broken down into multiple sub-stages that can take place over minutes, hours or months.

Key value from monitoring at this stage is to detect potential security incidents as early as possible and before phase 3.

Addressing the first phase is critically important and involves a number of preventative measures, scenario development and rehearsal; and the need for extensive collaboration. It is also one of the main focuses of cyber security monitoring and logging, which is explored in the remainder of the Guide.

Monitoring indicators of compromise (which can identify potential cyber security incidents) are covered in *Part 5 Cyber security monitoring process*.

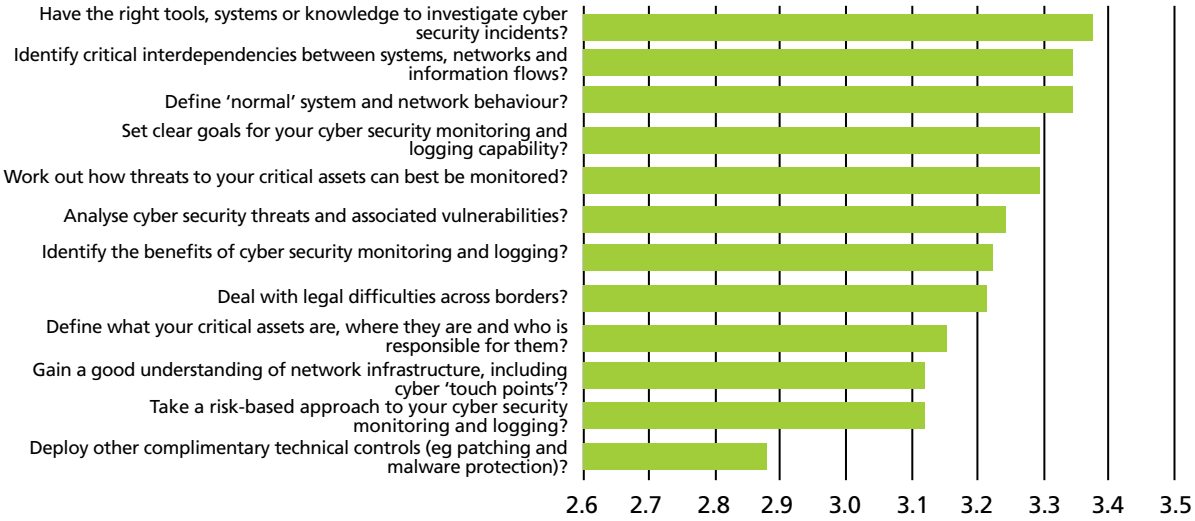
Main cyber security monitoring and logging challenges

Log files and alerts generated by IT systems often provide a vital audit trail to identify the cause of cyber security breaches and can also be used to proactively detect security incidents or suspicious activity that could lead to a cyber security incident.

> "You can't just add things to current security monitoring and logging solutions, you need to bake them into the development or implementation processes"

However, respondents to the Project Survey reported that there were many cyber security monitoring and logging challenges facing them (most of which can be addressed using this Guide), as shown in the chart below.

What level of challenge does your organisation face in being able to:



Cyber security monitoring and logging maturity

There was a big variation in the level of maturity respondents to the Project Survey believed that their organisations have for different cyber security monitoring and logging activities.

What level of maturity does your organisation have for the following cyber security monitoring and logging activities?	Very low	Low	Medium	High	Very high
Logging all necessary cyber security related events	9%	12%	30%	21%	23%
Collating and analysing logs	12%	18%	30%	17%	21%
Using threat intelligence	14%	9%	35%	21%	15%
Identifying suspected (or actual) cyber security incidents	8%	14%	32%	20%	21%
Responding to cyber security incidents	6%	12%	38%	20%	21%

Respondents showed greater maturity in cyber security monitoring and logging than in the identification and analysis of unusual events – which is the focus of this project.

Many respondents seemed to believe that their organisation was more mature in cyber security monitoring and logging than their responses to the rest of the Project Survey would indicate, showing that there is still a strong need for awareness in this area.

Standards and guidelines

There are many standards that specify (or allude to) requirements for cyber security logging (but very few about cyber security monitoring), which include:

- ***10 Steps to Cyber Security*** and the ***Cyber Security Essentials*** from CESG
- ***ISO 27002*** - Section 12.1 Logging and Monitoring
- ***PCI DSS V3.1***, particularly:
  - Part 10. Track and monitor all access to network resources and cardholder data
  - Part 11. Regularly test security systems and processes
- The SANS ***20 Critical Controls for Effective Cyber Security Defence*** particularly:
  - Control 14 – Event logging
- The ***NIST 800-137 Information Security Continuous Monitoring (ISCM)*** for Federal Information Systems and Organizations as part of a directive from the Federal Information Security Management Act (FISMA).

"Being fully compliant with standards is still likely to leave you exposed to cyber security incidents"

There are also a number of good sets of guidance in this area, which include:

- ***Effective Log Management*** from the Centre for the Protection of National Infrastructure (CPNI) in conjunction with Context (April 2014)
- CESG's ***Good Practice Guide 13 (GPG13): Protective Monitoring for HMG ICT Systems***
- Magic quadrant analysis of related tools, such as the ***Gartner Magic Quadrant for Security Information and Event Management 2014***
- SANS Analytics and Intelligence Survey (October 2014)
- IDC Market Analysis – ***Worldwide Specialized Threat Analysis and protection 2013 – 2017 forecast***
- ***Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment*** from the SANS Institute InfoSec Reading Room (July 2012)
- ***Guide to Computer Security Log Management*** (SP 800-92) from NIST (Sept 2006)
- Many different vendor publications (often product-led).

However, although these compliance and guidance documents are often very useful, they do not typically provide:

1. Coverage of all aspects of cyber security monitoring and logging in one framework - more focus is needed on the actual monitoring process, plus specialised areas like security intelligence, SOCs and analysis of advanced persistent threats (APT)
2. Best practice for ***logging and monitoring*** cyber security (eg. focused on identifying, interpreting and responding to indicators of compromise - IOC), particularly for consumer organisations outside government or Finance sectors
3. Guidance on how best to use scarce security budgets and resources – what's the best ***'Bang per buck'?***
4. Advice on who organisations can ask for help – backed up by selection criteria.

The need for support from third party experts

Organisations of all types are struggling to identify and address potential indicators of cyber security incidents effectively, with a growing number of cyber security incidents now occurring on a regular basis – often causing significant business impact.

Many larger organisations can carry out a number of cyber security monitoring and logging activities themselves, sometimes very successfully – but smaller organisations typically need expert help. However, when it comes to identifying indicators of compromise for sophisticated cyber security attacks (particularly at an early stage) virtually all organisations should consider employing the services of one or more specialist third party cyber security monitoring and logging providers for at least some activities (eg. analysing events in a Security Operations Centre; providing situational awareness; performing advanced data analytics; investigating advanced types of cyber security attack; or analysing evidence of unusual occurrences).

There are many benefits in procuring cyber security monitoring and logging services from a trusted, certified external company who employs professional, ethical and highly technically competent individuals. Many CREST member companies are certified cyber security monitoring and logging organisations (CREST CSIR members) who fully meet these requirements, having been awarded the gold standard in technical cyber security services, building trusted relationships with their clients.

Requirements

Important security-related events should be recorded in logs, stored centrally, protected against unauthorised change and analysed on a regular basis. This will help in the identification of threats that may lead to a cyber security incident (also known as 'indicators of compromise' or IOCs), maintain the integrity of important security-related information and support forensic investigations.

Your organisation should adopt a real time solution that automatically isolates the key events you need to know about (which you should have specifically defined), when you need to know them, so that you receive instant advice about useful or critical matters that are no longer buried in a mountain of less important data. This will help to ensure appropriate cyber security-related events are identified earlier – and then analysed and actioned more quickly and effectively.

Requirements for cyber security event logging should cover:

- Management of event logging (eg. setting policy, defining roles and responsibilities, and reporting)
- Identification of business applications and technical infrastructure systems on which event logging should be enabled, including those that have been outsourced or are 'in the cloud'
- Configuration of information systems to generate the right cyber security-related events
- Regular 'tuning' and review to reduce the number of false positives to an acceptable level
- Storage of security-related events within event logs (eg. using local systems, central servers, SIEMs or by using storage provided by an external service provider)
- Analysis of security-related event logs (including normalisation, aggregation and correlation)
- Synchronisation of time stamps in event logs to a common, trusted source
- Protection of security-related event logs (eg. via encryption, access control and backup)
- Defined retention requirements and/or log rotation periods
- Taking necessary actions to remediate any issues identified and respond to cyber security incidents in a fast, effective manner.



Some organisations that have synchronised their logs have not actually done this as well as they think they have, so events in certain timelines could be missed.

Analysis was restricted to monitoring from a cyber security incident management perspective, but logs can also be used for compliance and awareness purposes, covering topics like:

- Monitoring/efficiency/performance
- Status/asset management.



Storage solutions are often cloud-based (with doubtful or unknown security arrangements) and the security of actual physical servers can be overlooked.

Findings from project research revealed that effective logging can save you time and money if you should experience a cyber security incident – and that it can also be very helpful as part of a defence (or prosecution) in a court case. You should therefore:

- Establish cyber security-related logging standards and procedures
- Configure systems to record the most important cyber-security related events and monitor these events for specified purposes
- Respond to alerts correctly (eg. to avoid overlooking indicative alerts or over-reacting to benign alerts)
- Aggregate what may seem like benign alerts into what is a coherent threat message
- Make appropriate event logs available to investigators in a suitable format
- Retain logs according to retention standards/procedures, storing them securely for possible forensic analysis at a later date.

Logging challenges

There are many challenges facing organisations when it comes to monitoring the relevant events on their systems and networks for signs of a cyber security attack. For example, organisations often collect a lot of cyber security-related data, but do not have the resources, technical skills or awareness to analyse that data effectively.

> "Organisations can put blind trust in the monitoring tools they have purchased, giving them a false sense of security"

Project research revealed that many long established, 'traditional' logging challenges still remain, which includes organisations:

- Struggling to understand the purpose, importance and effectiveness of the full range of data sources (putting them into some sort of 'pecking order' of importance)
- Suffering from the sheer volume of log management tasks such as:
  - o Turning on relevant logs, logging them correctly and keeping them long enough
  - o Prioritisation, storage, correlation and protection of logs
- Failing to examine alerts in an effective manner (eg. handling false positives, performing situational analysis and remediating issues)
- Being unsure as to which logs they need to pay most (and least) attention or the implications of the events that they record
- Not being able to find the right tools and people to help them easily, effectively and at the right price.

Many challenges reported are still traditional logging challenges that go back many years, but they have actually got worse in recent times due to the:

- Proliferation of data located outside the perimeter, such as in-cloud service providers or outsourced arrangements
- Vast amounts of structured and unstructured data, fuelled by the rise of consumerism (eg. social networking), creating data sets so large and complex that traditional data processing approaches are inadequate – often referred to as 'Big Data'.

> "We are not just looking for a needle in a haystack; we have to find the right haystack(s)"



Addressing many of the traditional logging challenges in depth – such as examining detailed fields in event logs - is out of scope for this project as they are well covered in other guidance, such as the CPNI/Context report *'Effective Log Management'*.

Configuring cyber security event logs

Workshop participants identified four main types of event logs that can be useful for cyber security monitoring, as shown in the table below. These logs are primarily used to help with detection of potential cyber security incidents and / or their investigation.

Type of logs	Examples
System logs	• System activity logs (eg. Administrator), including storage • Endpoint (and agent-based) logs • Logs from standard (eg. SAP) and customised applications • Authentication (eg. Windows) logs • Physical security logs
Networking logs	• Email, firewall, VPN and Netflow logs
Technical logs	• HTTP proxy logs • DNS, DHCP and FTP logs • Web and SQL server logs • Appflow logs
Logs from cyber security monitoring and logging tools	• Malware protection (eg. anti-virus) logs • Network intrusion detection systems (NIDS) • Network intrusion prevention systems (NIPS) • Data loss protection (DLP) • Tools that employ potential malware isolation and investigation techniques (eg. sandboxing or virtual execution engines) • Other relevant security management appliances or tools

These cyber security event logs should be configured to:

- Enable event logging (using a standard format, such as syslog, MITRE Common Event Expression, or equivalent)
- Generate appropriate event types
- Incorporate relevant event attributes in event entries (eg. IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name)
- Use a consistent, trusted date and time source (eg. using the Network Time Protocol (NTP, supported by global positioning.)



There are many different possible cyber security-related events that need to be recorded in these event logs, such as:

- System crashes, service creation and object deletion
- Failed login attempts and inappropriate login of authorised users (eg. at unusual times or when they are absent)
- Unsuccessful changes to access privileges
- Deletion of user accounts

Cyber security-related event logging should be:

- Enabled at all times
- Protected from unauthorised access and accidental or deliberate modification or overwriting (eg. using write-only media or dedicated event log servers)
- Configured so that when event logs reach a maximum size, the system is not halted through lack of disk space and logging continues with no disruption.

Turning on significant event monitoring for a system can:

- Produce unpredictable results and could seriously detract from the resources available to the rest of our systems or networks
- Place a large overhead on bandwidth, host processing capacity and memory

Centralised log management

You should combine key information from as many of the different logs as possible (where relevant) into one central repository, such as a ***Security Information and Event Management (SIEM)*** system.

For example, evidence of an incident may be captured in several logs that each contains different types of data:

- A firewall log may have the source IP address that was used, whereas an application log may contain a username
- A network IDS sensor may detect that a cyber security attack was launched against a particular host, but it may not know if the attack was successful.

An investigator may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.

SIEM solutions are a combination of SIM (security information management) and SEM (security event manager) systems. SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.

Some modern SIEMs provide additional features, such as the ability to handle 'Big Data' or the provision of a dashboard for analysis and monitoring.

SIEM services

A number of services that suppliers can provide for the cyber security monitoring and logging arena are in the SIEM arena, which includes:

- Managed Security Services Providers (MSSP) solutions for SIEM and threat intelligence
- 'Dropship' SIEM solutions (basically a server supplied by the supplier with the customer managing the service with no real external support)
- Hybrid SIEM MSSP services - with threat intelligence fed into the SIEM, supported by SOC analysis.

Workshop participants agreed that 'information is only any good if it is actionable'. It therefore needs context, analysis and interpretation. It should also include Big Data, taking a much richer set of data sources into account (over and above just event logs) in the detection, triage and investigation processes at the heart of cyber security monitoring.

Examples of producing actionable intelligence include generating metadata from every single web, email and other key network transaction; and taking contextual data sources such as device catalogues and user account data. The value of this in a cyber security monitoring context is the increased ability to detect particular attacks that have been crafted to avoid being detected by traditional security devices and hence logs from such devices are of limited use on their own.

Finally, information being analysed should be backed up with proper security intelligence and be supported by automation.

From an MSSP perspective, there are differing approaches to classifying and managing "Personally Identifiable Information" (PII) in log streams. For example, there are multiple locations where organisations store and back up data and they are rightly concerned from a DPA compliance perspective about where that data is stored and how it is protected.

You should therefore review the need for your organisation to:

- Store data in a data centre (even using cloud computing) in your own region (eg. Europe)
- Identifying when and how to filter out PII data, if necessary
- Obfuscate or mask data to protect PII information – considering how attackers might be able to remove this protection.

Prioritising log use

Many of the log management challenges are associated with:

- The vast volume of event logs produced by myriad applications, systems, tools and networks;
- Which ones are most relevant; and
- The cost (and resources) required to handle them effectively.

Your organisation should therefore seek to understand the wide range of logs available and prioritise which logs you need to monitor. Your organisation may not be able to monitor everything (or wish to do so) due to a lack of security budget or specially skilled analysts. It is therefore important that you concentrate on the data and services that are absolutely critical to your business.

Event logs can typically be categorised as system logs, network logs, application logs and logs generated by commercial tools, such as malware protection and intrusion detection (IDS) software. However, these logs can also be considered in terms of their value from a cyber security monitoring perspective.

Workshop participants determined what they believe are typically ***essential, important or useful*** logs; what they are commonly used for; and how much they cost (broadly speaking). This data was then supplemented by the extent to which five different actions were carried out by respondents to the Project Survey for each of these types of logs.

Prioritisation of cyber security-related logs during the workshop was mainly based on typical requirements for identifying possible cyber security attacks, so may vary for other types of cyber security incident, such as fraud or abuse.

The results of this analysis are presented in the tables below. There was not complete agreement amongst experts, for example with some analysts arguing that endpoint logs are often important or even essential.

Essential - priority 1						
	Cost	**Collect**	**Retain**	**Monitor**	**Analyse**	**Respond**
Email	Free	59%	56%	44%	24%	17%
HTTP proxy	Free	54%	44%	39%	22%	15%
Malware protection logs	£	59%	46%	66%	46%	51%
NIDS	££	59%	49%	51%	44%	41%
NIPS	££	54%	41%	41%	32%	29%

Important - priority 2						
	Cost	Collect	Retain	Monitor	Analyse	Respond
System activity logs (eg Admin)	Free	63%	56%	59%	37%	29%
Firewall	Free	66%	51%	56%	34%	34%
DNS	Free	46%	37%	41%	17%	15%
DHCP	Free	44%	24%	29%	17%	15%
Web Server logs	Free	49%	29%	37%	20%	12%
SQL server logs	Free	44%	29%	34%	10%	10%
Sandboxing techniques (including vitual execution engines)	£££	27%	22%	32%	29%	15%

Useful - priority 3						
	Cost	Collect	Retain	Monitor	Analyse	Respond
Endpoint (and agent-based) logs	£	49%	44%	49%	27%	24%
Authentication logs (eg Windows)	Free	56%	51%	49%	32%	29%
Physical	££	44%	37%	32%	24%	17%
VPN	Free	61%	49%	44%	22%	27%
Netflow	Free	34%	24%	29%	10%	17%
FTP	Free	37%	22%	27%	7%	10%
Appflow	Free	17%	12%	17%	5%	2%
Data loss protection (DLP)	££	24%	22%	32%	24%	27%



Costs cover purchase and ongoing cost of any relevant tools and services, but exclude resourcing. Logs marked in the cost column as 'None' should be freely available unless you are using outsourcers or MSSPs.

No logs are completely free as they will all involve some cost (eg. to obtain, store and analyse) - but those marked as free are already 'baked-in' to systems, networks, tools or services that your organisations has already paid for.

Whilst this analysis should be very useful for many organisations, these logs are only the ones that workshop participants believed could ***typically*** be categorised in these ways.

In practice, the importance, cost and use of these logs may differ considerably for any given organisation, for example based on the type of organisation, the nature of their business, and their maturity in cyber security. Consequently, log management will need to be evaluated on a case-by-case basis.

Targeted log identification

Analysis carried out by participants at the project workshop outlined a possible approach to help identify the logs you require for specific purposes, which included:

- Identifying relevant business objectives
- Understanding the risks in achieving these business objectives
- Prioritising logs required based on Use Cases, recognising the maturity of your organisation in terms of cyber security monitoring and logging (a reality check)
- Starting small, then increasing knowledge and maturity
- Presenting guidance in terms of business objectives (eg. what logs do you need to detect malware infection?)
- Categorising log sources in terms of what they help to detect.

An example of a possible ***Use Case*** to detect 'improper or unauthorised account usage' is outlined in the table below.

Component	Description
Business objective 1	Detect suspicious, improper or unauthorised activity (internal or external who has penetrated)
Use Case 1	Segregation of duties
Scenario 1	• Same account on multiple machines • Two or more accounts used on same machine
Main log(s)	• Business application
Logs used as sources of intelligence	• Authentication (application, Active Directory) • DHCP • Proxy (for cloud apps – and internal?) • VPN (if applicable) • Physical

Based on the 'Use case' approach, workshop participants highlighted that there would typically be:

- Many business objectives
- Multiple Use Cases produced for any given business objective
- One or more scenarios for each Use Case
- Less logs, as the same logs would be used to support multiple scenarios.

A possible Use Case model is illustrated in ***Figure 5*** below.

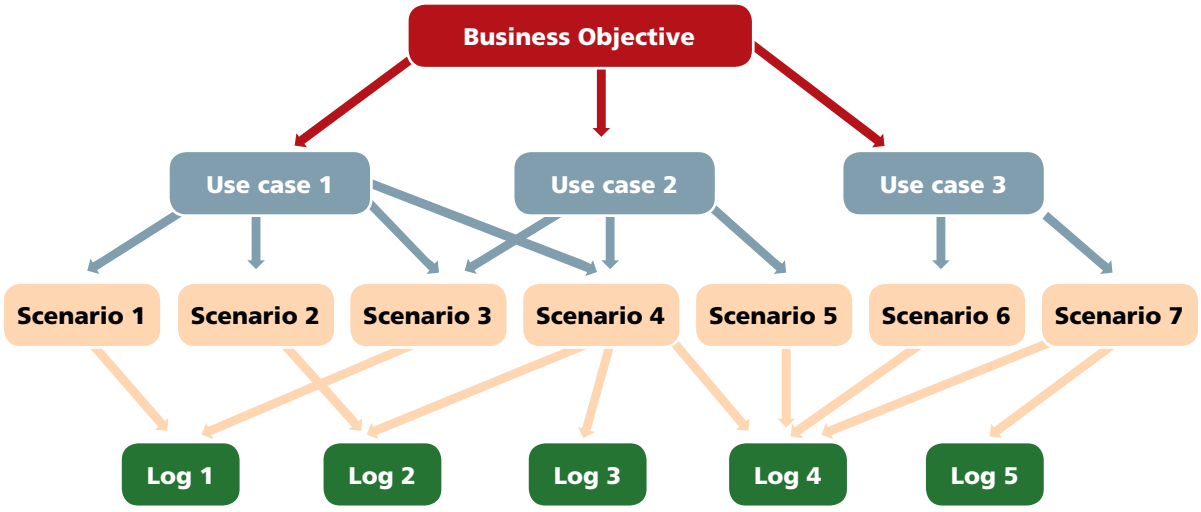


Figure 5: Possible model for multiple Use Cases

This model can be used to inform and broaden conversations with the business.

Analysing logs and alerts

Security-related event logs should be analysed regularly by skilled analysts (eg. using automated security information and event management (SIEM) tools or equivalent) to help identify anomalies, and include:

- Processing of key security-related events (eg. using techniques such as normalisation, aggregation and correlation)
- Interpreting key security-related events (eg. identification of unusual activity)
- Situational awareness (putting the events in context), backed up by various types of internal, commercial and government sources of cyber security intelligence
- Responding to key security-related events (eg. passing the relevant event log details to a cyber security incident management team).

Security information and event management (SIEM) tools should be configured (often referred to as tuning) to:

- Identify expected events (to help reduce review and investigation activities for legitimate business events)
- Detect unexpected events (to help reduce the likelihood false negatives)
- Manage confusing or misleading data, often referred to as 'noise' (as opposed to 'signal') generated by event logs.

"We have been working with a SIEM for some time and the biggest challenge is to find appropriate use cases which makes sense and are possible to be implemented"



Organisations may believe they are monitoring events to detect potential indicators of compromise, but even though they have an IDS (or even a SIEM), they fail to:

- Monitor all relevant events
- Carry out monitoring regularly enough - or in an appropriate manner
- Aggregate what may seem like benign alerts into what can be a coherent threat message

Using log management tools

To help face these log management challenges, many organisations use a variety of log management tools and techniques, such as IDS, SIEM and tools that employ potential malware isolation and investigation techniques (eg. sandboxing or virtual execution engines).



Responses to the Project Survey revealed extensive use of tools and services, be they basic log management tools, SIEMs, managed security services (MSS) or Security Operations centres (SOCs). However, only just over half the respondents stated that they use a SIEM (although their SOC probably would, where they use one), which may cause them difficult log management issues.

Findings from the Project Survey revealed that organisations face significant challenges in acquiring cyber security log management tools and services, nearly all respondents found it difficult or very difficult to:

1. Find effective cyber security monitoring and logging products at a reasonable price
2. Obtain relevant log details from service providers (eg. because it is not in the contract)
3. Configure their cyber security appliances or tools effectively
4. Create meaningful and helpful requests for proposals (RFP), rather than just re-using standard format
5. Deal with the proliferation of 'specialist' (often proprietary) tools and their lack of integration
6. Use a SIEM tool for cyber security purposes
7. Determine which cyber security appliances, tools or services they need
8. Purchase cyber security appliances or tools for cyber security purposes, rather than to just meet compliance requirements
9. Clarify the specific functionality and purpose of products and services that vendors are actually selling.

"It's tough to do cyber security monitoring and logging well – and expensive. It is often easy for organisations to do something (like buy an IDS or SIEM product), but tough to make it effective"

Analysis of external log management tools

Workshop participants identified and evaluated a range of commercial and open source tools that can be used to support cyber security logging in two main different categories, being log management/analysis and SIEM. They evaluated these tools in terms of their usefulness, value for money and complexity.

The results of this analysis indicate that:

- Many log management/analysis tools, be they commercial or open source, can be very useful at a reasonable cost, but are often complex
- Most leading SIEM tools are very useful (although sometimes not as useful as vendors claim), but are typically both expensive and complex to implement properly.



Organisations could make better use of free open source tools (there are many), and home grown scripts.

Workshop participants highlighted that there are a wide range of issues to consider when selecting an appropriate set of log management tools, which go beyond the topics highlighted above and often include the need to consider:

- Implementation and preliminary work required for each tool
- The volume of data, how it is stored and retention requirements
- Log data jurisdiction and compliance requirements
- Data retention requirements
- Searching and querying data
- Data segregation.



It can be useful to do a SWOT analysis to look at the security monitoring tools and boxes you need, considering a range of topics, such as :

- Your objective for log management, as well as the criticality of the data and services concerned
- Whether the device or tool is in-line (such as a firewall) or sits to the side
- Commercial, open source or home grown solutions

The essentials of cyber security monitoring

The previous chapter examined the essentials of cyber security log management, but this is only one of a number of different components required in a cyber security monitoring process if an organisation wants to identify, investigate and respond to indicators of compromise effectively. The main components of a typical cyber security monitoring process are shown in *Figure 6* below and explored in more detail in the remainder of this chapter.

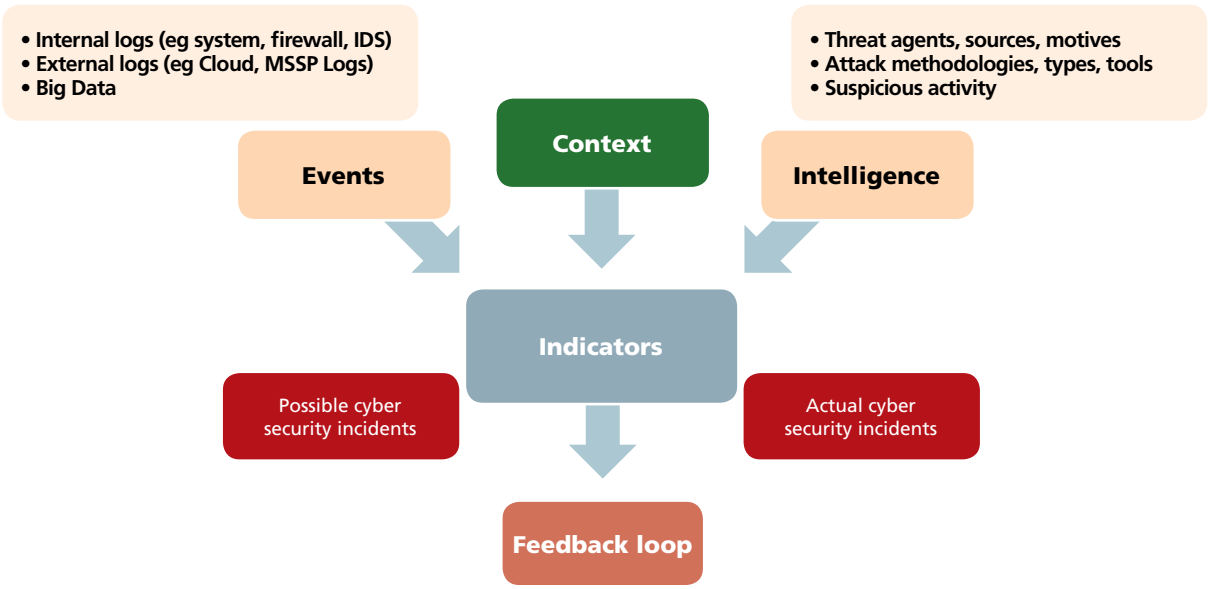


Figure 6: Cyber security monitoring process

> "Cyber security monitoring can be compared to maintaining motor cars: some cars are not maintained at all, some have regular servicing by qualified engineers and others (like in F1 motor racing) have real-time monitoring"

Monitoring purpose and scope

Most respondents to the Project Survey said the main focus of their cyber security monitoring process was in:

- Looking for indicators of potential cyber security incidents
- Adhering to contractual or certification standards (eg. ISO 27001) and good practice (eg. ISF SOGP)
- Meeting compliance requirements (eg. for PCI DSS or FCA).

More than two thirds of respondents also stated that their main focus is on ***'doing the minimum'***, with 12 of them answering 'High' or 'Very High'.



Doing the minimum could be a good thing in some cases, as one of the major challenges was financial and a key finding is to *prioritise* activities.

Monitoring focus

Different types of cyber security monitoring can be categorised in a number of ways, such as by looking at a combination of:

1. In-line monitoring (eg. looking at traffic passing through a firewall)
2. Not in line monitoring, which includes:
    - Analysing information about 'activity' based intrusion detection
    - Employing heuristic-based rules
    - Taking the 'Big data' approach.

Most respondents to the Project Survey said that their cyber security monitoring process covered their:

- Network perimeter
- Endpoints (eg. PCs and laptops)
- Core devices and systems (internal).

However, many respondents stated that their cyber security monitoring process does not fully cover core devices and systems that are outsourced or cloud based.

Monitoring systems that are outside your direct control (eg. those that have been outsourced or are run 'in the cloud') can be an extremely daunting prospect – but can be critical in helping to identify IOCs in a timely and effective manner.

About three quarters of respondents said they considered cyber security monitoring and logging in:

- Cloud computing services
- Outsourcing arrangements
- New projects.

But far less considered them for mergers and acquisitions.

Cyber security monitoring challenges

A range of different monitoring challenges were experienced by most respondents to the Project Survey, with the top five being to:

- Determine where best to spend the cyber security budget
- Detect anomalous system and network behaviour, distinguishing real anomalous behaviour from 'noise'
- Determine that an event is actually a cyber security incident
- Link threat intelligence and log outputs to provide an overall picture of your threat profile
- Justify the cost / time to deal with very rare cyber security incidents.

For many organisations, the most challenging part of the monitoring process is accurately detecting and assessing possible cyber security incidents - determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

"Not every attack is a cyber security attack – so situational awareness is important"

Organisations often treat a cyber security incident as if it is a single one-off event. In reality, for most sophisticated incidents, they may have been going on for some time (including reconnaissance) and/or cover more than one part of your organisation.

Prerequisites for cyber security monitoring

When monitoring cyber security events, one of the most important actions is to be properly prepared. In the event of a cyber security incident occurring this will help you to recover your systems more quickly, minimise the impact of the attack, instil confidence in your customers and even save you money in the long term.

Preparation is often crucial, but can easily be overlooked because of a lack of awareness, support or resources.

Workshop participants identified that to build an effective cyber security monitoring process; you should take a ***prioritised*** approach, which can be built around a few initial steps (prerequisites).

Most respondents had a very high level of support (around 3.5 out of 5) for most of the prerequisites explored in the Project Survey, which included:

- Agreeing objectives and scope
- Defining primary or critical assets – and determining where they are within the organisation
- Identifying external cyber (eg. internet) 'touch points'
- Determining what possible cyber security attacks on critical assets might look like
- Minimising attack paths to these assets
- Addressing key technical controls on the perimeter – and reducing the attack surface
- Reviewing and revising cyber security (and other) controls currently in place in this area.



These steps help to create a 'baseline' environment where the cyber security monitoring process can be focused – and for which senior management 'buy in' can be obtained.

Cyber security threat analysis

In the past, enterprise risk and security decisions have been mainly based on theoretical risk assessment exercises only. This trend was encouraged by a compliance-oriented mind-set – which still persists in many organisations that are less mature in their approach to cyber security.

This led to the emergence of threat landscape monitoring and threat intelligence capabilities. Cyber threat intelligence strengthens monitoring and response capabilities by supplying the required information, which can be made actionable and help organisations prepare for emerging threats.

> "Compliance does not equal security"

To undertake cyber security monitoring, it can be useful to understand the level of threat to your organisation from different types of cyber security incidents, which is often achieved by carrying out a cyber security threat analysis. To do this, you should first have produced a definition of what cyber security incidents mean to your organisation and created a set of examples of the types of threats associated with these incidents, such as malware, hacking and social engineering.

In order to contextualise the cyber security threat analysis, you will need to gain a solid understanding of the:

- Nature of your business, business strategy, business processes and risk appetite
- Key dependencies your organisation has; for example on people, technology, suppliers, partners and the environment in which you operate
- Assets that are likely to be targeted, such as infrastructure, money, intellectual property or people – and the computer systems that support them
- Potential compromise to the confidentiality of sensitive information; the integrity of important business information and applications; or the availability of critical infrastructure.

Bearing in mind these important business elements, you can then focus your threat analysis on the:

- Technical infrastructure that supports your critical assets
- Cyber security landscape relevant to your organisation
- Different types of cyber security threats that you are concerned about
- Sources of these threats, such as organised crime syndicates, state-sponsored organisations, extremist groups, hacktivists, insiders – or a combination of these
- Possible threat vectors for attacks to exploit (eg. Internet downloads, unauthorised USB sticks, misconfigured systems, inappropriate access, or collusion)
- Vulnerabilities to each particular threat (eg. control weaknesses or special circumstances).

Focus should be placed on addressing the root cause of potential cyber security incidents and not merely fixing flaws discovered during cyber security threat scenario exercises.

Key phases in the monitoring process

Once the prerequisites have been completed, there are four key phases that are required to perform an effective cyber security monitoring process on a continuous basis, as shown in ***Figure 7*** below.

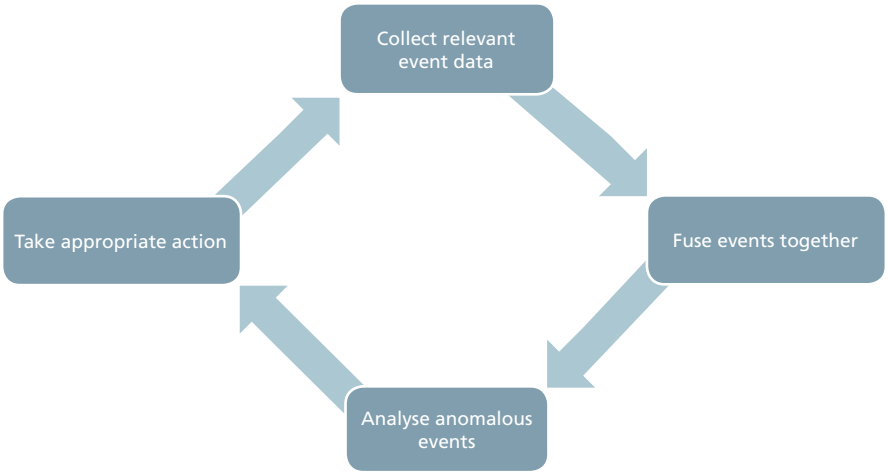


Figure 7: Cyber security monitoring – key components

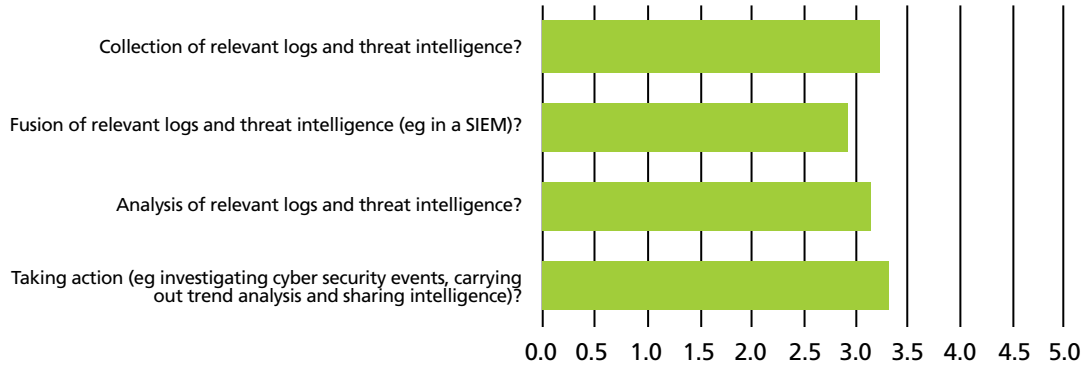
These four phases are part of a continuing cycle with lessons learnt from actions taken in stage four being fed back into the other three phases.

Workshop participants reviewed each of the four phases in the cyber security monitoring process, outlining the main components of each in the table below.

Phase	Main components
COLLECTION (mostly machine)	• Log identification • Normalisation (if going on to monitor) • Retention • Filtering
FUSION (mostly machine)	• Automation (typically in a SIEM) • SIEM rules • Firewall rules • IDS signatures/IOC
ANALYSIS (mostly human)	• Predetermined rules • Triage (investigation) • Workflow • Trends/patterns/risk analysis • Cyber security intelligence
ACTION (mostly human)	• Response, remediation and recovery • Escalation (internal and external) • Investigation • Incident management (including root cause remediation) • Reporting • Change management

Varying numbers of respondents to the Project Survey said that they covered each of the phases in the cyber security monitoring process, as shown in the chart below.

To what extent does your cyber security monitoring process cover:



Fusion of logs appears to be a particularly challenging activity for many organisations, reinforcing the point that SIEM tools are a key part of any effective cyber security monitoring process.

Indicators of compromise

In many organisations, thousands of possible signs of incidents may occur each day, recorded mainly by logging and computer security software, but IT and other management do not always know the best ways to detect them.

Many of these security events can be indicators of compromise (IOC) as they can show that a cyber security incident may be in progress, about to take place or has already occurred.

Ways in which IOCs can be detected include:

- Understanding threat actors and how they operate, keeping up to date with their techniques and 'modus operandi'
- Identifying the way attack (including reconnaissance) tools are developed
- Linking cyber security threat intelligence to forensics
- Determining how attackers maintain a persistent connection as this often underpins many aspects of their overall attack strategy
- Distinguishing real anomalous behaviour from 'noise'.

Project research revealed that one of the key objectives for cyber security monitoring and logging is in identifying *anomalous* – rather than just abnormal – behaviour.

"How do we work out what 'bad' looks like?"

Logs and other sources that can be potential indicators of compromise (also known as triggers, alerts or alarms) will be either (or both):

- Precursors, which are signs that an incident may occur in the future
- Indicators, which are signs that an incident may have occurred or be occurring now.

Examples of possible cyber security incidents	The sources of these signs include…..
Precursors can include: • Web server log entries that show the usage of a vulnerability scanner • An announcement of a new exploit that targets a vulnerability of the organisation's mail server • A threat from a group stating that the group will attack the organisation. Indicators (there are many) can include: • A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server • Antivirus software alerts when it detects that a host is infected with malware • A system administrator sees a filename with unusual characters • A host records an auditing configuration change in its log • An application logs multiple failed login attempts from an unfamiliar remote system • An email administrator sees a large number of bounced emails with suspicious content • A network administrator notices an unusual deviation from typical network traffic flows.	• Security software (eg. IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software, monitoring services (often provided by a third party)) • Logs (eg. operating system logs, service and application logs, network device logs and network flows) • Publicly available information (eg. information on new exploits, information exchange groups, third party organisations, governments) • People from within your organisation • Third parties (eg. customers, suppliers, IT providers, ISPs, partners; government bodies).

Sources of IOCs

There are many different sources of data that relate to IOCs, which include:

- Security software (eg. IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software, and monitoring services (often provided by a third party))
- Tools that employ potential malware isolation and investigation techniques (eg. sandboxing or virtual execution engines)
- Logs (eg. operating system logs, service and application logs, network device logs and network flows)
- Publicly available information (eg. information on new exploits, information exchange groups, third party organisations, governments)
- People from within your organisation
- Third parties (eg. customers, suppliers, IT providers, ISPs, partners; government bodies).

Workshop participants identified a range of publicly available sources of data that can be used in conjunction with cyber security events to help identify indicators of compromise (IOC), evaluating the purpose, likely criticality and cost of each source.

The results of this analysis are presented in the table on page 31 (in descending order of criticality), together with their purpose, criticality and relative cost.

Ref	Name of source	Purpose	Criticality	Cost
1	Internal/historic	• Trends • Priorities	Essential	Free
2	Commercial – mainstream	• Awareness • Commodity malware	Important / Essential	£
3	Law enforcement	• Criminals	Important / Essential	Free
4	Government	• Breach notification - very specific (national element)	Important / Essential	Free
5	Communities of interest (eg. CISP)	• Can cover all - specific value in target organisation	Important	£ or free
6	Open source intelligence (OSINT)	• Covers all (consider quality)	Important / Specialised	Free
7	CERT	• Specific value in target organisation	Important / Specialised	£ or free
8	Specialist COI	• Specific value in target organisation	Important / Specialised	£ or free
9	Commercial – specialist	• Targeted attack	Specialised	££

Open-source intelligence (OSINT) is intelligence collected from publicly available sources. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to closed industry or professional groups; and covert or clandestine sources); it is not related to open-source software or public intelligence.

The cost to process many of these sources of data tends to be the inverse of the cost to buy them.

Logs used to help identify IOCs

When analysing potential sources of information for indicators of compromise, most respondents analysed internal logs. However, very few (around 20% or less) analysed the following data to a high or very high extent:

- Threat intelligence (eg. reconnaissance data; suspicious threat agent activity; analysis of impact)
- External logs (eg. Cloud, MSSP)
- 'Big Data'.

Without analysing information from these three areas it will be very difficult to detect or address many potential indicators of compromise.

Cyber security threat intelligence

When monitoring cyber security events, it is essential to have access to appropriate, up-to-date cyber threat intelligence. This should include research into the attackers to determine their capabilities, motives and likely actions. Much of this kind of intelligence can be provided by the government, CERTS, collaborative groups or expert third parties, such as many CREST members.

If you use cyber threat intelligence, you will more clearly understand the tactics, techniques and procedures of the attackers and your organisation may be able to defeat some attacks by disrupting or degrading their efforts. Threat intelligence can also help you detect an incident during the reconnaissance phase, before you have actually been attacked.

One of the main ways in which good threat intelligence can add value to cyber security monitoring is by providing additional context to help the security analyst effectively triage and investigate events to accurately identify genuine positives and understand the true nature and extent of the business risk posed.

Segregating threat data, news and intelligence

Workshop participants agreed that it was important to distinguish the difference between threat data, news and intelligence, when carrying out cyber security monitoring, as shown in the table below.

Threat information type	Examples	Related phase
Threat data	• Suspect IP addresses • Known bad endpoints	FUSION
Threat news	• General awareness (eg. knowing there is a new attack type)	ANALYSIS
Threat intelligence	• Analysis of impact of above on a business • So what if it happens?	ANALYSIS

"Buyer beware – that's news, not intelligence"

A good supplier can help you move beyond 'passive detection monitoring' to include determining how to obtain intelligence, rather than just news about events.

Your organisation should therefore be asking itself:

1. What is the intelligence being provided (and where did it come from)?
2. What does it actually mean to our organisation?
3. What should we do with this intelligence – how do we use it in our organisation?

"Threat intelligence is only as good as the quality, relevance and completeness of the data provided"

Sources of cyber threat intelligence

Workshop participants identified a range of potential sources of cyber security intelligence that can be used to support cyber security monitoring, evaluating the likely criticality and cost of each source.

The results of this analysis are presented in the table below (in descending order of criticality), together with useful comments, where appropriate.

Ref	Name of source	Criticality	Cost	Comments
1	Internal	Essential	Low	
2	CERT services	Essential	Low	Examples include GovCertUK, USCERT, AUSCERT
3	Vendors	Essential	Low	
4	Blacklists/whitelists	Essential	Medium	Phishing
5	Vulnerability feeds	Essential	Medium	
6	Business logic	Essential	High	Internal information
7	Domain/brand monitoring	Essential	Low	
8	Malware	Important	Low – high	Sample DBs
9	Free IOC	Important	Low	
10	Specialist media	Important	Low	Social networks, blogs etc
11	Outsourced honey pots	Important	Medium	
12	Social media	Specialised	Low - medium	
13	Commercial IOC	Specialised	Medium - high	
14	Government	Specialised	Low	Feeds into certs, but also focus on public sector
15	Industry groups	Specialised	Low	Examples include PCI
17	Criminal forums	Specialised	Medium	Dark Web/TOR
17	Academia	Specialised	Low	
18	Insourced honey pots	Specialised	High	



Situational awareness can be improved by using a combination of threat intelligence, data fusion and big data analytics.

Links to cyber security incident response

The cyber security monitoring process is closely linked to cyber security incident response. As can be seen from the simple diagram in ***Figure 8*** below, monitoring activities can highlight events that are then identified as actual (or potential) cyber security events following analysis by a suitably skilled analyst.

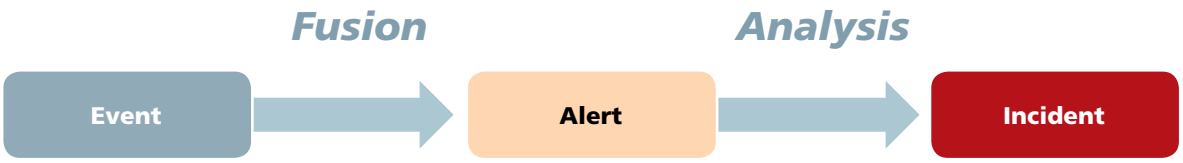


Figure 8: Link to cyber security incident response

Security event reports should be produced for cyber security incidents (particularly those with a high priority), which should cover a range of important details, such as:

- Activity date and time
- External endpoints affected
- Activity details (symptoms of the event)
- Risk (details about a possible attack)

As a result of an earlier research project carried out by Jerakano, CREST has produced a Guide that provides advice and guidance on how to establish an appropriate cyber security incident response ***capability***, enabling you to assess your state of readiness to:

1. *Prepare for a cyber security incident:* performing a criticality assessment; carrying out threat analysis; addressing issues related to people, process, technology and information; and getting the fundamentals in place.

2. *Respond to a cyber security incident:* covering identification of a cyber security incident; investigation of the situation (including triage); taking appropriate action (eg. containing the incident and eradicating it's source); and recovering from a cyber security incident.

3. *Follow up a cyber security incident:* considering your need to investigate the incident more thoroughly; report the incident to relevant stakeholders; carry out a post incident review; build on lessons learned; and update key information, controls and processes.

Copies of all the deliverables from the CREST Cyber Security Incident Response project can be found on the CREST website at: http://www.crest-approved.org

Investigating cyber security events

In the early stages of investigating a cyber security incident, the precise nature of the incident may be unknown and initial analysis will be required. When investigating a cyber security event, the approach taken can be either:

- Intelligence driven, based on information gathered from: government agencies (eg. CPNI), monitoring of internal resources, open source information or data provided internally
- Evidence-driven, based on information gathered from corporate infrastructure or applications (typically event logs).

Investigators will often wish to:

- Examine important alerts or suspicious events in logs or technical security monitoring systems (eg. IDS, IPS, DLP or SIEM)
- Correlate them with network data (including data from cloud service providers)
- Compare these against threat intelligence.

When carrying out an investigation, each possible trigger event should be thoroughly investigated, including:

- Date/time
- Internet protocol (IP) address (internal or external)
- Port (source or destination), domain and file (eg. exe, .dll)
- System (hardware vendor, operating system, applications, purpose, location).

Consequently, it is important that your cyber security monitoring and logging process enables you to provide all the information needed to carry out a fast and effective investigation.



Investigations should often be carried out by expert third party cyber security specialists.

Specialised, experienced and well qualified cyber security incident response experts can help you to work out the specific actions you need to take in response to a cyber security incident in order to mitigate the risk, which may be a mixture of technical and business measures.

Without this step being in place, monitoring can cost you more money than is necessary and deliver little security value.

The need for collaboration

Project research revealed a need for greater collaboration in cyber security monitoring, the main aims of which are to help your organisation, your sector and the government to:

- Proactively respond to cyber security attacks (eg. by closing channels or 'attacking the attacker')
- Close down criminal operations
- Prosecute those responsible for the attack
- Reduce the frequency and impact of future security incidents.

Some of the main challenges organisations face in collaborating about cyber security monitoring and logging are in:

- Dealing with cloud computing and other outsourced suppliers
- Using cyber security intelligence sharing platforms and collaboration forums effectively
- Adopting a common language for communicating.

The UK is one of many governments around the world that recognise the serious nature of the threat that is emerging from cyber-space. Nations of the world are giving high priority to implementing cyber security strategies that will both improve their resilience to cyber security incidents and (where possible) reduce the impact of cyber security attacks.

Fusion cell and the CISP

The UK has set up a cyber security "fusion cell" for cross-sector threat information sharing. The intention is to put government, industry and cyber security analysts side-by-side for the first time. Public and private sector analysts will be joined by members of intelligence agencies, law enforcement and government IT as they exchange information and techniques and monitor cyber security attacks in real time.

The fusion cell is a cyber security attack monitoring operations room at an undisclosed location in London as part of a government cyber security initiative. The Cyber Security Information Sharing Partnership (CISP) also includes a secure web portal and programmes aimed at building cross-sector trust to underpin information sharing. The web portal is based on a social networking structure, giving members of the CISP freedom to choose who they wish to share information with in real time.

Note: This sort of information sharing is typically only available to very large organisations – and should only be considered as part of your armoury for responding to cyber security incidents.

Furthermore, a number of international organisations (eg. ENISA, NIST, ISF and ISACA) work constantly to promote or use collective defences to analyse the latest developments in cyber threats and cybercrime.

One of the roles of the UK National Crime Agency (NCA) - previously called the Serious Organised Crime Agency (SOCA) - is to promote the collaboration between many key bodies to improve the provision of cyber security intelligence and situational awareness generally. This would include helping to build data about the Modus Operandi (MO) of criminals and about attack vulnerabilities.

The NCA also support the three pillars of GovCertUK, which are to:

- Be part of the international *cert* to *cert* network
- Provide incident management and response support
- Improve situational awareness (through the CISP), such as the sharing of IP addresses that are about to attack a network and alerting organisations to large scale malware harvesting.



Both GovCertUK and the NCA help to provide attribution of malicious events.

Overview

To help carry out cyber security monitoring and logging activities, organisations often deploy industry-leading security technology, including the provision of firewalls; malware protection and analysis; network intrusion detection; host-based-protection and SIEMs. This heterogeneous approach to selecting security solutions provides organisations with the best-of-breed technologies and offers improved security by not relying on any single vendor or security platform.

The combination of technologies does, however, present a significant challenge - there is no inherent way to normalise, aggregate, and correlate the security events across technologies. Further, one team may support the firewalls, another may support the network IPS devices, and yet another may support the host-based security tools. This often leads to discrete and incomplete cyber security monitoring, performed using different tools and by different teams.

Piecing together the details of an attack in real-time becomes extremely difficult and even forensic analysis after an attack is slowed by the need to combine event streams. In reality, building and maintaining a strong cyber security posture necessitates a centralised effort to monitor, analyse, and respond to security events across technologies as quickly as possible. To meet this need, more and more organisations are using a Security Operations Centre, which is often outsourced.

A Security Operations Centre (SOC) is where enterprise information systems (web sites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. The SOC is typically dedicated to the detection, investigation and response of log events triggered through cyber security-related correlation logic.

A SOC is an example of a more advanced cyber security monitoring approach. A good SOC needs to go beyond monitoring, and help respond to cyber security events quickly and effectively.

> "A SOC is only the engine; it still needs to support robust processes"

SOCs, NOCs and SNOCs

Project research revealed a shared understanding of Network Operations Centres (NOCs), Security Operations Centres (SOCs) and Security and Network Operations Centres (SNOCs), identifying that a:

- NOC is driven by the need to ensure business critical networks run well and continue to be available (eg. by managing resilience, traffic flow, alternative routing; and monitoring performance, latency, capacity and technical vulnerabilities)
- SOC is a central location where cyber security threats and alerts can be monitored, analysed, investigated using technology and intelligence supported by skilled individuals
- SNOC is a combination of one or more NOCs and SOCs.



Some organisations simply extend their NOC capability to include SOC requirements (creating a Security and Network Operations Centre – or SNOC), However, many of them struggled as they just made the NOC manager responsible for the SOC functionality and they often got lost because a different set of skills and objectives are required.

SOC services

If you decide to use a SOC (either outsourced or developed internally) the services of the SOC should be customised to your threat landscape and data assets to enable a targeted analysis of data based on your organisation's security objectives.

You should also make sure that, where required, your SOC:

- **Accumulates** all relevant traffic entering and leaving your network for a fixed duration
- **Analyses** all captured data, putting it into context using situational awareness - forensically sound capture files can be retained should evidence be required
- **Alerts** you to certain events or trends in real-time by capturing data across multiple capture locations and analysing it in numerous dimensions
- **Reports** evidence of real events and actual incidents, sophisticated attack detection – including infiltration and exfiltration incidents, corporate or third party security policy violations, and specific compliance non-conformities
- **Enables** effective remediation of cyber security incidents
- **Assesses** both the general health and security posture of your organisation at network level as well as the effectiveness of existing cyber security controls.

"A good SOC should not just be a detection centre"

Many major SOC offerings run 24/7 every day of the year, providing a wide range of commercial services. They deliver a 'service wrap' of offerings for their clients, effectively integrating a wide range of technical security services.

People, process, technology and information

Any SOC needs to be supported by the right blend of people, process, technology and information, as outlined in ***Figure 9*** below.

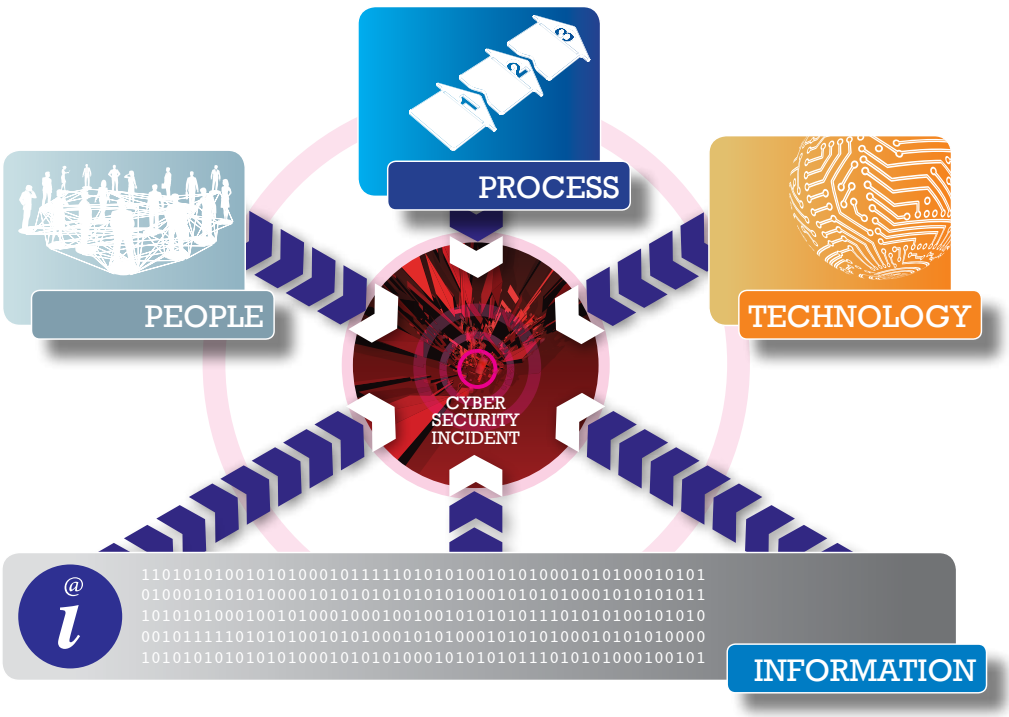


Figure 9: Main considerations for each phase of the cyber security monitoring and logging process

Workshop attendees determined how four different types of individual in the SOC (there can be more roles) would typically use processes, technologies and information to help them carry out their roles effectively. The results of this analysis are presented in the table below, illustrating how various roles (shown in the people column) are supported by processes, technology and information.

People	Process	Technology	Information
Technical delivery manager	• Reporting • Client relations • Collation of information • Compliance	• Reporting • Analytics • Commercial understanding	
First line analysts	• Event filtering • Collation of information • Alert/alarm monitoring • Escalation of alerts/alarms • Ticket management • Initial customer contact	• Log management tools • SIEM tools • Ticketing • Knowledge base • Customer relationship management (CRM) • Configuration management database (CMDB)	• Customer • Asset • Alerts • Alarms • Events
Second line analysts	• Incident assessment • Trend analysis • Root causes analysis • Deep dive investigations • Escalation to third line analysts • Incident lifecycle management • Alarm configuration • Production of metrics • Contact with key assets	• Threat intelligence	• Customer • Asset • Alerts • Alarms • Events • Customer profile • First line evidence
Third line analyst (very technical, incident response)	• Host intrusion analysis • Malware analysis • Network intrusion analysis	• Specialist tools	
SOC Manager	• SOC process • Team management • Production of SOC metrics • Career progression • SOC validation of PPTI • Point of escalation • Capacity management • Compliance	• Ticketing • Reporting • Incident management • HR systems • Tools for metrics	

Security engineers, system administrators and marketing executives are omitted from the SOC analysis because, rather than being an integral part of the SOC itself, these roles sit outside the SOC, supporting it, for example in terms of marketing, pre-sales and infrastructure services.

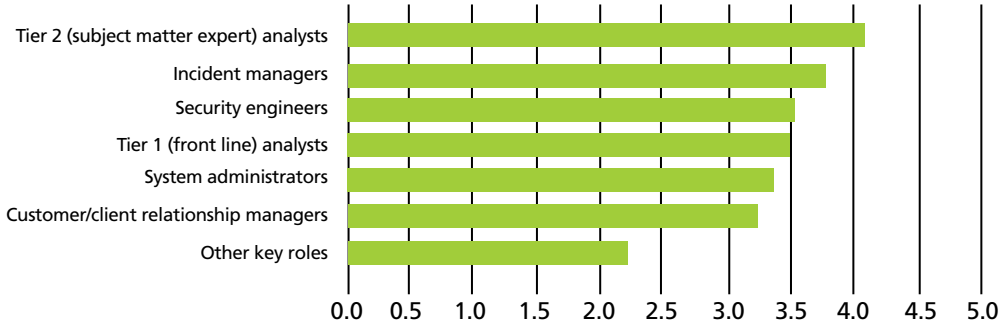
Security engineers are often critical in the delivery of Security Device Management services that are extremely common, particularly amongst MSSPs. Such services take on the ongoing management and maintenance of the security devices that are critical to effective monitoring.

Bringing this into the SOC can be extremely effective since well-maintained security devices can improve both the efficiency and effectiveness of monitoring. Indeed poorly-maintained security devices can significantly reduce the value of any monitoring carried out on the output of those devices.

People

Most respondents placed considerable value on many different types of people being employed by SOCs, as shown in the chart below.

What value would you place on each of the following types of people being employed in Security Operations Centres (SOC)?



There was an extremely high level of requirements for expert analysts (Tier 2) and expert providers concur that good analysts are worth their weight in gold.

Indeed, many expert providers of specialist technical security services agree that the ***People*** component is the most important, backed up by a balanced solution combining all four elements.

"A good analyst can detect the low and slow anomalous events"

Professional SOC qualifications

There are many different professional qualifications available for a range of technical security services, such as penetration testing and cyber security incident response. However, there are few, if any, available for the provision of Security Operations Centres or the analysts they employ.

Analysis of responses to the project survey showed strong support for suppliers of SOC (and NOC) services to be supported by professional qualifications, accreditation and a code of conduct – as outlined by the high average responses shown in the table below (scores are shown as a possible rating of 1 to 5).

Requirement	SOC-related	NOC-related
Holding a professional certification (similar to that used by CREST for the providers of penetration testing and cyber security incident response services)	3.73	3.41
Employing individuals with professional qualifications	3.67	3.26
Being supported by a professional code of conduct (eg. to gain assurance over the quality and integrity of services provided and to administer an independent problem resolution process)	3.52	3.24

In some cases, professional services companies are accredited to particular codes of conduct, but do not use qualified individuals to conduct cyber security monitoring services, so the required quality of cyber security monitoring may not be achieved. In other cases, an individual may be qualified but not work for an accredited organisation, meaning that there are fewer assurances about the protection of confidential information or the overall quality of the service provided - and any complaint may be difficult to resolve.

The optimum combination is shown in the green box in ***Figure 10*** below. This is the only combination that provides you with a tangible level of protection should things go wrong – and also reduces the likelihood of a problem occurring in the first place.

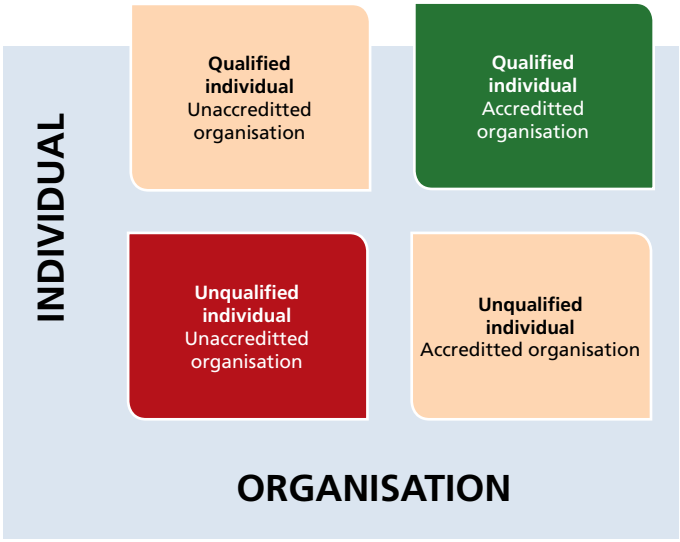


Figure 10: Combinations of accreditation for organisations and the individuals they employ

Project research identified that there are some existing qualifications and learning options available (eg. SANS) that will need to be examined and contextualised.

Higher apprenticeship work is currently being carried out (supported by the UK Government) to develop learning and development pathways that will lead to better skilled and suitably qualified people working in the NOCs and SOCs.

Process

Project research identified that many organisations do not have adequate policies, processes or methodologies (if they have any at all) to help them monitor cyber security-related events effectively. They struggle to know what to do, how to do it, who to contact – and can even compromise investigations by their actions.

SOCs are typically supported by different types of processes for different purposes, such as:

- Operational (eg. call-out, case management, event management, monitoring, staff management, triage)
- Analytical (eg. event analysis, incident response, reporting, research, threat intelligence)
- Business and technological (eg. access management, architecture, compliance, BCP, process improvement, use cases).

Most respondents placed very high value on many different types of processes being employed by SOCs, the top six being:

- Incident response (4.2 out of 5)
- Event correlation and analysis (4.1 out of 5)
- Signatures, rules and analytic development (including incident investigation, malware analysis, maintenance of commercial blacklist and maintenance of intelligence database)
- Situational awareness
- Threat briefing (including passing on of expertise, feedback on threat intelligence provided, two-way information transfer and sharing of investigative resources)
- Quality assurance (including addition of signatures, incident review, incident trend monitoring and correlation of new malware families and analytics).

Much of these can be integrated into an effective event analysis process, such as the one outlined on the following page.

Expert suppliers of cyber security monitoring services can help you develop an appropriate process – or implement their own tailored version.

You should appoint a suitable supplier(s) in advance, who is ready to help at short notice, as required (for example by keeping third parties on a retainer for times of need). Should you suffer a cyber security incident, you will then be able to undertake fully-fledged breach investigation and eradication quickly and effectively.

The event analysis process

Many SOCs use a work flow approach to help them deal with relevant events from various sources. Events are categorised, prioritised and assessed by an assigned analyst according to a defined process, such as the one shown in ***Figure 11*** below.

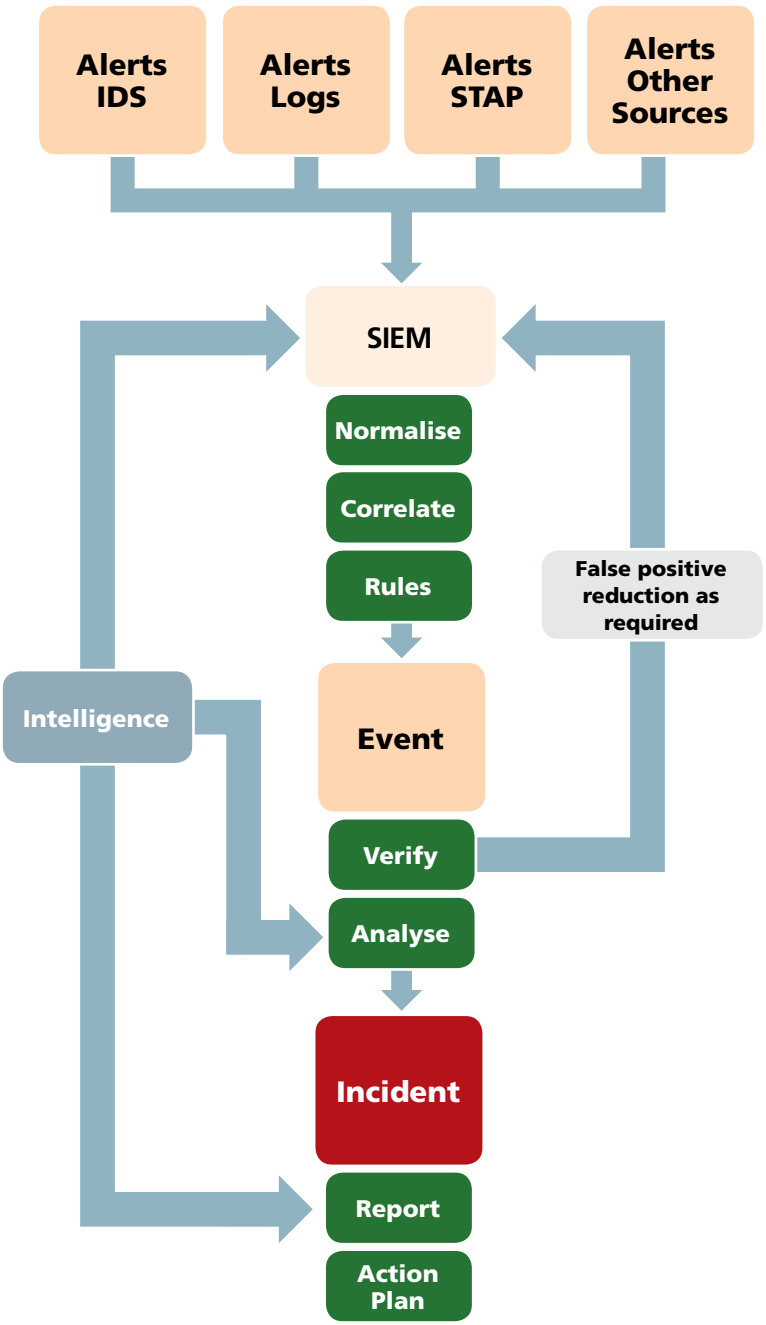


Figure 11: The event analysis process

It is then up to a skilled analyst to find the unusual and anomalous events using tools, processes, intelligence and their own experience and ingenuity.

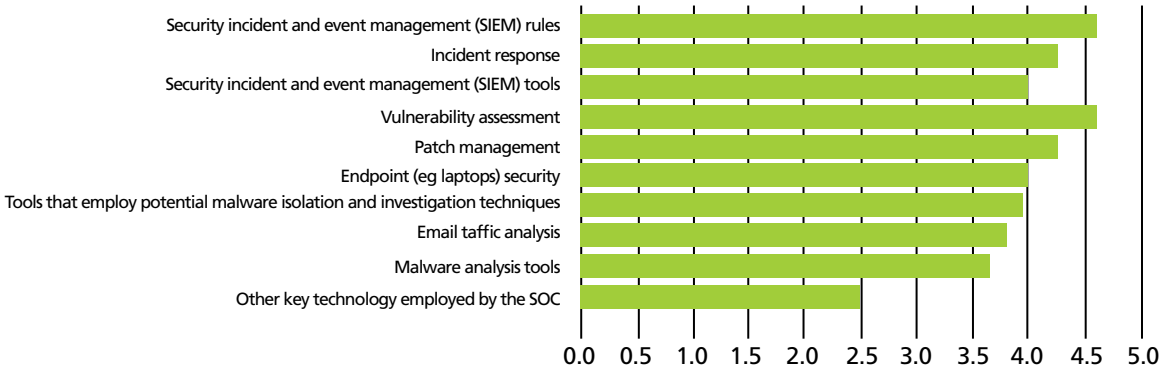
> "You should sometimes let the analysts be hunters to go find anomalies"

Technology

Every SOC will be supported by a range of tools and other technology, typically centred around a good (commercial) SIEM engine.

Most respondents to the Project Survey placed a great deal of value on all aspects of SOC technology as shown in the chart below.

What value would you place on each of the following types of technology being employed in Security Operations Centres (SOC)?



SIEMs were given the highest value of all SOC technologies by respondents to the Project Survey, which is not surprising as they are at the heart of nearly every SOC.

"You can do a lot more with tools that are freely available if you invest more in people, rather than commercial products"

Information

It is essential to make sure that any SOC has the information readily available that will help the cyber security monitoring and logging process.



The amount and type of information required in a SOC will differ based on a number of factors, such as its size, market sector, internal capabilities and nature of the particular cyber security monitoring and logging services provided.

Most respondents to the project survey had a high level of support for many types of information being used in a SOC, with the top five being:

- Source inputs/material, such as vulnerability management; risk assessments; and SIEM monitoring
- Security incident response teams (SIRT)
- Intelligence and analysis (eg. a security risk register; security operations; and threat intelligence)
- Management information (strategic and tactical reports) such as current risk and trends; threat and horizon scanning; operational metrics; and programme status
- Tailor-made internal intelligence data.



Organisations can overlook the need to gain fast access to cyber security-related events at their outsourced service providers (ie. access to premises or equipment). They often have difficulties in getting their third party suppliers (eg. cloud service suppliers, infrastructure outsourcers and managed service providers) to provide important information (eg. event logs) pertaining to cyber security events, sometimes having to wait for several days for something to be actioned.

Cyber security monitoring and logging approaches

Project research evaluated many different ways in which cyber security monitoring and logging can be carried out. The advantages and disadvantages of each approach are shown in the table below.

Approach	Advantages	Disadvantages
Cloud & Appliance based/Software as a Service provider	• Cost • Compliance • Good for small companies • Entry-level • Easy to deploy	• One size does not fit all • Inflexible • Compliance not security centric • Not integrated with in-house processes • No knowledge/context for your environment • Technical driven – will report, but less deep analysis
Shared/MSSP – (Sourced from a Network Service Provider/IT Service Outsourcer)	• All in one service, alongside existing contract • Cost often embedded in existing budget • Cost benefits versus in-house • Ability to provide 24/7 or 'follow the sun' services	• Less core focus on security, second priority to availability/ SLA etc • Conflict of interest • Multi-tenant sharing issues • Security not a core competency for MSSP • Loss of business context
Shared/MSSP – (Sourced from a Managed Security Services Provider)	• Security professionals • 24/7 support and continuity • Integrated solutions and scenarios (eg. incident response)	• Costs can rise due to specialists required • Vendor/solution lock-in • Additional opex costs • Loss of business context and focus • Lack of flexibility versus in-house
Captive outsourced (Hybrid model)	• Retain solution choice • Custom SLAs • Separate solution and service provider choice	• More expensive than MSSP in small environment
In-house/in-sourced service	• Greatest control • Integration with operations • Greater knowledge of business • Choice of software/hardware solutions • Custom SLAs • Less data privacy issues	• Possible efficiency loss • Responsibility for routine upgrades and maintenance of software/hardware • Ongoing requirement to maintain capability and investment • Highest cost (usually) • People/skills/retention • Lack of global 'visibility' • Diverting staff from other tasks

The supplier selection process

If your organisation decides to appoint an external provider of cyber security monitoring and logging services, whatever approach you choose it is important that you appoint a supplier who can most effectively meet your requirements – and at a reasonable cost.

Suppliers of technical security services identified that there are two main types of client for cyber security monitoring and logging services, those that are looking for:

- A 'tick box' solution (often in highly regulated industries), logging the bare minimum needed to meet audit, compliance and regulatory requirements
- Cyber security as they are concerned about security breaches and attacks – and want to be more proactive.

There is often a good deal of overlap between the monitoring required for compliance and that needed to improve cyber security. So by using a provider able to meet both compliance and cyber security requirements, you may be able to achieve cost-effective security through a relatively small uplift to basic compliance expenditure.

This raises many questions that you will need to answer, such as:

- What type of service do I need?
- How much service do I buy?
- Who do I buy it from?
- How much will it cost?
- What do I need to look for from a potential supplier?

Consequently, a systematic, structured process has been developed to help you select a suitable supplier, as shown in *Figure 12* below.

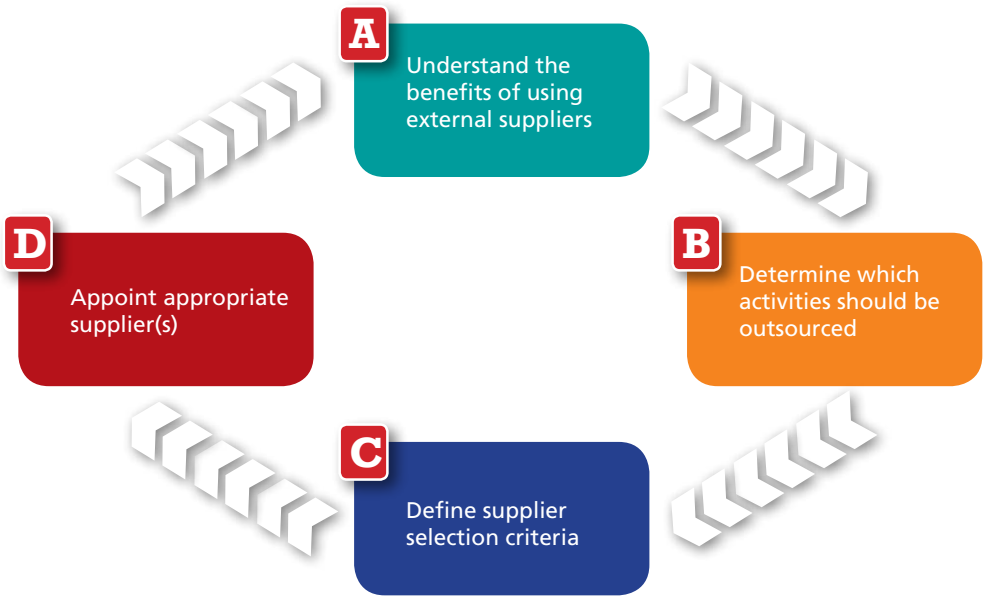


Figure 12: The supplier selection process

Each of these steps is outlined throughout the rest of this chapter.

Each of these four phases is examined in detail in the companion CREST report *Cyber Security Incident Response – Supplier Selection Guide.*

Understand the benefits of using third party experts

There are many reasons why an organisation may wish to employ external cyber security monitoring and logging providers, such as to help carry out activities outlined in previous chapters.

Most respondents to the Project Survey placed a high value on the many differing benefits of outsourcing cyber security monitoring and logging services, which included:

- 24 x 7 x 365 coverage
- Cost advantages over developing your own solution (eg. because of leveraging, personnel, tools and approaches)
- Access to cyber security monitoring and logging specialists
- Cyber security (protective) monitoring
- Access to 'surge support' (swift deployment of experienced coordination)
- Fast provision of an effective cyber security monitoring capability.

Other factors that were also well supported included: lower risk delivery of services; independent view of risk; quick and easy, low-risk compliance; and SLAs with service credits.



You should procure cyber security monitoring and logging services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals. CREST member companies are independently assessed and can provide you with a certified, trusted relationship, backed by an effective industry body.

Outsourcing challenges

Whilst there are many benefits associated with outsourcing cyber security monitoring and logging services, there are also a number of challenges to address. Project research identified a number of challenges associated with the provision of appropriate cyber security monitoring and logging services which included:

- Significant variations in the (type and quality of) provision of services
- Lack of clarity about what is actually being offered
- The proliferation of 'specialist' (often proprietary) tools and their lack of integration
- Insufficient links (in a number of cases) to cyber security incident response services
- No related standard or qualification for their provision
- No standard generic for assessing knowledge, skill and competence of service providers, particularly SOC and Cloud-based solutions
- No codes of conduct for M&L service providers
- Vendor hype.

Respondents to the Project Survey were asked about the extent to which they consider a range of topics prior to outsourcing activities or services to external cyber security monitoring and logging providers. Most respondents fully consider a wide range of important topics which could cause problems when outsourcing, which were:

1. Loss of control of your data (particularly sensitive data)
2. Gaining access to your own data stored by outsourcers
3. Level of support in responding to a cyber security incident
4. Reduced access to business context information
5. Location of analysts and how they can be contacted.



Concerns over these types of issue were typically more highly rated than the benefits of outsourcing. However, if these types of issues are handled effectively then the outsourcing of some or all cyber security monitoring and logging services should make good business sense.

"You need to provide great clarity around requirements before outsourcing – but if you are going to outsource, then do it properly"

Technical considerations

The type and quality of products and services in the cyber security and monitoring arena varies enormously. Consequently, clients are often:

- Bewildered by what is actually being offered and what they will be delivered
- Unsure of how to differentiate the quality and type of services on offer
- Saddled with unsuitable (sometimes expensive) services
- Over-reliant on product-led solutions that they do not fully understand or optimise.

One of the possible reasons for this situation is that a large part of cyber security budget is often technology-led with security dollars being owned by technology vendors, rather than by suppliers of security services.

"Cyber security monitoring is not just about having the latest technology box"

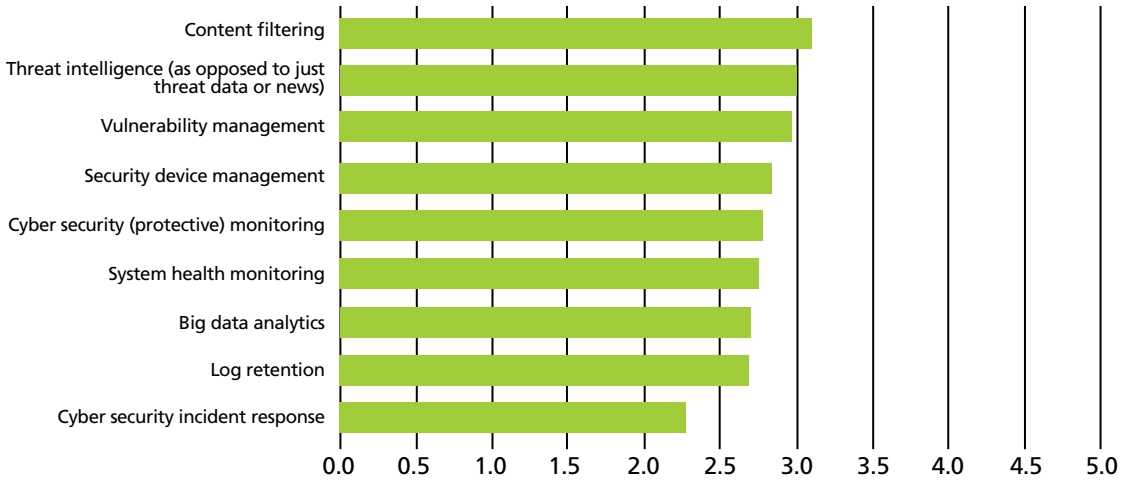
Many providers of cyber security services offer turn-key solutions, yet the best value is typically for a client to develop deeper relationships with their suppliers - thinking of them as a force multiplier, rather than just an outsourcer. Even at a more detailed level, technical security services need to be more integrated, ensuring the smooth inter-relationships between components like triage, forensics and root cause analysis.

Determine what activities should be outsourced

Once you have reviewed your requirements for cyber security monitoring and logging, you should now determine the types of service you require and which of these services you will consider outsourcing to expert suppliers.

Many respondents to the Project Survey were willing – to an extent - to consider outsourcing a range of cyber security monitoring activities, as shown in the chart below.

To what extent would you consider outsourcing the following to providers of cyber secuity monitoring and logging services?



Most organisations need professional help in carrying out cyber security monitoring and logging activities in an effective manner. However, it is very difficult for them to identify trusted organisations that have access to competent, qualified experts who can respond appropriately whilst protecting sensitive corporate and attack information.



There can sometimes be a dichotomy between what information an outsourced service provider should disclose (eg. to support a forensic investigation) and what a buyer should be able to have access to (RFP; SLA clauses; cloud services).

Types of service available

The main services offered by third parties in the cyber security monitoring and logging arena include:

- Protective monitoring (often delivered in real-time from their SOC)
- Advanced threat detection (using tools and techniques to provide threat intelligence and monitor all connections between devices on an organisation's network and the Internet)
- Security device management.



Many other complementary services can be offered by a number of suppliers, such as risk assessment, penetration testing, incident response, malware analysis and remediation services.

For each of these services there are different ways you can pay for them – all of which should be evaluated and then negotiated - which include being charged by one or a combination of:

- Devices per hour
- Events per second (EPS)
- Logging capability.



Many reputable suppliers will help you select the most appropriate method of payment, typically saving you money.

Define supplier selection criteria

You should now be in a position to define your supplier selection criteria, based on topics covered earlier in the chapter.

When defining supplier selection criteria, you should consider findings from project research which identified that a reputable supplier will:

- Understand and meet your outsourcing requirements
- Have a clear, shared understanding of the scope of the services being discovered, for example in terms of skills, approach and output
- Develop a suitable approach to tackle your specific cyber security monitoring and logging requirements, backed up by a consistent and repeatable response process
- Help you initiate an effective remediation and improvement programme.

They will also be able to provide experts in cyber security monitoring and logging who:

- Have the necessary qualifications/ability (eg. security clearances) to work within relevant environments, both at your premises and at those of your relevant suppliers or partners
- Maintain an up-to-date, relevant understanding of your business and technical environment (which may be sector specific)
- Have experience in dealing with the types of cyber security events you wish to monitor
- Conduct the investigation and response in a fast, effective and professional manner
- Can bring in additional cyber specialisms if required
- Collaborate with relevant third parties, such as law enforcement, CERTs and the Government.



Senior management in many client organisations do not appreciate the cost, resources or rationale required to adequately monitor the complete cyber security picture. They do not realise that an on-going cyber security monitoring cycle is required to help learn about attackers and make it more difficult for them to carry out a cyber security attack.

A good supplier will not only provide SIEM solutions, but go beyond the standard offerings providing services based both on 'rules' and on data analytics. They then develop 'attack trees', which they use as models to:

- Understand the nature of the threats to clients
- Identify trends behind the rules
- Map the threats to analytics.

Appoint selected supplier(s)

The final step is to appoint and monitor your selected supplier(s). They should be able to manage cyber security-related event logs effectively, implement a suitable cyber security monitoring process and use appropriate tools for the target environment.



There may be other considerations when selecting a supplier. For example, your organisation may have a well-established (or preferential) relationship with a particular supplier or a need to appoint (or reject) an organisation for commercial or political reasons.

You should take into account the need to differentiate between:

- Quality, tailored and integrated services;
- Middle of the road (but often fit for purpose) offerings; and
- Suppliers who are really just providing the bare minimum or adopting a 'tick in the box' mentality.

You can then use your outsourcing requirements to help you determine more specifically what you will require from your supplier. Findings from the project workshop revealed that what you really need to look for is a ***reputable*** commercial supplier who you can ***trust***.

Benefits of using CREST members

What organisations often need is the ability to access demonstrably skilled, knowledgeable and competent individuals working for organisations that have been independently assessed against best practice and who have the policies, processes and procedures in place to monitor all relevant events whilst protecting confidential information.

Many CREST members are well placed to meet these – and other – requirements. By appointing one of these CREST organisations you can rest assured that you are procuring cyber security monitoring and logging services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals.

Respondents to the Project Survey placed extremely high value on a range of cyber security monitoring activities offered by CREST members, with the top six being that they:

- Are up-to-date with the latest cyber threats, adversaries, techniques and countermeasures
- Respond to cyber security incidents in a fast, effective manner
- Provide a high (and assured) baseline standard in terms of both skills and processes
- Adhere to processes and procedures that are subject to regular reassessment
- Offer fast provision of an effective cyber security monitoring capability
- Help organisations to achieve compliance with legal, regulatory, corporate or government standards, managing both business constraints and risks.

Make the appointment

After carefully considering all the relevant supplier selection criteria – and evaluating potential suppliers - you will then need to formally appoint one or more suppliers. The key consideration should still be to appoint a supplier who can help you meet your specific requirements – at the right price - not just one who can offer a variety of often impressive products and services, some of which may not necessarily be relevant to your organisation.

Summary of key findings

This Guide has brought together all aspects of cyber security monitoring and logging in one place, highlighting what is typically ***best practice*** for each main component. It explains how your organisation can:

- Capture and correlate the most relevant cyber security-related events in the right logs – overcoming the wide range of log management challenges
- Introduce a suitable cyber security monitoring process, helping to identify and analyse indicators of compromise (which may be caused by potential or actual cyber security incidents); and respond to anomalous cyber security events quickly and effectively
- Build an appropriate cyber security monitoring and logging capability, considering the benefits of using a Security Operations Centre (SOC)
- Find the right cyber security monitoring and logging tools, processes and people to help you easily, effectively and at the right price.

Implementing a cyber security monitoring and logging capability

This Guide will have given you a good understanding of the most important elements of cyber security monitoring and logging, highlighting the main challenges and describing ways in which they can be overcome.

However, building, reviewing or improving your own cyber security monitoring and logging capability in practice is not easy. Consequently, a seven stage process has been deigned to help you do this more effectively. The overall process is outlined in *Figure 13* below and then each step is described in more detail in the remainder of this chapter.



Figure 13: Implementing a cyber security incident management capability in practice

1. Develop a cyber security monitoring and logging plan

Before wading straight in and trying to build your cyber security monitoring and logging capability, you should first develop a plan. This will help you to design the capability more effectively, gain senior management support and produce a solution that is more likely to be implemented as you would like.

> "A careful, realistic and well thought through plan can be worth its weight in gold"

The first step is typically to create an outline plan, based on the design of cyber security monitoring and logging capability that you have in mind. This plan should define requirements, identifying what the broad budget, resourcing and approach will be. Once you have gained authorisation for this approach you can then produce a more detailed plan.

To help you design an appropriate cyber security monitoring and logging capability you should review a range of relevant material, including the contents of this Guide, and consult with key stakeholders, such as IT management, key business owners and group departments.

Workshop attendees defined what a perfect scenario would look like for cyber security monitoring and logging, which can be broken down into four main categories, as outlined in the table below.

Approach	Advantages
Clear purpose	• Setting clear goals – knowing want you want to achieve • Identifying the benefits of cyber security monitoring and logging • Knowing your own organisation / environment.
Risk-driven, process-based approach	• Taking a risk assessment driven approach to cyber security monitoring and logging • Cyber security risk intelligence and actual incidents linked back to risk assessments • Assessments based on business processes • Adopting a simple process-driven approach • Solid cyber security monitoring and logging baseline foundation.
More focused threat analysis	• Tools to deal with logs cleanly • Understanding normal system/network behaviour • Timely access to threat source data • Integrated, useable threat data/news/intelligence • Good KPIs that can produce meaningful ROI data.
Better resourcing	• Investment in people skills • Integral part of SLA (both internal and external) • Dedicated, longer term time/resources for building partnerships with providers of cyber security monitoring and logging services.

Whilst you may not reach utopia in your own organisation, many of the elements outlined above are achievable in practice. You should review these elements, identify which ones are most relevant to your organisation and create a plan for incorporating them into your own cyber security monitoring and logging capability,

2. Carry out prerequisites for cyber security monitoring and logging

This Guide has identified a number of initial steps (prerequisites) that you should take before you can build an ***effective*** appropriate cyber security monitoring and logging capability. These prerequisites include:

- Agreeing objectives and scope
- Defining primary or critical assets – and determining where they are within the organisation
- Identifying external cyber (eg. internet) 'touch points'
- Determining what possible cyber security attacks on critical assets might look like
- Minimising attack paths to these assets
- Addressing key technical controls on the perimeter – and reducing the attack surface
- Reviewing and revising cyber security (and other) controls currently in place in this area.

It is important that you carry out these prerequisites in a diligent manner prior to building your cyber security monitoring and logging capability.

3. Identify sources of potential indicators of compromise

In many organisations, thousands of possible signs of cyber security incidents may occur each day, recorded mainly by logging and computer security software, but it can be difficult to determine which ones are most important to you – and to separate 'signal' from 'noise'.

There are many different sources of information relating to IOCs, which include:

- Security software (eg. IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software) and monitoring services (often provided by a third party)
- Tools that employ potential malware isolation and investigation techniques (eg. sandboxing or virtual execution engines)
- Logs (eg. operating system logs, service and application logs, network device logs and network flows)
- Publicly available information (eg. information on new exploits, third party organisations, governments)
- People from within your organisation
- Third parties (eg. customers, suppliers, IT providers, ISPs, partner and government bodies).



Dependent on the requirements you defined, you need to identify the most relevant and important sources of information for indicators of compromise to support your cyber security monitoring and logging capability.

Do not just consider internal logs - you also need to analyse:

- External logs (eg. Cloud, MSSP)
- 'Big Data'
- Threat intelligence (eg. reconnaissance data; suspicious threat agent activity; analysis of impact).

4. Design your cyber security monitoring and logging capability

Once the perquisites have been completed, and you have identified relevant sources of indicators of compromise, you can now design your overall cyber security monitoring and logging capability.

To implement an effective capability you will need to consider many aspects of:

- People – particularly skilled analysts
- Process – such as the cyber security event analysis and incident response processes
- Technology – typically centred around a well-tuned SIEM, supplemented by a range of log management and event analysis tools
- Information – particularly reliable, insightful and up-to-date cyber security intelligence.

At the heart of any capability are four key phases, which are required to carry out an effective cyber security monitoring process on a continuous basis, as shown in ***Figure 14*** below. This process should be supported by various types of cyber security intelligence to bring context to the events.

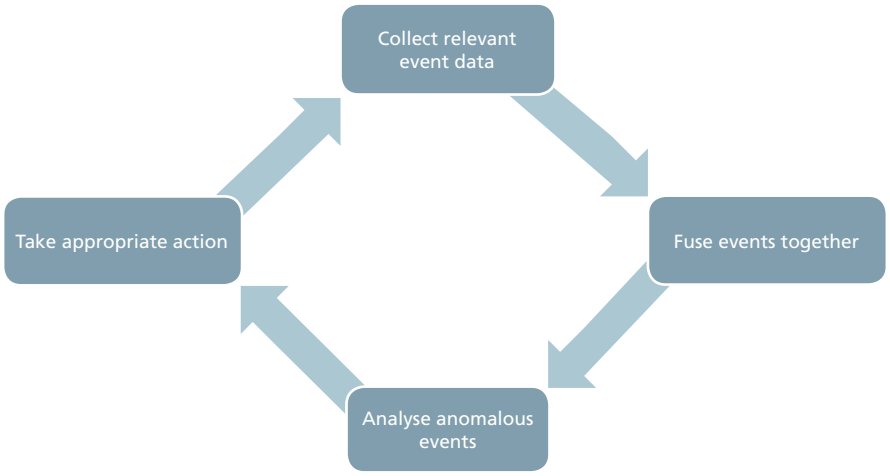


Figure 14: Cyber security monitoring – key components

Without situational awareness, it can be very difficult to identify potential indicators of compromise, particularly during the early (eg. reconnaissance) phase of a sophisticated cyber security attack.

5. Build or buy cyber security monitoring and logging services

Having designed your cyber security monitoring and logging capability, you will now need to determine how to run it in an effective manner, but at a reasonable cost. A good cyber security monitoring and logging capability will be supported by a range of different tools and services, most of which you can either build yourself and/or buy from third parties.

More and more organisations are now choosing to use a Security Operations Centre (SOC), with many of them outsourcing their SOCs to specialised third parties.

Project research identified many different ways in which cyber security monitoring and logging services can be provided (evaluating their advantages and disadvantages), which include:

- In-house/in-sourced service
- Cloud & appliance based/Software as a Service provider
- Shared/MSSP – either sourced from a Network Service Provider/IT Service Outsourcer or a Managed Security Services Provider (MSSP)
- Captive outsourced (hybrid model)
- A combination of the above.

Most respondents to the Project Survey placed a high value on the many differing benefits of outsourcing cyber security monitoring and logging services, which included:

- 24 x 7 x 365 coverage
- Cost advantages over developing your own solution (eg. because of leveraging, personnel, tools and approaches)
- Access to cyber security monitoring and logging specialists
- Cyber security (protective) monitoring
- Access to 'surge support' (swift deployment of experienced coordination)

If you choose to outsource some or all of your cyber security monitoring and logging services, a systematic, structured process has been developed to help you select suitable suppliers (described in Part 6 of this Guide), as shown in *Figure 15* below.

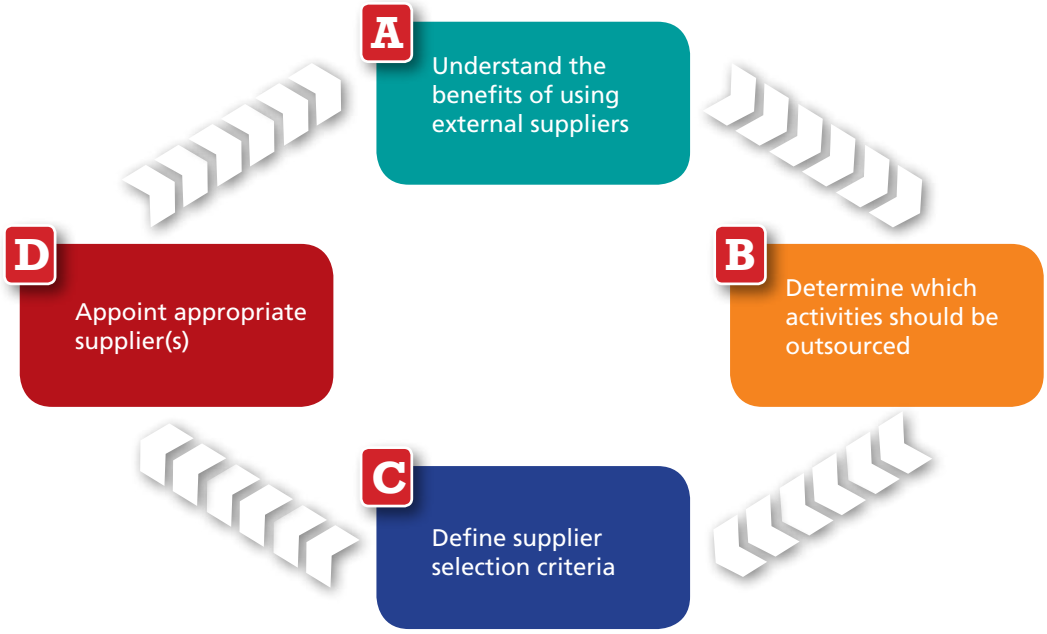


Figure 15: The supplier selection process

You should procure cyber security monitoring and logging services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals. CREST member companies are independently assessed, providing a certified, trusted relationship, backed by an effective industry body.

6. Integrate the capability into your cyber security framework

This Guide has shown how you can design and implement a suitable cyber security monitoring capability, which needs to be supported by a range of cyber security event data from myriad system logs - and informed by different sources of cyber security intelligence. Whilst this capability will help you identify and respond to indicators of compromise in an effective manner, project research has revealed that this should still only be part of a wider cyber security framework.

The types of thing that you will need to consider in your own cyber security framework are shown in ***Figure 16*** below.

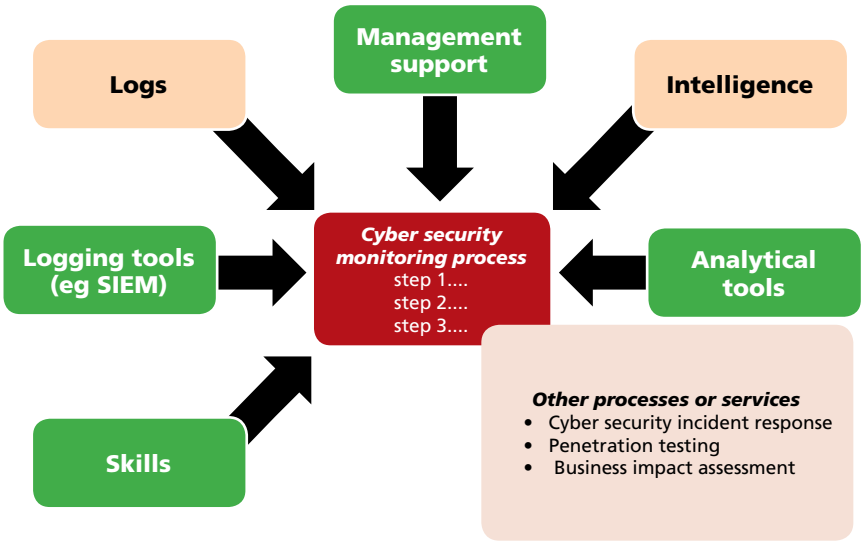


Figure 16: Cyber security framework

Both clients and suppliers can put too much focus on products, rather than using them to support processes, such as intrusion monitoring, asset management, incident response and business continuity. For example, before buying a SIEM product, steps should be taken to understand all the surrounding processes it needs to support.

"Even the best cyber security monitoring and logging is not a panacea for all ills – it will still need to be supplemented by a complete cyber security framework"

7. Maintain the cyber security monitoring and logging capability

Once operational it is important that you maintain your cyber security monitoring and logging capability, ensuring that it continues to meet requirements.

An independent review or audit of your cyber security monitoring and logging capability will help you build on strengths and address weaknesses.

It can be useful for your organisation to understand what the experts are likely to be doing in the future when it comes to cyber security monitoring and logging, so it is always a good idea to keep an eye on developments.

To give you a flavour, workshop attendees identified their main focus areas for the future in terms of cyber security monitoring and logging. Analysis of their number one focus areas for 2015 indicates that they have four main types, as shown in the table below:

Focus area	Activities
Log management	• Ensuring companies are logging cyber incidents and that the logs are configured correctly and of good quality • Looking beyond existing compliance regimes (not just logging, but logging the right things) • Analysis of logs • Integrating new techniques/tools.
Incident response	• Bringing the attacker mind-set into the realms of defending from an attack • Use of new technologies in compromise activity • Encouraging best practice in incident response • Reaction times and methods.
Cyber security intelligence and situational awareness	• Utilisation of information gathered • Managing security assessments beyond SIEM • Developments of SOCs, particularly to be used as a glorified SIEM tool • Incorporating cyber threat intelligence into monitoring • True situational awareness.
The customer experience	• Bespoke solutions for customer analytics – education/how best to deploy solutions • Assessment of value • Risk based reporting and metrics; • Interpretation simplification to clients (ie. make reports easy to understand/less technical) • Maturity of managed security services and bringing value to customers, particularly around reporting.

Conclusion

Organisations seldom have an adequate cyber security and monitoring capability. They often suffer from a lack of budget, resources, technology or recognition of the type and magnitude of the problem.

Whilst you are unlikely to achieve utopia in cyber security monitoring and logging, you can build a more effective cyber security and monitoring capability. To achieve this you will need to:

- Identify and investigate anomalies in cyber security-related events
- Recognise that detail is important
- Prioritise your cyber security and monitoring and logging activities
- Correlate suspicious events with cyber security intelligence
- Consider building or a buying a Security Operations Centre as this appears to be one of the main ways forward to support cyber security monitoring and logging effectively
- Seek the right kind of help from expert external suppliers for carefully selected activities
- Keep an eye on future requirements.



What organisations often need is the ability to access demonstrably skilled, knowledgeable and competent individuals working for organisations that have been independently assessed against best practice and who have the policies, processes and procedures in place to monitor all relevant events whilst protecting confidential information.

Many CREST members are well placed to meet these, and other, requirements. By appointing one of these CREST organisations you can rest assured that you are procuring cyber security monitoring and logging services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals.

The quadrants in this diagram outline the four main areas that deliver the benefits of the CREST vision

CREST is a not-for-profit organisation that represents the technical information security industry, particularly penetration testing, cyber security incident response and security architecture services.

CREST offers public and private sector organisations a level of assurance that the technical security advisors they appoint are competent, qualified and professional with current knowledge. It also ensures that the companies they engage with have the appropriate processes and controls in place to protect sensitive client-based information.

For further information contact CREST at **http://www.crest-approved.org**



Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG

T: 0845 686 5542
E: admin@crest-approved.org
W: www.crest-approved.org