Introduction

SECURITY INFORMATION AND EVENT MANAGEMENT (**SIEM**)

Agenda

SIM

SEM

SIEM

Best Practices

Examples of tools

Security information and event management

What is SIEM?

- Security information and event management (SIEM) was coined by Amrit Williams in 2005
- The basic technologies are:
  - SIM (Security information management) focuses on log collection & report generation
  - SEM (Security event manager) analyses events using event correlations and alert mechanisms
- Together SIEM provides network security intelligence and in real-time (systems, network, apps)

Comparison

	Security Information Management (SIM)	Security Event Management (SEM)	Security Information and Event Management (SIEM)
Overview	Collection and analysis of security-related data from computer logs.	Real-time threat analysis, visualization and incident response.	SIEM, as the name suggests, combines SIM and SEM capabilities.
Features	Easy to deploy, strong log management capabilities.	More complex to deploy, superior at real-time monitoring.	More complex to deploy, complete functionality.
Example Tools	OSSIM	NetIQ Sentinel	SolarWinds Log & Event Manager, Splunk

What is SIEM

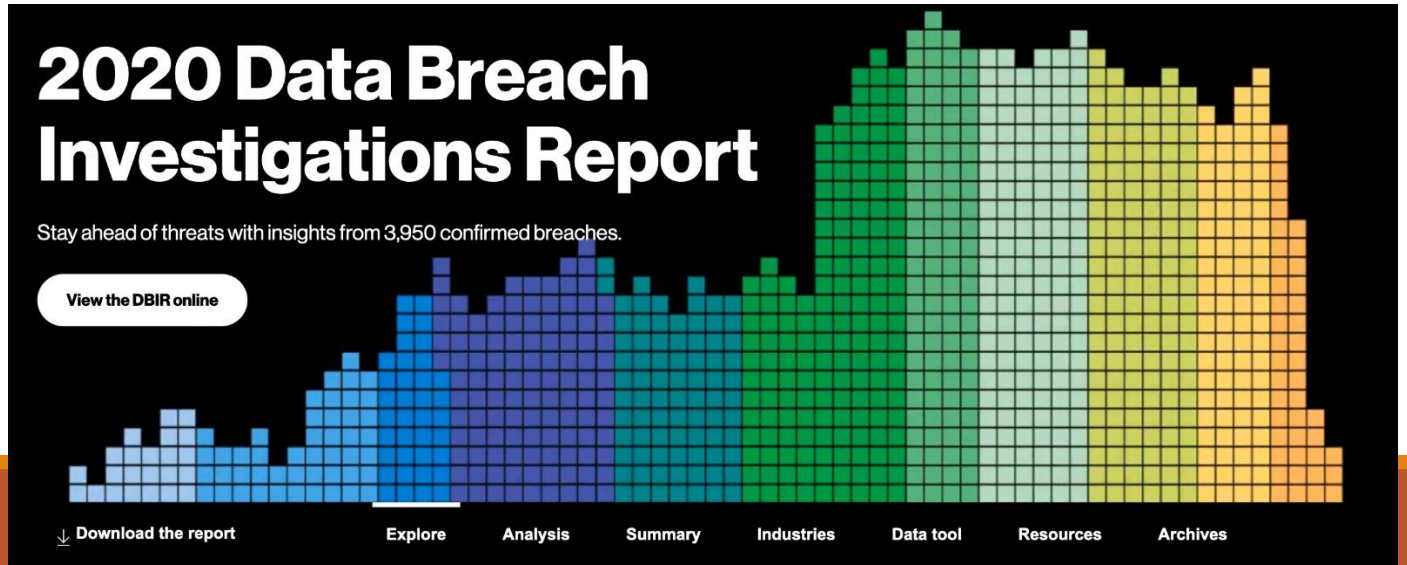
Security Information and Event Management (SIEM) system is generally thought of as providing the following collection of services:

- Log management
- IT regulatory compliance : build filters or rules and timers to audit (monitor against a standard) and validate compliance, or to identify violations of compliance requirements imposed upon the organization.
- Event correlation
- Active response
- Endpoint security (example: monitor whether the firewall on a PC or server is running, when the AV definitions were last updated, when a node becomes infected with spyware, etc.)

Why is SIEM needed?

Using situational awareness:

- Risk in Data breaches increasing for internal/external threats
- Attackers adaptive and often innovative or persistent
- Mitigate/detect attacks
- Manage increasing volume of attacks, logs, and log sources
- Meet compliance requirements



Verizon Data Breach Investigations Report 2020

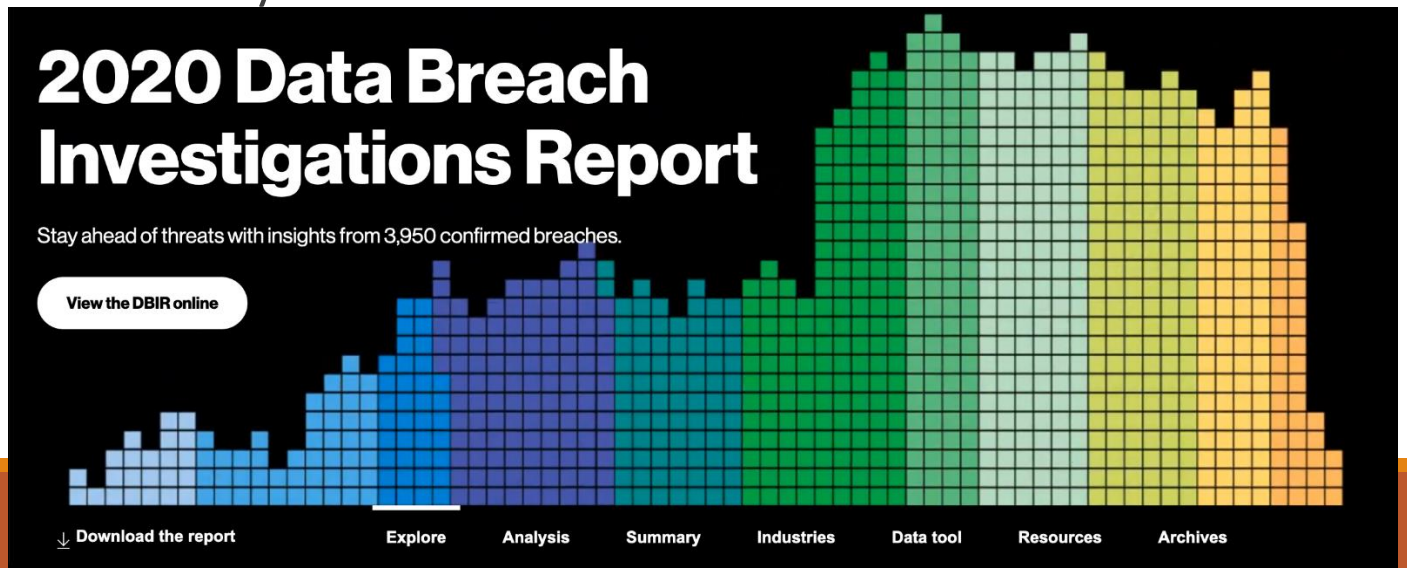
* nearly half (45%) of the breaches featured Hacking

* 86% of breaches are financially motivated

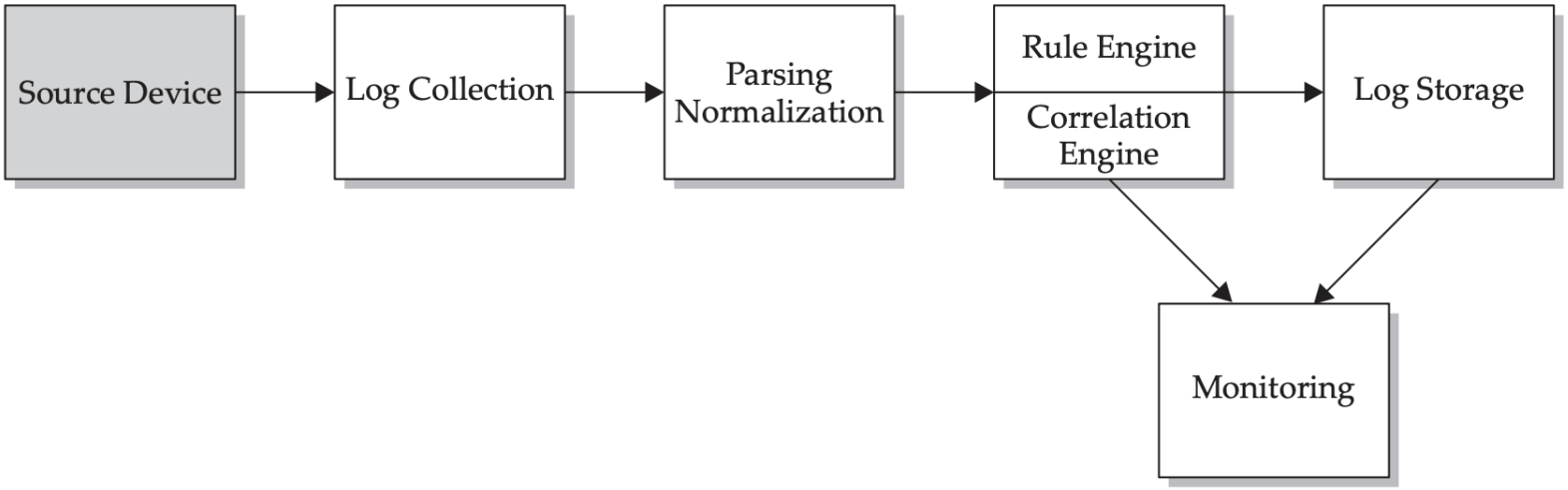
* near the half (43%) of the breaches involved Web Applications

* 37% of breaches stole or used credentials

* breaches where misconfiguration was leveraged have increased by 4.9% from last year



Anatomy of a SIEM



Anatomy of a SIEM (cont)

- A *source device* is the device, application, or some other type of data that you want to retrieve logs from. The source device is not an actual part of the SIEM but it is a vital piece of the overall SIEM process.

- Log collection is to get all the different logs from their native devices to the SIEM.

- Parsing normalization is to reformat the logs into a single standard format that is usable by the SIEM

- The rule engine expands upon the normalization of events from different sources in order to trigger alerts within the SIEM due to specific conditions in these logs.

- The correlation engine is a subset of the rule engine. What the correlation engine does is to match multiple standard events from different sources into a single correlated event.

- Log storage is to store them for retention purposes and historical queries.

- Monitoring allows to interact with the data stored in SIEM

How to choose a SIEM solution

8 things to consider

1. Log collection
2. Activity Monitoring
3. Real-Time event correlation
4. Log retention
5. IT Compliance Reports (OT not covered in this module)
6. File integrity Monitoring
7. Log Forensics
8. Dashboards

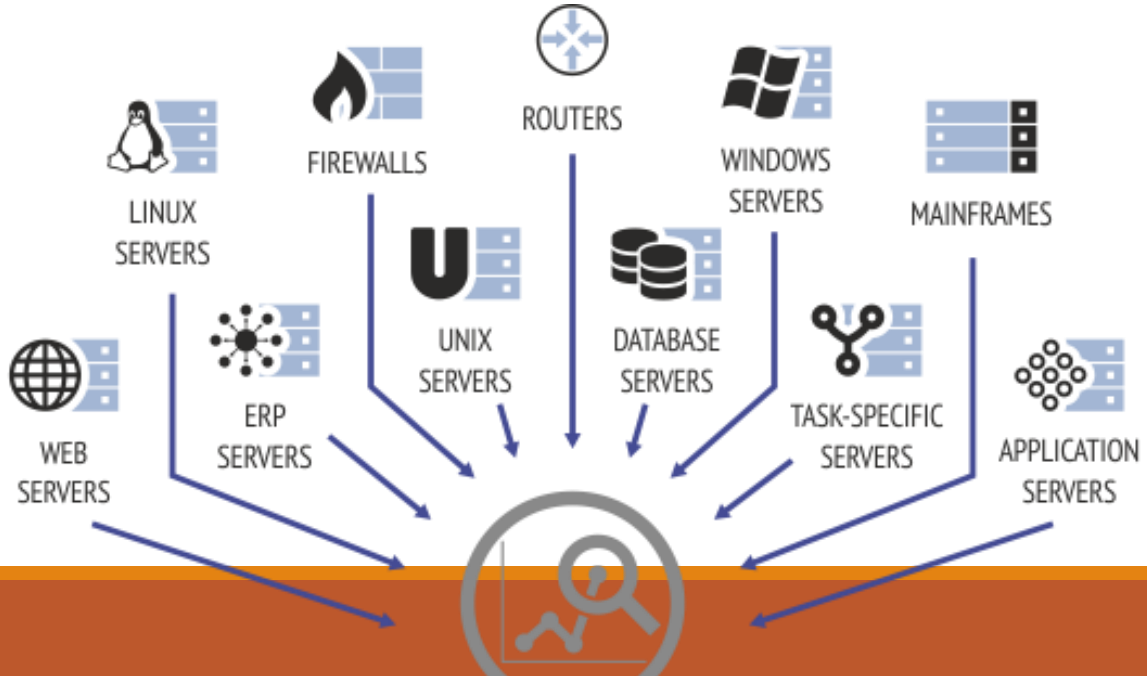
1. Log collection

There are universal log collection & log collection protocols

Tend to be centralized (but who knows for the future)

Collection needs to be secure and to secure storage

Event collection rate (per second EPS, shorter, or longer)



2. User Activity Monitor

Can monitor user activity (legit or malicious)

SIEM Solutions normally have Out-of-the-box user activity monitoring

- In-the-box monitoring increases chances of tampering (internal threat)

Privilege user monitoring and audit (PUMA) another feature

This is to ensure a “Complete audit trail”

1. Which user preformed …
2. What action on
3. What device/server/device,
4. Where the action was triggered and
5. When the action was triggered



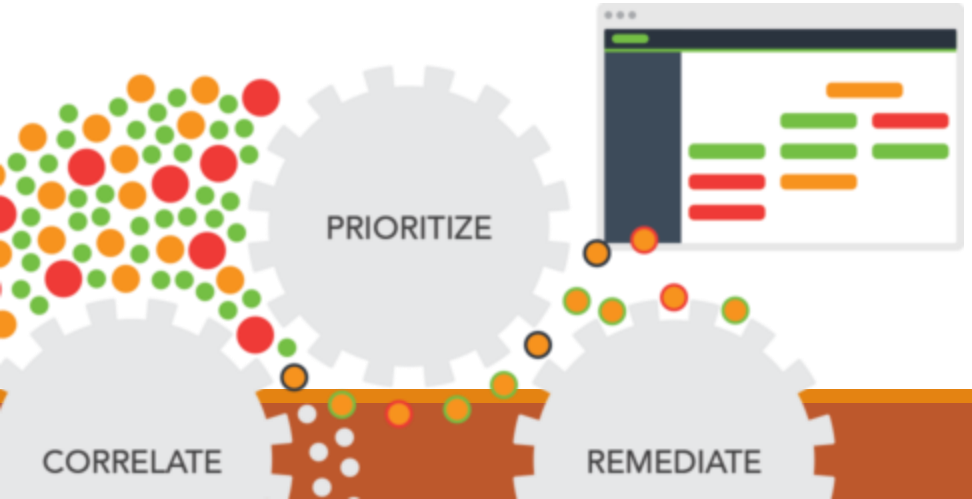
3. Real-Time Event Correlation

Real-time event correlation helps prioritize and remediate threats

- Correlation boosts network security by processing millions of events simultaneously to detect certain behaviours

Correlation can be based on log search, rules, and alerts

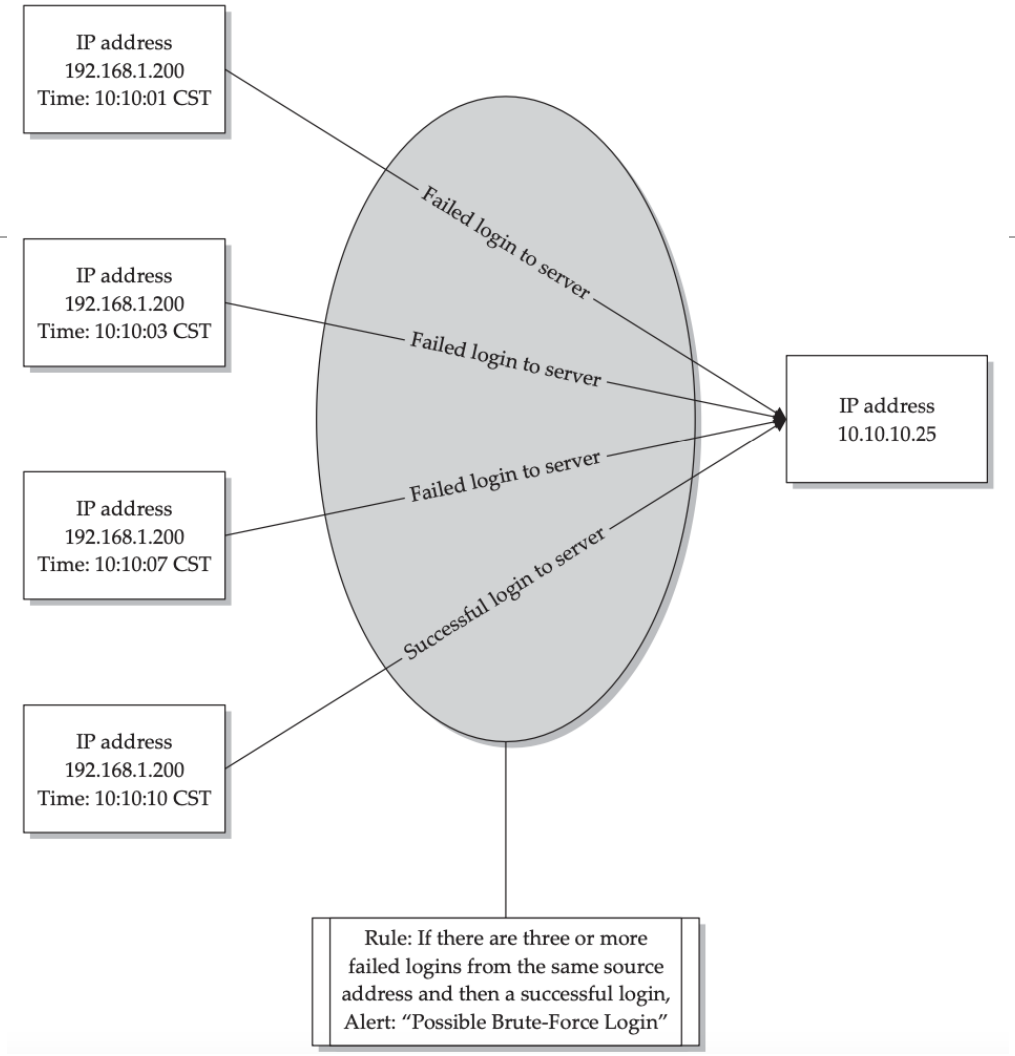
- Predefined rules and alerts good first step, but not sufficient
- Customer rule and alert builder better (IDS/IPS)



Want something fast, accurate, and easy to use

Example

Time	Event Number	Source	Destination	Event
10:10:01 CST	1035	192.168.1.200	10.10.10.25	Failed login to server
10:10:02 CST	1036	192.168.1.90	10.10.10.21	Successful login to server
10:10:03 CST	1037	192.168.1.200	10.10.10.25	Failed login to server
10:10:04 CST	1038	192.168.1.91	10.10.10.35	Failed login to server
10:10:05 CST	1039	192.168.1.10	10.10.10.2	Successful login to server
10:10:06 CST	1040	192.168.1.10	10.10.10.3	Successful login to server
10:10:07 CST	1041	192.168.1.200	10.10.10.25	Failed login to server
10:10:08 CST	1042	10.10.10.54	192.168.1.201	Failed login to server
10:10:09 CST	1043	10.10.10.34	192.168.1.10	Failed login to server
10:10:10 CST	1045	192.168.1.200	10.10.10.25	Successful login to server


IP address
192.168.1.200
Time: 10:10:01 CST
IP address
192.168.1.200
Time: 10:10:03 CST
IP address
192.168.1.200
Time: 10:10:07 CST
IP address
192.168.1.200
Time: 10:10:10 CST
Failed login to server
Failed login to server
Failed login to server
Successful login to server
IP address
10.10.10.25
Rule: If there are three or more failed logins from the same source address and then a successful login, Alert: "Possible Brute-Force Login"

4. Log Retention

- SIEM Solution should automatically archive log data from system
- Repositories tend to be centralised
- Process should be “tamper proof” with encryption and time stamps as a minimum to comply with regulations and forensics purposes
- Valid users need easier retrieving/analysing data tools



5. Compliance Reports

Focus of this module is on IT

IT compliance is the core of every SIEM solution

Ensure that the SIEM solutions has regulatory compliance reports such as PCI DSS, FISMA, GLBA, SOX, HIPAA, etc.

SIEM solutions should be flexible enough to build new compliance records when new future regulatory acts appear



6. File Integrity Monitoring

File integrity monitoring helps security professionals watch files/folders
Things to track files and folders (and more):

1. Created
2. Accessed
3. Viewed
4. Deleted
5. Modified
6. Renamed



7. Log forensics

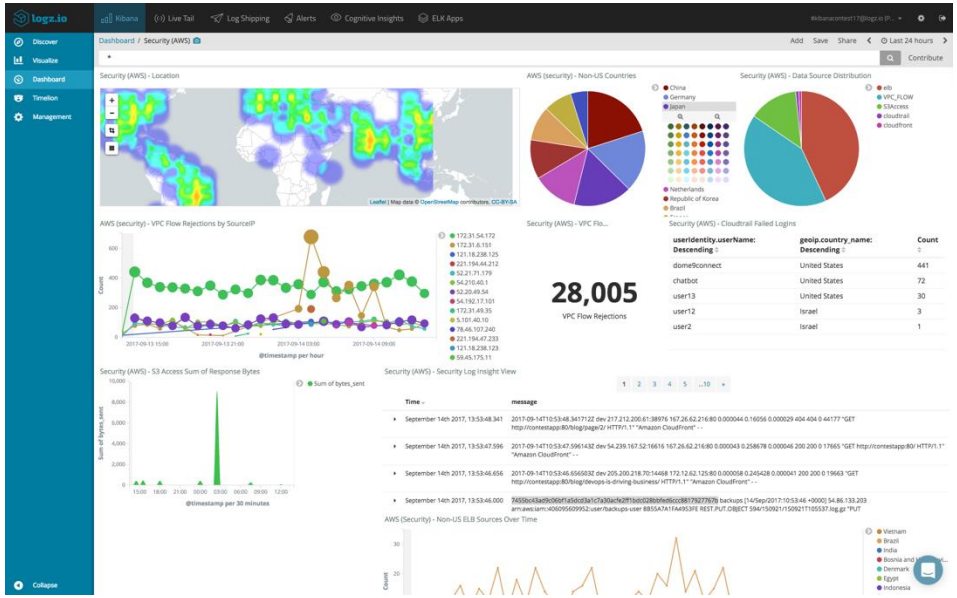
SEIM solutions should always allow users to track down intruders (user or machine) or the event activity using log search capabilities

The log search capability should be very intuitive and user-friendly, allowing IT admin to search through raw log data quickly

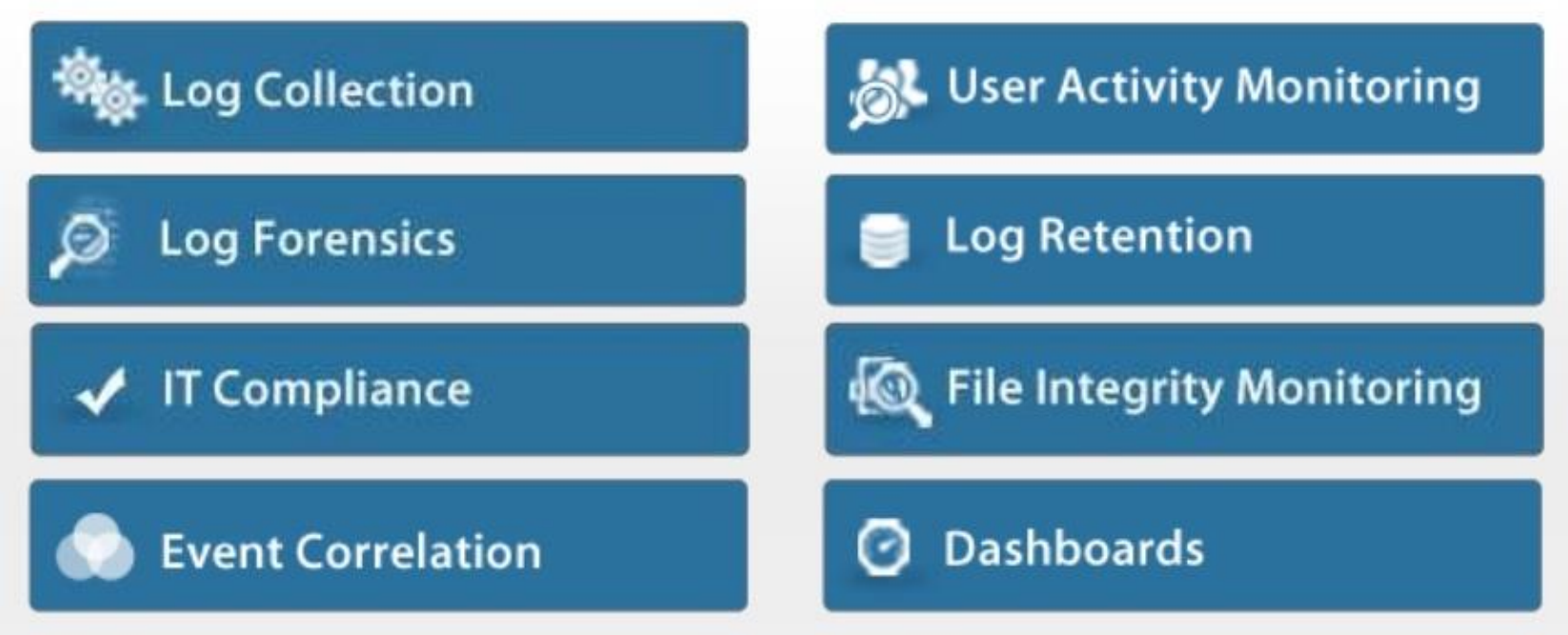


8. Dashboards

- Dashboards drive SIEM solutions and help IT administrators take timely action and make the right decisions during network anomalies
- Security data must be presented in an intuitive manner to reduce stress and to increase productivity
- Most find customizable dashboards useful between users



Here they are again



Top 5 Reasons Enterprises Benefit From SIEM Solutions

In the world of cybersecurity, there is a lot of unknowns to the average individual and one of these unknown pieces of information is what a SIEM is. Perhaps you understand that SIEM stands for Security Information Event Management and that they can help companies withstand cyberattacks, but do you know how it functions and what benefits it offers?

Here is our list of the Top-5 reasons companies love to rely on our SIEM.



Centralizing Your Security Information

There are multiple devices within your company that all fulfill different purposes. Each device generates different activity and with a SIEM solution, you can centralize that activity so that you can read reports from one source.

Pinpoint Detection; Not Just Log Aggregation

A SIEM solution not only runs reports passively like a log aggregation but also detects actireal threats. They can produce automated cross-correlation and analysis from several services, which will provide you with better detection.

Customizing Your System For The Best Protections

Along with recognizing your network devices and understanding actual threats, a SIEM solution is designed to customize a tailor-made protection force that monitors your network to filter out specific dangerous activity. By designating a SIEM solution to target common threats that your company faces, you'll be setting up the best protection possible!

Real-Time Notifications And Time Efficiency

While the SIEM constantly detects and protects against changes, it gathers fully configured information and recognizes changes in threat feeds, blacklists, and geolocations. Unlike other cybersecurity systems, these notifications have no delay; a detailed report will be made and a team of experts will be ready to find a solution within minutes.

Regulatory Compliance Fulfillment

All companies with personal information must stay within the bounds of FFIEC, HIPAA, PCI and other security regulations. When one of these entities is looking for an audit report or exam, the SIEM can generate the needed reports on things such as log user access, system changes, and any other monitoring adherence they need.

STRATOZEN

SIEM Best Practices

The Infosec Institute suggests 10 best practices for successful implementation of a SIEM platform.

- **Defining SIEM requirements:**
- **Define requirements** for monitoring, reporting and auditing, consulting all relevant stakeholders before deploying a SIEM.
- **Determine the scope of the SIEM** – which parts of the infrastructure it will cover, necessary credentials, and log verbosity.
- **Define audit data** accessibility, retention, how to achieve data integrity, evidentiary rules, and disposal for historical or private data.

SIEM Best Practices

- **Ensure you leverage the SIEM to monitor and report on all of the following:**
- **Access monitoring** – transgression and anomalous access to key resources
- **Perimeter defences** – status of perimeter defences, possible attacks and risky configuration changes
- **Resource integrity** – critical network resources – status, backups, change management, threats and vulnerabilities
- **Intrusion detection** – incidents reported by intrusion detection, or correlated/inferred using SIEM data
- **Malware defence** – violations, threats, or activity regarding malware controls
- **Application defences** – status, configuration changes, violations and anomalies for web servers, databases and other web app resources
- **Acceptable use** – status, issues and violations regarding acceptable, mandated or metered use of system resources

Next Gen SIEM

SIEM is a mature technology, and the next generation of SIEMs provide new capabilities:

- User Event Behavioural Analysis (UEBA) advanced SIEMs go beyond rules and correlations, leveraging AI and deep learning techniques to look at patterns of human behaviour. This can help detect insider threats, targeted attacks, and fraud.
- Security Orchestration and Automation (SOAR) – next-gen SIEMs integrate with enterprise systems and automate incident response. For example, the SIEM might detect an alert for ransomware and perform containment steps automatically on affected systems, before the attacker can encrypt the data.

https://www.exabeam.com/siem-guide/what-is-siem/

10 Best SIEM Tools in 2020

https://www.dnsstuff.com/siem-tools

1. SolarWinds Security Event Manager
2. Micro Focus ArcSight ESM
3. SolarWinds Threat Monitor
4. Splunk Enterprise Security
5. LogRhythm NextGen SIEM
6. IBM QRadar
7. AlienVault Unified Security Management
8. Sumo Logic
9. RSA NetWitness Suite
10. McAfee Enterprise Security Manager

Splunk Enterprise

https://help.splunk.com/en/splunk-cloud-platform/get-started/search-tutorial/10.1.2507/part-6-creating-reports-and-charts/save-and-share-your-reports

Splunk – Indexing data

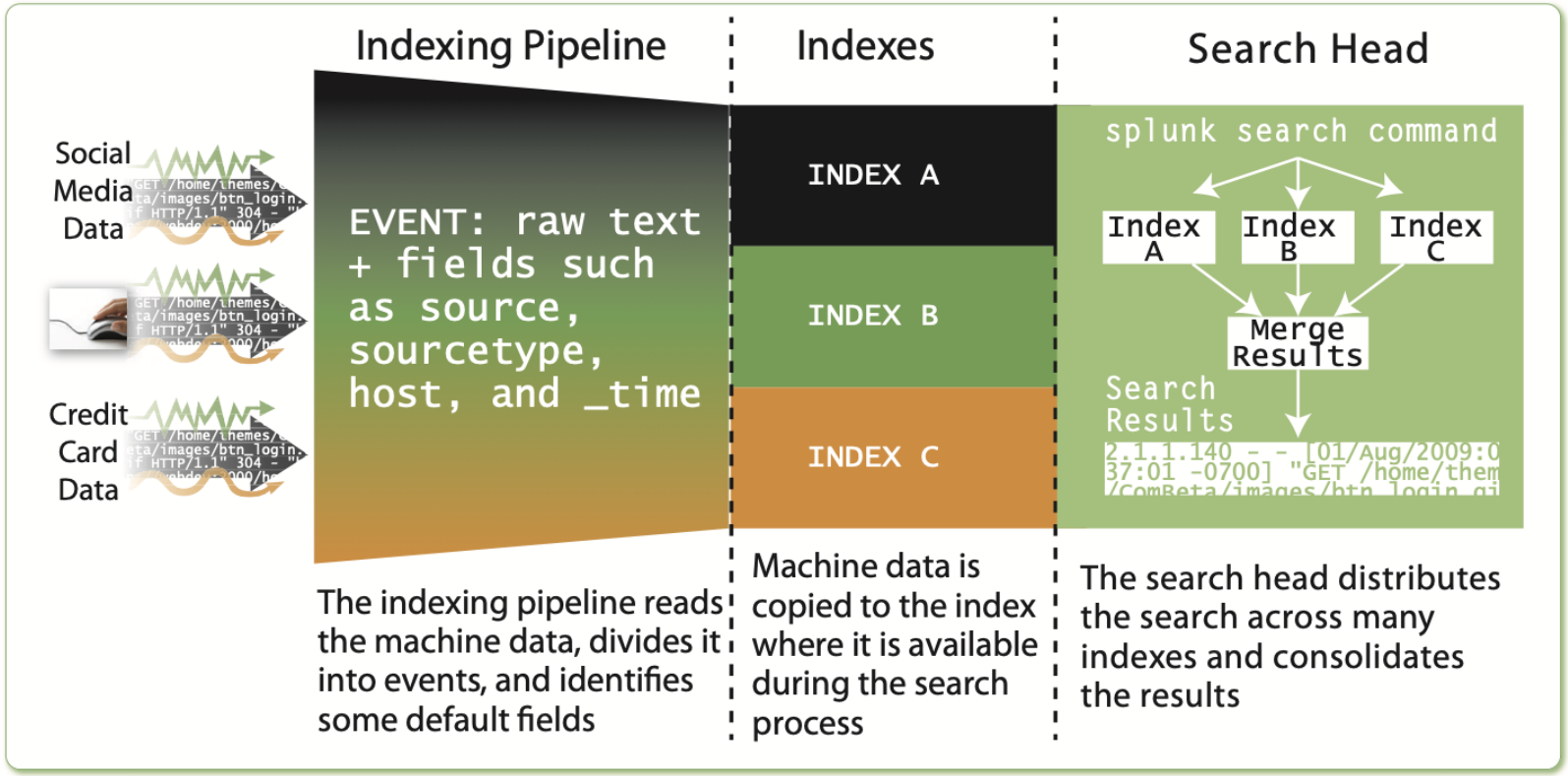


Figure 2-5. The Unique Characteristics of Splunk Indexes

Event

Every event in Splunk has at least the four default fields

Table 2-1. Fields Splunk Always Indexes

Field	Answers the question	Examples
source	Where did the data come from?	files (/var/log/), scripts (myscript.bat), network feeds (UDP:514)
sourcetype	What kind of data is it?	access_combined, syslog
host	Which host or machine did the data come from?	webserver01, cisco_router
_time	When did the event happen?	Sat Mar 31 02:16:57 2012

/var/log/syslog
/var/log/auth.log

SPL™: Search Processing Language

The entire string: **sourcetype**=syslog ERROR | **top** user | **fields** - percent is called a search, and the pipe character (|) separates the individual commands that make up the search.

- **top, fields**: are search commands
- | (pipe character)
- Implied command: **search**. Totally there are 3 commands: search, top, fields
- Implied **AND**: sourcetype=syslog AND ERROR
- **Top**: returns the top 10 most common values for the specified field (e.g. field user) in descending order. The output of top is a table of 3 columns (user, count, and percent), with 10 rows of values.
- The output of TOP command becomes the input of the next command after the pipe (e.g. fields)
- fields -percent: fields is the command, -percent is the argument. Tells Splunk to remove the percent column from the output of the top command.

Example:

What are the top 50 source and destination IP pairs?

…| top limit=50 src_ip, dest_ip

Who are the top users for each host?

sourcetype=”access” | top user by host*

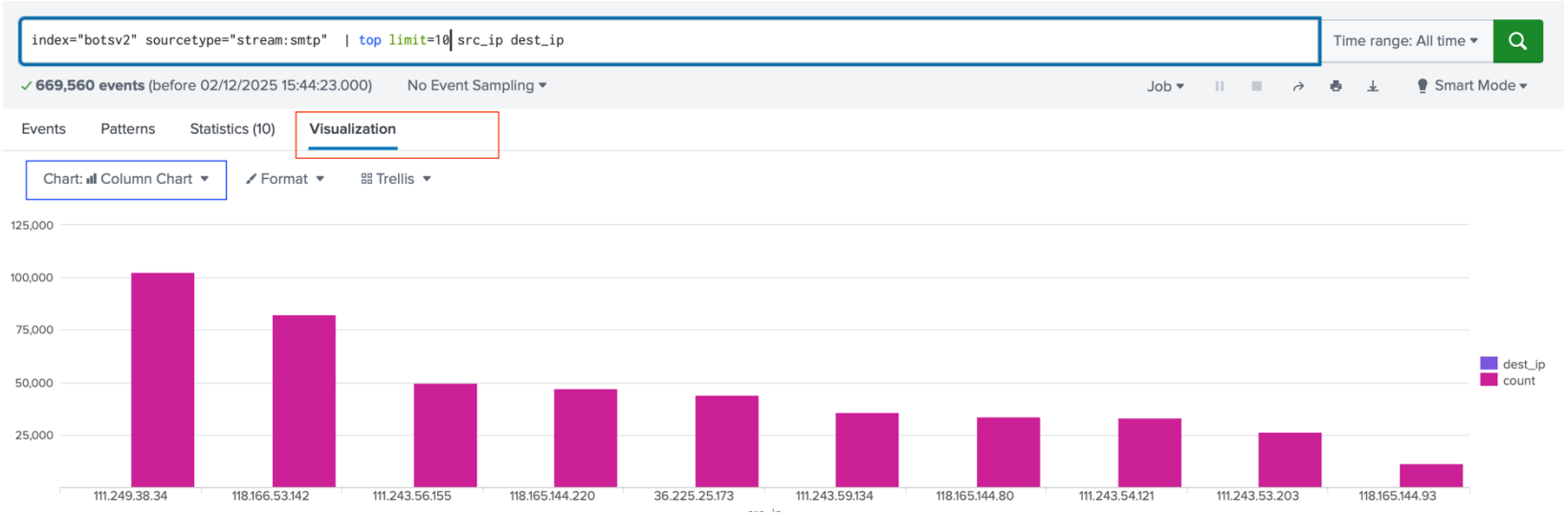
What are my top 10 web pages?

sourcetype=”access” | top uri*

Creating visualizations

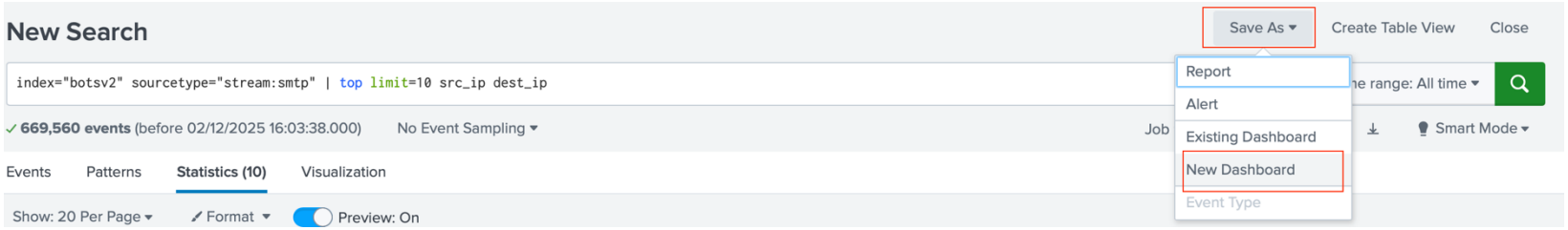
After you run a search, select “Visualization”. You can choose the type of chart by configuring “Chart”

Example



Creating dashboard

After you run the search, select “Save As” -> ”New dashboard” to create a new dashboard (or “Existing dashboard” to add the report/ chart into an existing dashboard)



Save Panel to New Dashboard

Dashboard Title: dashboard_ex1

dashboard_ex1 Edit ID

Description: Optional

Permissions: Private

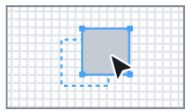
Dashboard type

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio
A new builder to create visually-rich, customizable dashboards

Select layout mode

Absolute
Full layout control



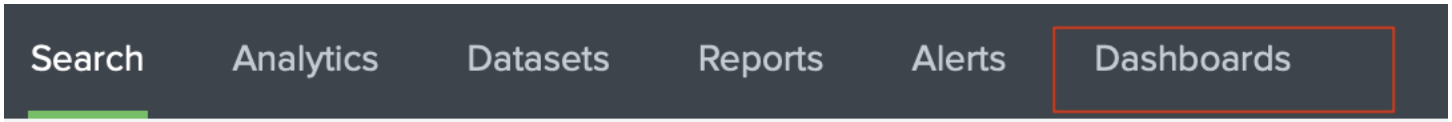
Grid
Quick organization



Panel Title: Optional

Cancel | Save to Dashboard

View existing dashboard



Networking example: Varonis

Varonis captures file event data from various data stores – on-premises and in the cloud – to give the who, what, when, and where of each file accessed on the network.

Varonis also collects DNS, VPN, and web proxy activity to correlate the network activity with the data store activity to paint a complete picture of an attack from infiltration through file access to exfiltration.

behavior analytics (UBA) to provide meaningful alerts based upon learned behavior patterns of users, along with advanced data analysis against threat models that inspect patterns for insider threats (such as exfiltration, lateral movement, account elevation) and outsider threats (like ransomware).

Demo Videos

https://www.youtube.com/watch?v=apYGbbzbOPU

https://www.youtube.com/watch?v=9TRqZuZqtKY

https://www.youtube.com/watch?v=gX_N_836Im0

https://www.youtube.com/watch?v=N7J0EwdbKF0

Sadly many of these are paid and we don't have access to all of them. We will be looking at parts, but they won't integrated and with a nice interface.

The Job(s)

Computer Security Incident Response Teams (CSIRTs) describes the tools, procedures and roles necessary to implement the team.

* Creating useful teams requires finding the right mix of people, processes and technologies (CSIRT/SOC/SIEM).

* it's all about striking the right balance between workforce talent and the right security tools

* CSIRT - computer security incident response team. Expert services can be provided by in-house CSIRTs or outsourced to external service providers (MSSPs).

* A CSIRT be a part of an organization's security operation centre (SOC), a group responsible for overall (IT) security including policies, compliance, governance and security of systems and applications.

Thank you!