Hello everyone!

In this blog i wanted to give you overview of security Operation Center also we are going to discuss about some use cases using SPLUNK. This blogs helps you to understand the operational goal of SOC and how we can build use cases using Splunk (one of the famous SIEM tool). This blog will help Student, Fresher, Industry Expert who wants to work for security Operation Center.

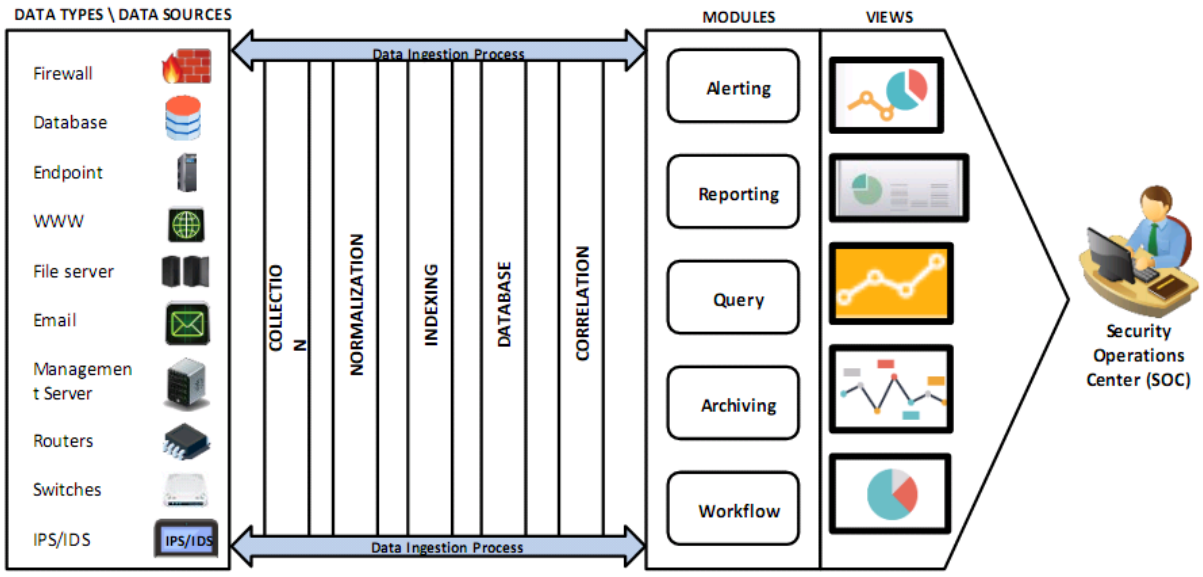
What is security Operation?

Security Operation is the continuous operational practice for maintaining and managing a secure IT environment through the Implementation and execution of certain services and process it's main purpose is to detect, prevent, prioritize and respond to security incidents.
Security Operation Consist of various security operation tasks, which include:

- **Security Monitoring**
- **Security Incident Management**
- **Vulnerability Management**
- **Security Device Management**
- **Network flow Monitoring**

Security Operation Center

SOC is centralized unit and a single point of view through which an organizations assets are monitored, assessed and defended from the threats. It also facilitates the situational awareness and real time alerting if any intrusion or attack is detected.



SOC capabilities

- **Situational Awareness and operational intelligence -** SOC provides information about what is going on across the different parts of IT infrastructure. It also provides the Operational intelligence about IT infrastructure.
- **Threat control and prevention -** Using Internal and external resource it provides the knowledge of IOC'S (Indicator of compromise) of attacks this enables SOC to provide Threat control and prevention.
- **Forensics -** SOC analysts use structured log data to conduct investigation and understand the root cause of attack and also restrict the attacker's ability to perform attack against the organization**.**

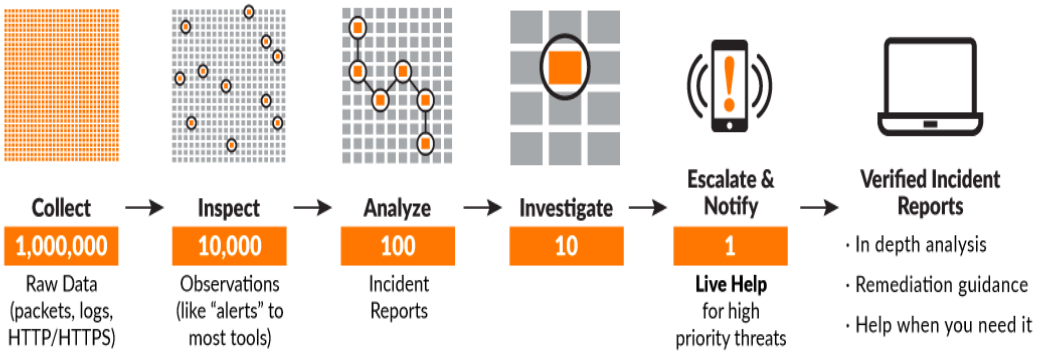
What Operations carried out in Security Operation Center?

1. **Log Collection** - Logs are collected from various device on a network that can have an impact on the security of the organization.

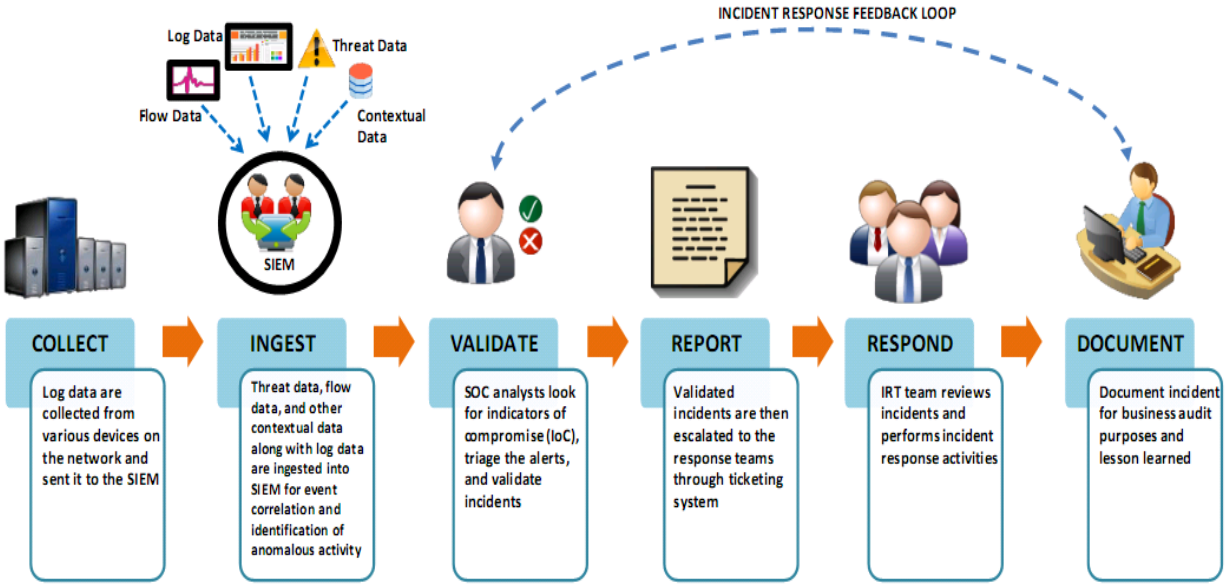
2. **Log Retention and Archival** - Collected logs are stored centrally and logs always have Retention and Archival period for better management.
3. **Log Analysis** - logs are analyzed through different SOC technology to extract information from raw data.
4. **Monitoring of Security Environments for security Events** - Information received by log analysis is transferred to the SOC team for

monitoring purposes so that it can be used to identify the current security position of an organization.

5. **Event Correlation -** The events from the various source are correlated and contextualized based on set of predefined correlation rules.
6. **Incident Management** - Prioritization of Incident as per the predefined rules and objective.
7. **Threat Identification and Reaction** - It is a process of determining threats correctly and a proactive measure obtained through. A SOC reacts either re-actively or proactive to threats.
8. **Reporting** - It generates Client detailed Security report



Security Operation Center Work Flow.



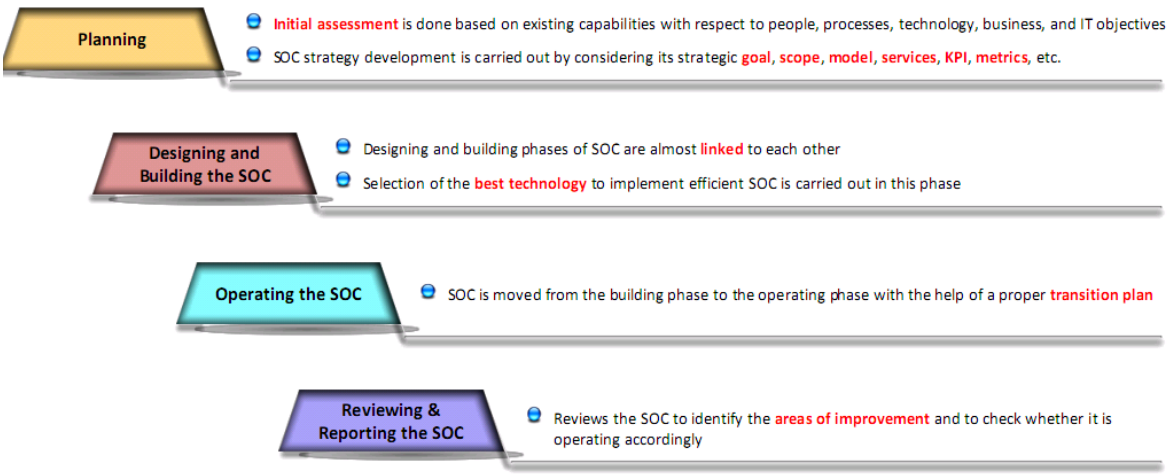
Components of Security Operation Center.

People <---------->Process <----------> Technology

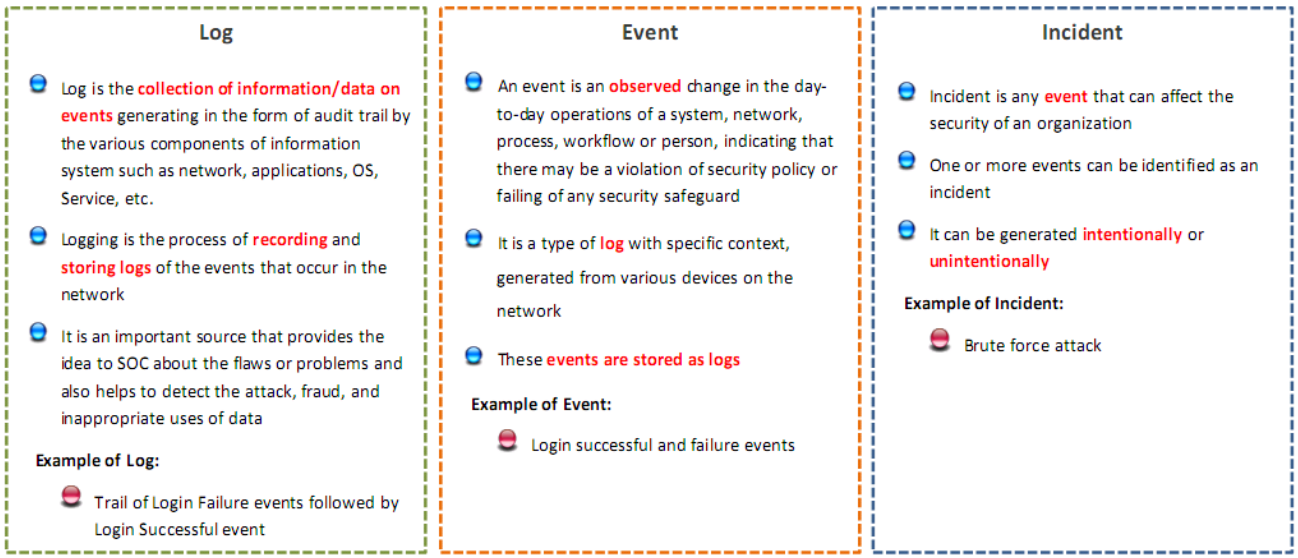
Type of Security Operation Center Models.

- Internal SOC model
- Outsourced SOC model
- Hybrid SOC model

SOC Implementation phases.



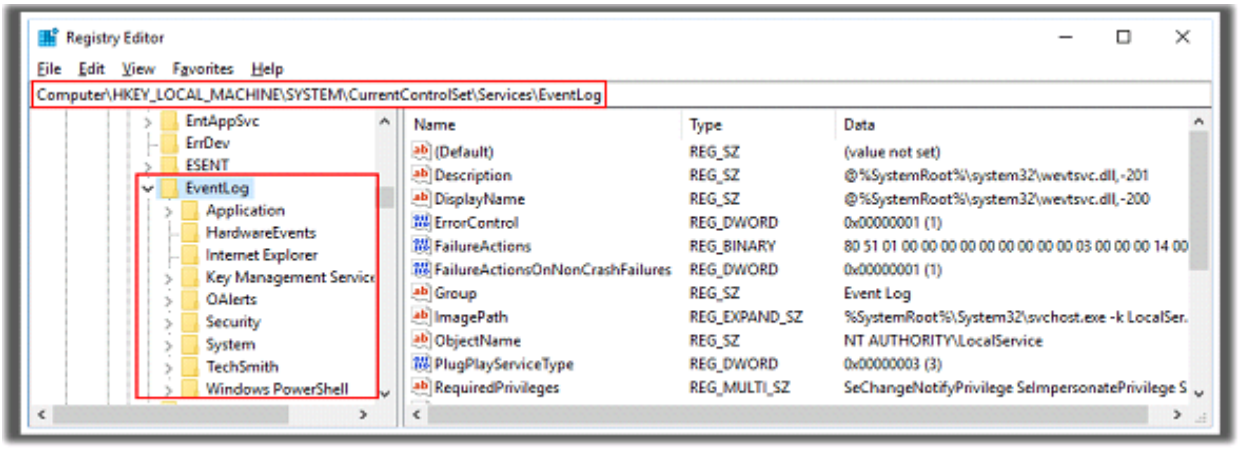
Difference Between Log Event and Incident.



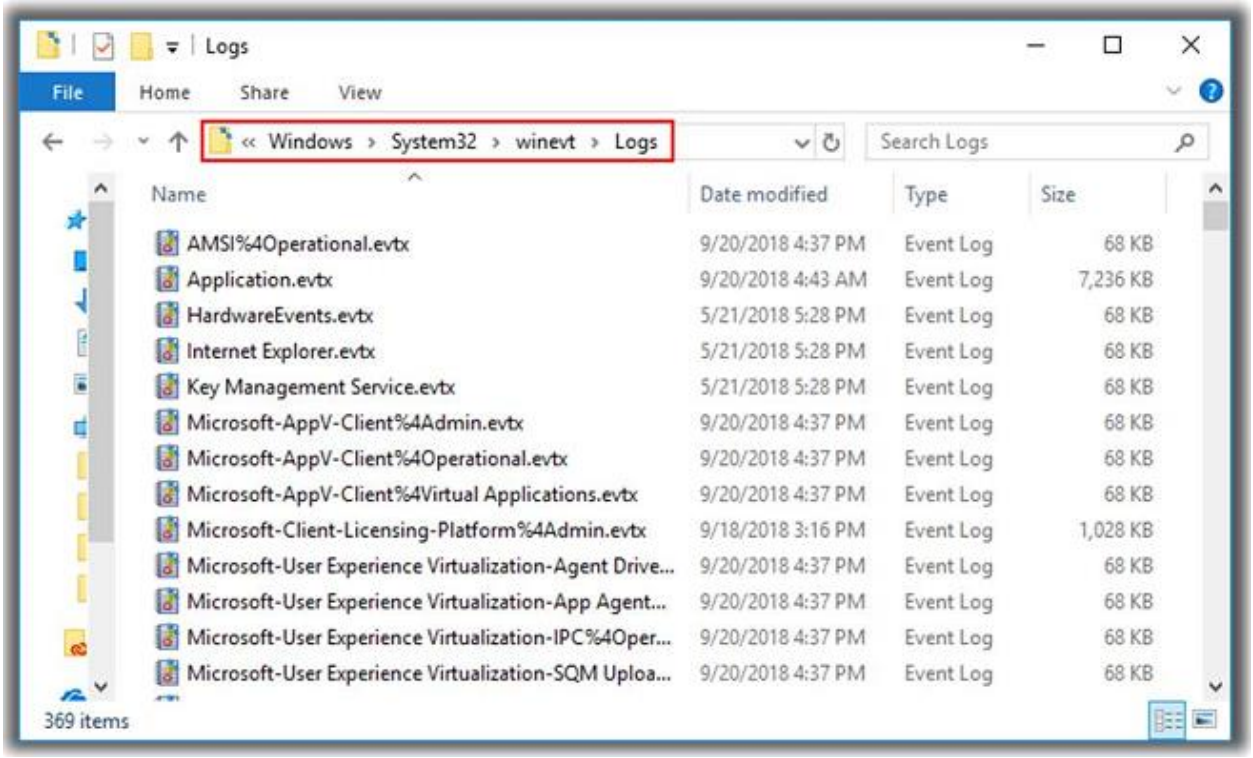
So let's understand where we can find logs which we need to collect for the Security Operation center and how to build use cases for detection of incident.

Window Logs and location.

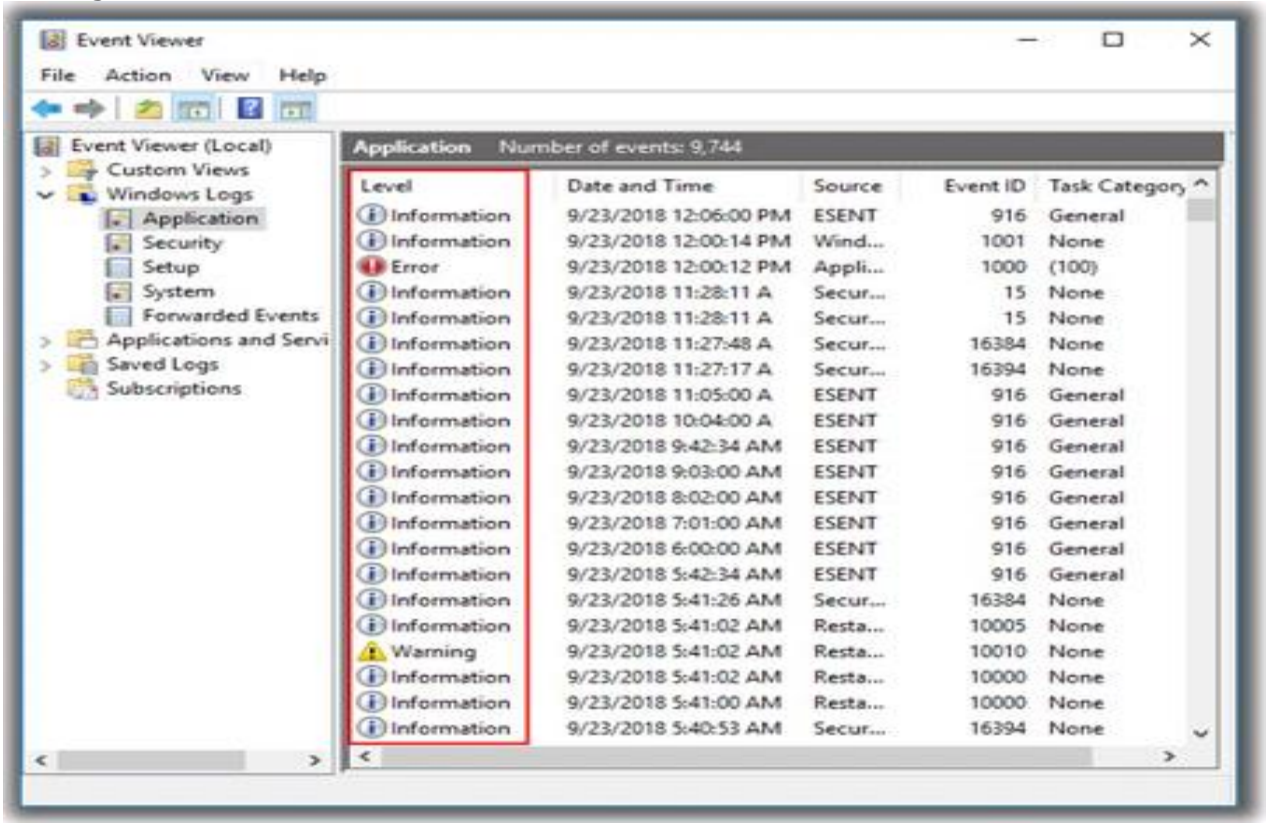
Windows Event log audit configuration are recorded based on the registry key.
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog



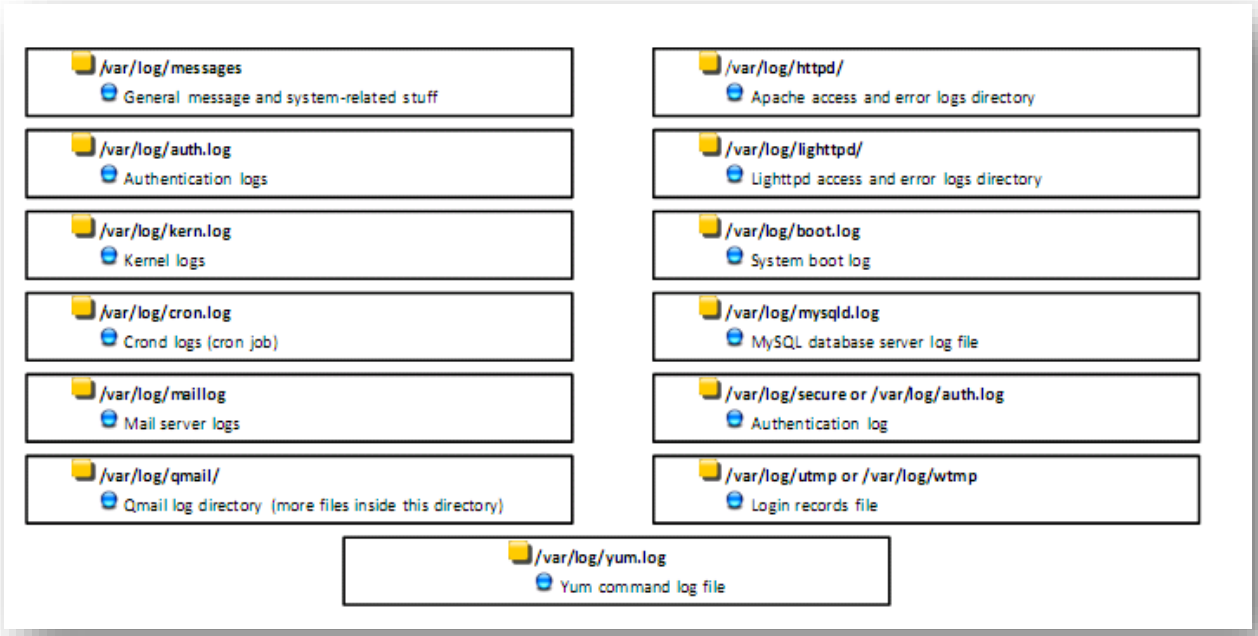
In windows machine event log are stored in system32\winevt\logs as shown below.



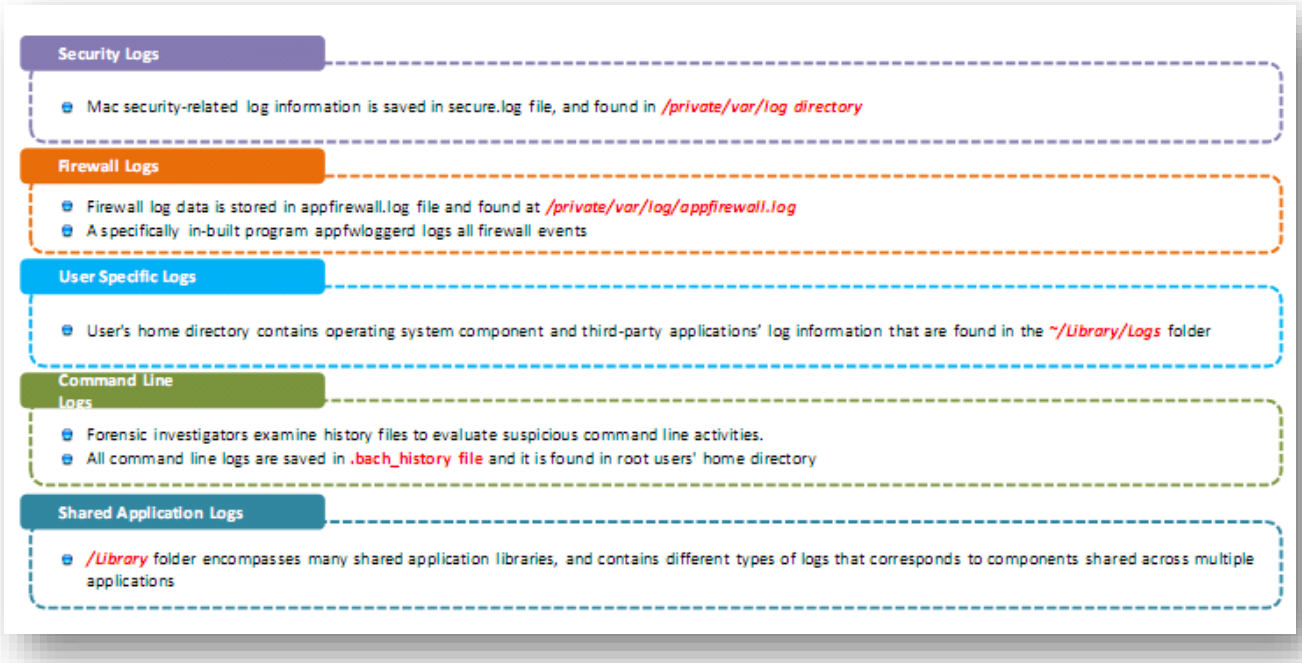
In windows machine event are stored in Event viewer which you can open through RUN "eventvwr".



Linux Log and Location.

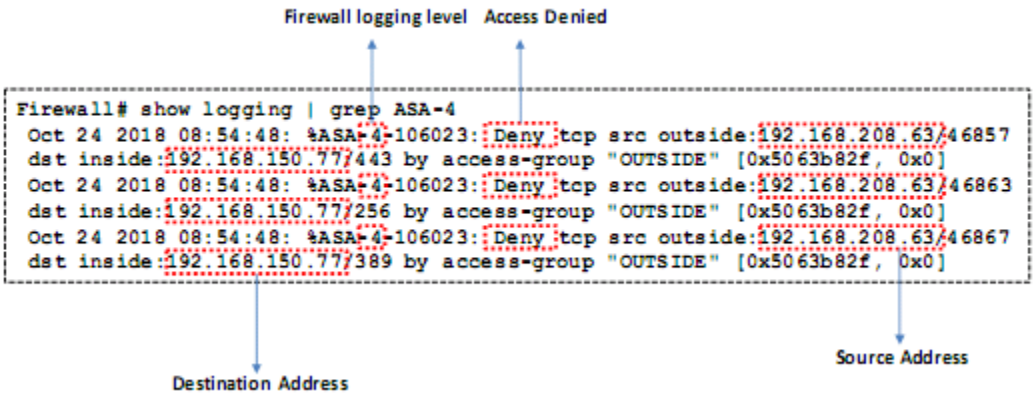


Mac Log and Location.

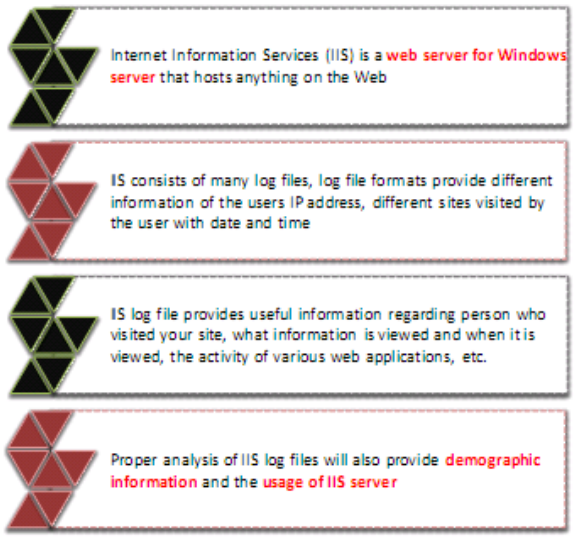


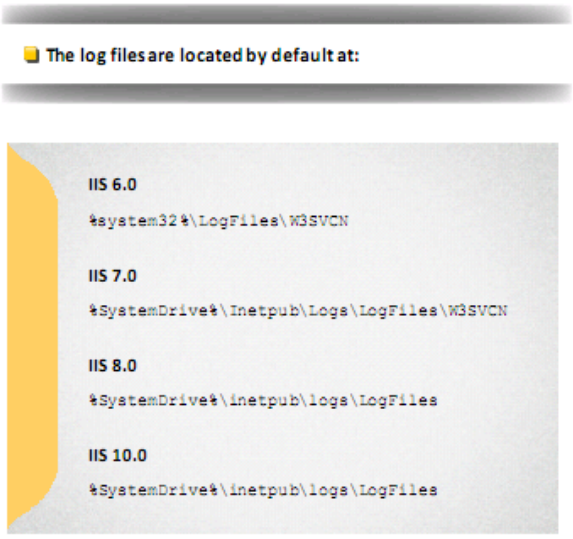
Log file	Location	Description
crashreporter.log	/var/log/crashreporter.log	Application usage history and application crash information written to this file
access_log	/var/log/cups/access_log	Printer access log information
error_log	/var/log/cups/error_log	Printer connection information and its error logs found here
daily.out	/var/log/daily.out	Network Interface History
log.nmbd	/var/log/samba/log.nmbd	Samba (Windows-based machine) connection information
Logs	~/Library/Logs	Home directory users and application-specific logs can found here
DiscRecording.log	~/Library/Logs/DiscRecording.log	Home users' CD & DVD media burning logs written to this file
DiskUtility.log	~/Library/Logs/DiskUtility.log	This file contains hard disk partitioning logs, CD/DVD burned media logs, ISO/DMG images files mount, unmount history, and file permission repair history
iChatConnectionErrors	/Library/Logs/iChatConnectionErrors	Log history of iChat connection attempts. Data such as username, IP address, and Date & Time of the attempt
Sync	/Library/Logs/Sync	This log file gives information on synchronized Mac systems and mobile devices such as cell phones and iPods, and their activities with date and time

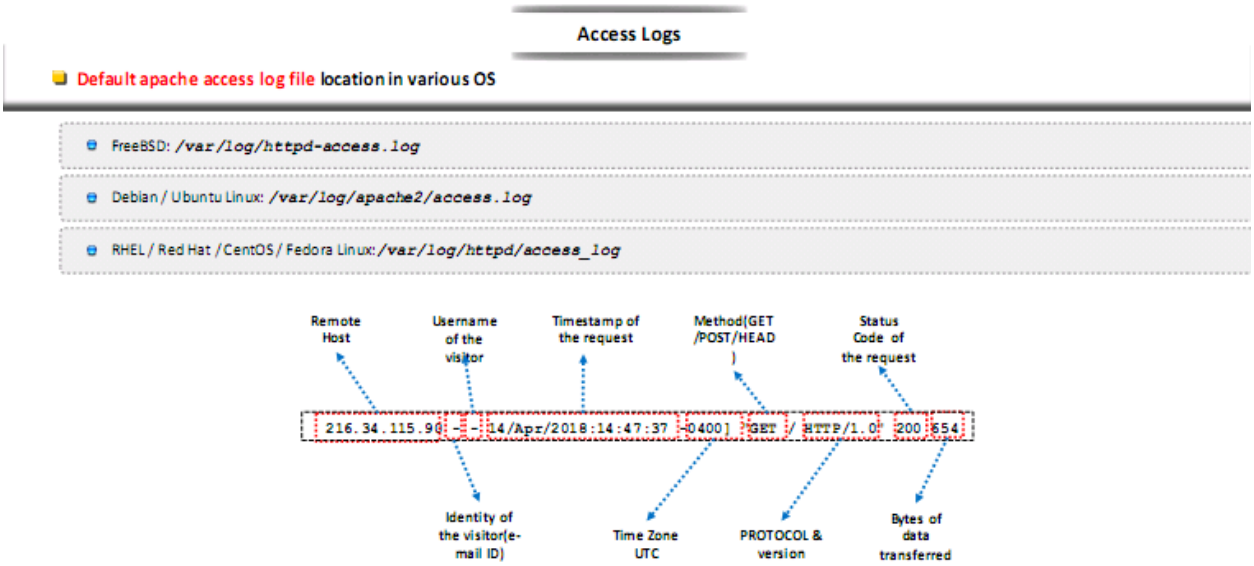
Firewall Log and Location.



Web server Log and Location.







Based on these log we can create a centralized log mechanism and able to identify potential incident. lets talk about some case studies using SPLUNK.

USE CASES of Operational Intelligence using SPLUNK.

CASE STUDY 1.

Problem Statement:-

You need to find the least accessed files on your server by your clients/ customers. As part of the cleanup process, you need to find the files which receive the least amount of user traffic. You can generate a report showing how the traffic has been distributed over different months.

Solution:

```
index=main sourcetype=access_combined_wcookie status=200 | rare file by date_month
```

CASE STUDY 2

Problem Statement:-

From a business perspective, you are expected to track the website traffic(user sessions) recorded on your server. The traffic coming in can be from various marketing campaigns run by your team. Besides tracking the traffic, you are also expected to find the number of products purchased by the users from various campaigns.

Now generate a report based on user sessions and campaigns.

Solution:

```
index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do |
dedup JSESSIONID | table JSESSIONID | rename JSESSIONID as UserSessions
```

CASE STUDY 3

Problem Statement:-

You are a part of the Operations team and you're expected to track the usage of your web application.

Generate a report which tells how many times each user has tried logging into the application.

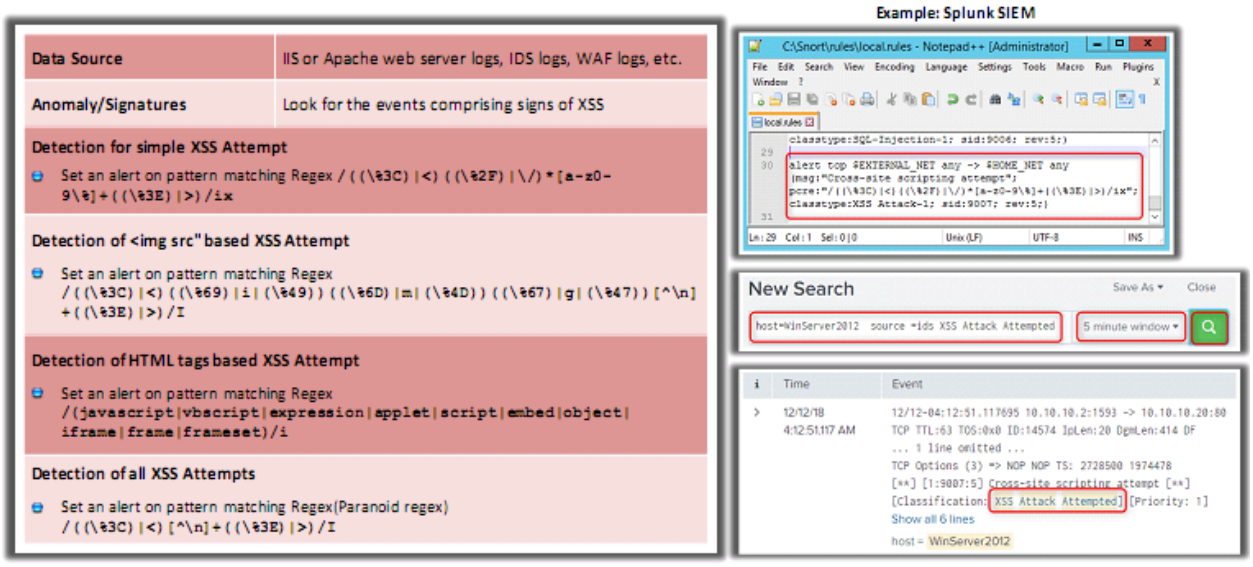
Solution:

```
index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID)
```

USE CASES for threats using SPLUNK.

XSS Attack detection using Splunk.

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

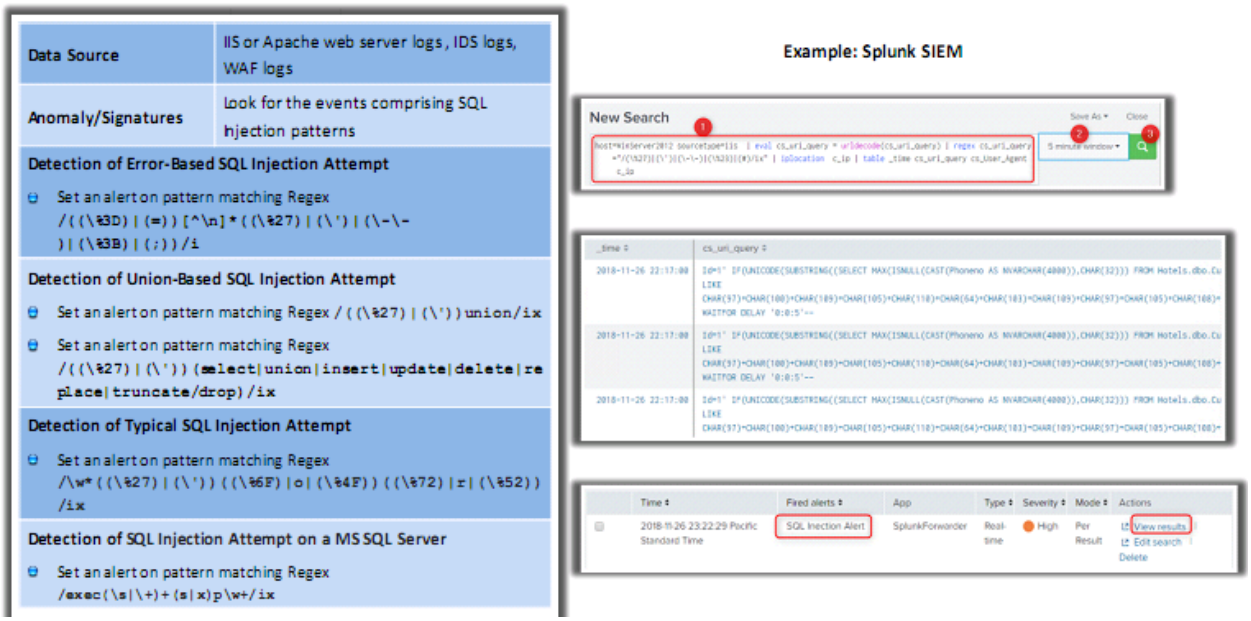


SQL Attack Detection using SPLUNK.

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It

generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.



Data Source	IIS or Apache web server logs, IDS logs, WAF logs
Anomaly/Signatures	Look for the events comprising SQL injection patterns

Detection of Error-Based SQL Injection Attempt

- Set an alert on pattern matching Regex `/((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/i`

Detection of Union-Based SQL Injection Attempt

- Set an alert on pattern matching Regex `/((\%27)|(\'))union/ix`
- Set an alert on pattern matching Regex `/((\%27)|(\'))(select|union|insert|update|delete|replace|truncate/drop)/ix`

Detection of Typical SQL Injection Attempt

- Set an alert on pattern matching Regex `/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix`

Detection of SQL Injection Attempt on a MS SQL Server

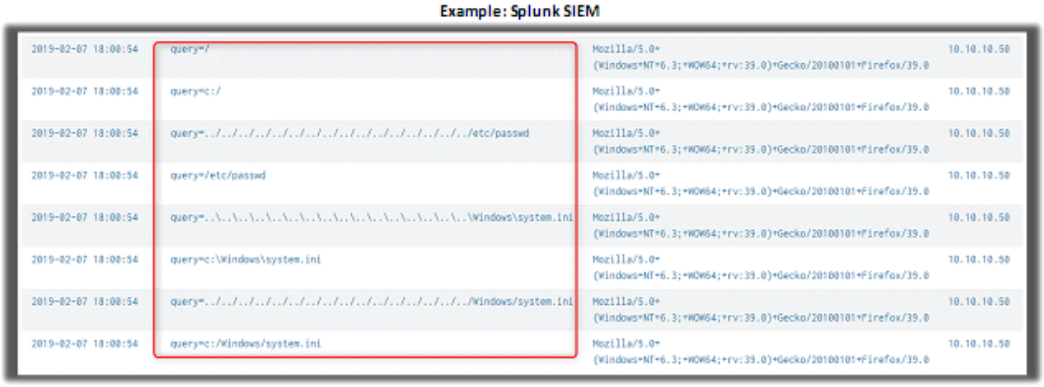
- Set an alert on pattern matching Regex `/exec(\s|\+)+(s|x)p\w+/ix`

Directory Traversal Detection using SPLUNK.

Directory traversal (also known as file path traversal) is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files. In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

Data Source	IIS or Apache web server logs , IDS logs, WAF logs. etc.
Anomaly/Signatures	Look for events comprising directory traversal suspicious patterns
Set an alert on pattern matching "/etc/passwd"	
Set an alert on pattern matching Regex / (\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\\|(%|%25)5C)/i	

Example: Splunk SIEM



2019-02-07 18:00:54	query=/	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=c:/	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=../../../../../../../../../../../../../../../etc/passwd	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=/etc/passwd	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\Windows\system.ini	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=c:\Windows\system.ini	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=../../../../../../../../../../../../../../../Windows/system.ini	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50
2019-02-07 18:00:54	query=c:/Windows/system.ini	Mozilla/5.0+ (Windows+NT+6.3;+WOW64;+rv:39.0)+Gecko/20100101+Firefox/39.0	10.10.10.50

Likewise we can detect all the threats using SPLUNK. Thanks for your time I hope you all have a seriously awesome week. This is just an overview let me know if you need more guidance for the same. HAPPY to HELP.