International School

Capstone Project 1

CMU-CS450

CAPSTONE ARCHITECT DOCUMENT

Version 1.0

Date: 10/12/2022

Command and Control Attack Simulation & Log Analysis

Submitted by

Pham Anh Khoa

Tran Minh Huy

Nguyen Huy Trung

Tran Van Khoa

Approved by

Tinh,Le Van M.Sc.

Proposal review panel representative

____

Name	Signature	Date

Capstone Project 1 – Mentor

____

Name	Signature	Date

PROJECT INFORMATION

Project acronym	C2 AS & LA		
Project Title	Command And Control Attack Simulation & Log Analysis		
Start Date	18– Aug – 2022	**End Date**	10 – Dec – 2022
Lead Institution	International School, Duy Tan University		
Project Mentor	Tinh, Le Van M.Sc. Email: letinh1000@gmail.com Tel: 0935779922		
Scrum master / Project Leader & contact details	Khoa, Pham Anh Email: khosasuke@gmail.com Tel: 0905648553		
Project Web URL			
Team members	Name	Email	Tel
	Trung, Nguyen Huy	huytr.work@gmail.com	0968580247
	Huy,Tran Minh	Minhhuy2015@gmail.com	0935010972
	Khoa, Tran Van	Tranvankhoa.1998@gmail.com	0522909360

REVISION HISTORY

Version	Date	Updates content	Author	Approval
1.0	18/08/2022	Initial Document	Member of C2NE.01	Yes
2.0	10/12/2022	Final Document	Member of C2NE.01	Yes

Table of Contents

1. Introduction 4

1.1. Purpose 4

1.2. Scope 4

2. An overview of Red Team Attack Infrastructure 4

2.1 Methods use in Red Team Attack Infrastructure 6

2.1.1 Web Protocols 6

2.1.2 DNS 6

3. An overview of SIEM 7

3.1. What Are the Core Components of SIEM Architecture? 7

3.2 Parameters for evaluating SIEM methodologies 8

4. How it execution 10

4.1. Overviews 10

4.2. Existing software 11

4.2.1. Cobalt Strike 11

4.3. What’s new in our system 11

5. SIEM data processing techniques 16

6. Conclusion 17

7. References 17

1. Introduction

1.1. Purpose

This document provides an overview of the Command and Control (C2) infrastructure of the implant software, which is a fundamental part of any Red Team operation. Over the years, there has been a proliferation of C2 frameworks to support the task of setting up and controlling software implants in the target environment. These include things like Empire, Cobalt Strike, Covenant, Merlin, Mythic, SILENTTRINITY, PoshC2, Sliver, and more.

1.2. Scope

This Architect document provides an overview of the C2 (Command and Control) attack simulation and the more general architecture of SIEM. Businesses must constantly protect themselves from the growing number of cyberattacks they face every day. Security Information and Event Management (SIEM) is a security system widely adopted by many businesses to protect their networks from these cyberattacks. A SIEM solution consists of various components that help security teams detect data breaches and malicious activities by continuously monitoring and analyzing network events and devices. This article details the various components of the SIEM solution architecture.

1.3. Technical Requirements

* Performing thorough analysis of the existing system of the organization.

* Design and implement SIEM event monitoring system.

* Check the monitoring system on the customer's computer for malicious code.

2. An overview of Red Team Attack Infrastructure

In today's world, Cyber and Systems Security is of paramount importance in the digital media environment. Along with the development of technology, many threats to information security have appeared, affecting sensitive transactions more heavily. Today, intruders can easily break through the walls of the network and can cause many types of breaches such as network incidents where the most dangerous incident that businesses always face is malware. Usually use C2 infrastructure. To avoid such breaches, it is very important for a security administrator to detect an intruder and prevent him from entering the network. In everyday life, new threats and related solutions are emerging together.

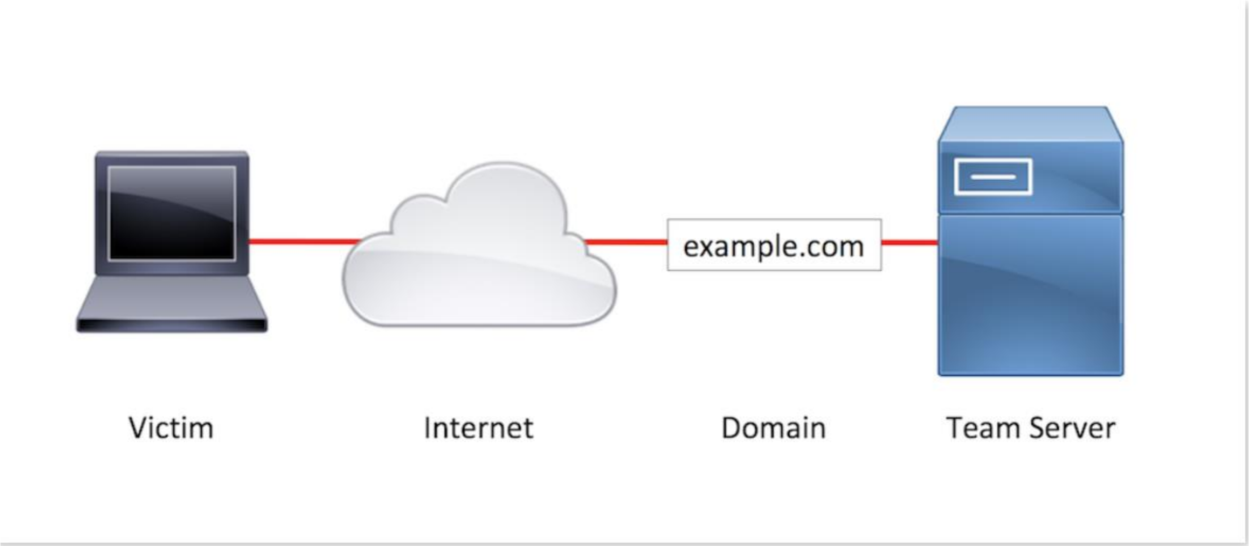


Figure 1: Sample Penetration Test Infrastructure

Attack servers typically perform phishing email initialization, payload storage, and C2. The only asset between the target network and the attack server is a domain. This setup means that if any individual component of the attack, such as a phishing email, is determined to be malicious, there is a high chance that a large part (or all) of the attack will occur. will be violated. Since phishing emails are likely coming from the same domain that the payload is hosted on, which is also where C2 connects, one email and web block for one domain can block the entire attack.

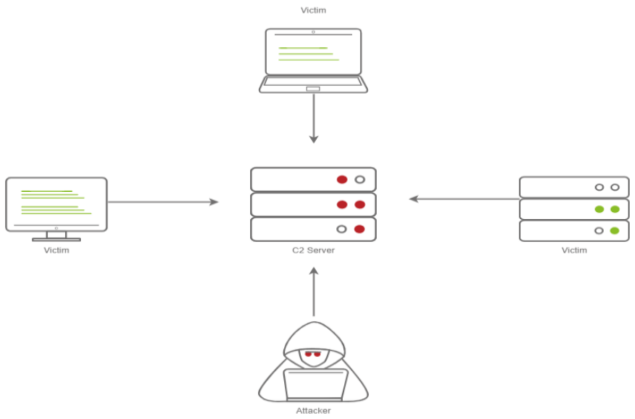
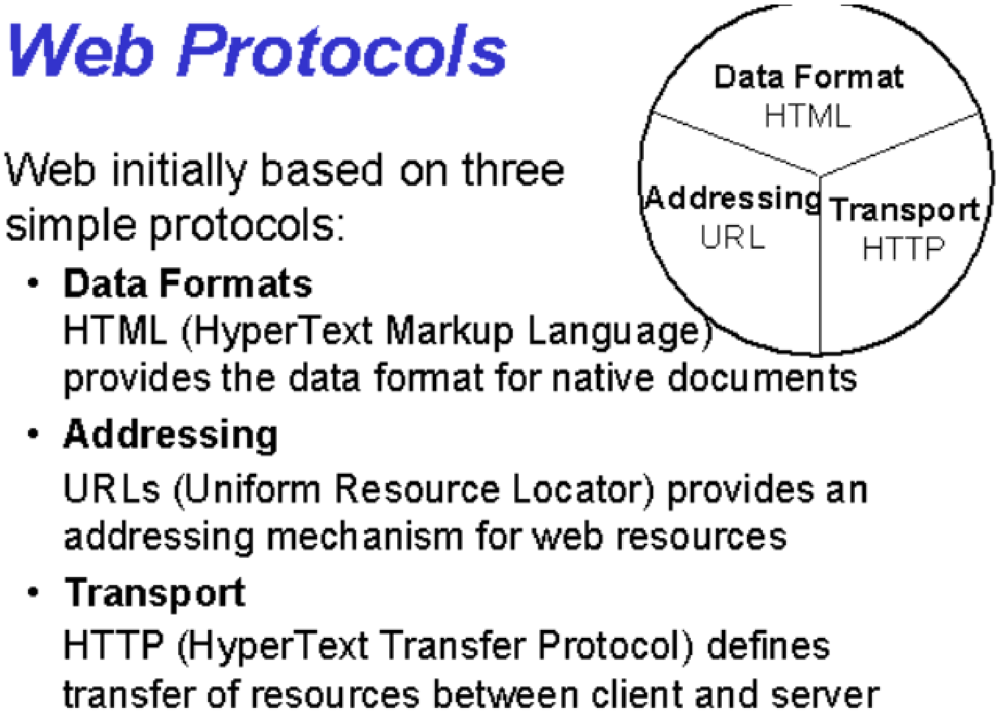


Figure 2: This screenshot depicts a basic C2 server diagram

2.1 Methods use in Red Team Attack Infrastructure

2.1.1 Web Protocols

Hackers can communicate using application layer protocols associated with web traffic to avoid network detection/filtering by mixing with existing traffic. Commands to the remote system and often the result of those commands will be embedded in the protocol traffic between the client and the server.



Web Protocols

Web initially based on three simple protocols:

- **Data Formats**
  HTML (HyperText Markup Language) provides the data format for native documents
- **Addressing**
  URLs (Uniform Resource Locator) provides an addressing mechanism for web resources
- **Transport**
  HTTP (HyperText Transfer Protocol) defines transfer of resources between client and server

Figure 3: Web Protocols

2.1.2 DNS

Hackers can communicate using the Domain Name System (DNS) application layer protocol to avoid network detection/filtering by mixing with existing traffic. Commands to the remote system and often the result of those commands will be embedded in the protocol traffic between the client and the server.

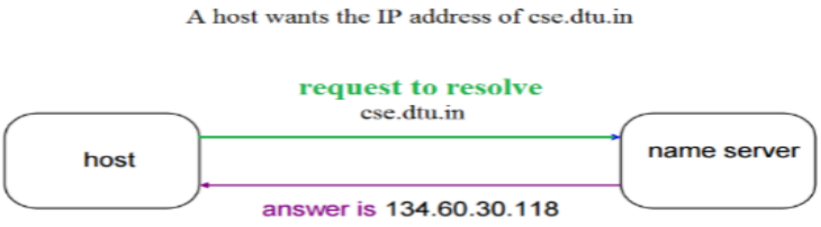


Figure 4: Basic DNS scheme

3. An overview of SIEM

In information warfare, the need to develop a SIEM architecture has become an important factor due to the existence of ever-increasing cyber threats and their creators - cyber-threats. SIEM (Security Information and Events Management) introduces a range of products or services aimed at managing security information and security events simultaneously. SIEM also provides analysis of security alerts in a timely manner. In order to enable SIEM to work effectively and comprehensively, attention must be paid to its construction, i.e. its technology and architectural process. As concise and concise as possible, this article aims to provide insight into the workings of the SIEM architecture.

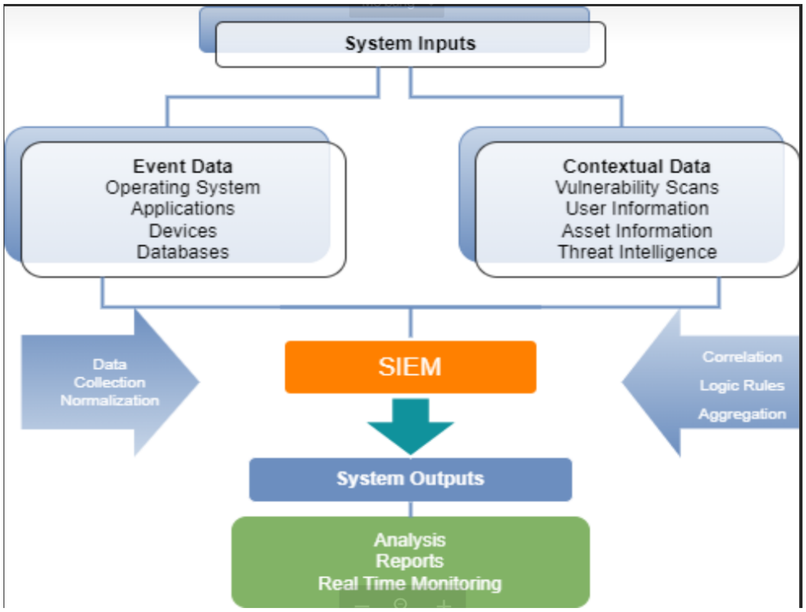


Figure 1: SIEM Architecture

3.1. What Are the Core Components of SIEM Architecture?

The architectural aspect of SIEM is basically concerned with the process of building the SIEM system and core components. In summary, the SIEM architecture consists of the following components:

Management of Logs

Normalization of Logs

Source of Logs

Hosting Chooses for SIEM

Reporting of SIEM

Real-Time Monitoring

Management of Logs

This involves data collection, data management, and previous data retention. SIEM collects both event data and contextual data as specified in Figure 1 above. Basically, the SIEM architecture collects event data from organized systems such as installed devices, network protocols, storage protocols (Syslog), and streaming protocols.

Normalization of Logs

It is clear from Figure 1 that the SIEM receives event and context data as input. However, such normalization is necessary. This has to do with how event data is transformed into relevant security insights. Essentially, this process entails removing extraneous data from the data generated through the filtering process. The main import of this is to retain only relevant data for future analysis.

Source of Logs

Logs are collected from network applications, security systems, and cloud systems. Essentially, this process is concerned with how organizations bring logs into SIEM.

Hosting Chooses for SIEM

There are different models of SIEM storage. These include Self-Host, Cloud-Host or Hybrid-Host.

Reporting of SIEM

Based on available logs, SIEM identifies and reports suspicious activities.

Real-Time Monitoring

SIEM provides real-time monitoring of an organization's infrastructure through threat detection and rapid response to potential data breaches.

3.2 Parameters for evaluating SIEM methodologies

Supplier 1 Product X	Indicators	Importance or weight	Evaluation	NOTES
Applicability	Level of Compliance Complexity Quality of services Robust Architecture Scalability Complete description Installation duration/ clearness of road map	High High High High Medium High High	Excellent Very Good Very Good Very Good Good Excellent Very Good	High compliance Very Flexible High availability is guaranteed Clear roadmap including all steps
Licensing and support services	Licensing Support Training Additional features	High Medium Medium Low	Very Good Good Good Good	Clear dimensioning including user acceptance test period 24 × 7
Advanced Features	Integration with third parties	Medium	Good	
Other indicators	Expertise/Skill of Vendor/Supplier Price	Medium Medium	Excellent Excellent	One major player
RESULT				ACCEPTED

Table 1. Methods of SIEM comparison

4. How it execution

4.1. Overviews

A Command and Control (C&C) server is a computer remotely controlled by a cybercriminal that is used as a command center to send commands to systems that have been infected with malware, and often a part of a large Bot network. Systems running malware that communicate with Internet-based C&C servers can steal critical data from your organization, such as when the Emoted virus takes user passwords and sends them to the server. C&C online. They can also cause even more damage

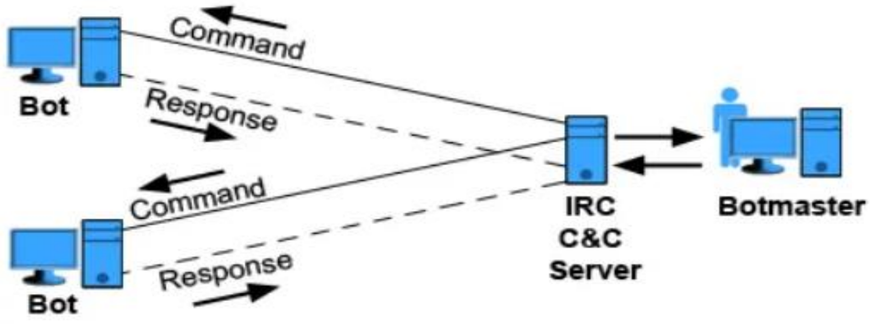


Fig 5. Working Command and Control

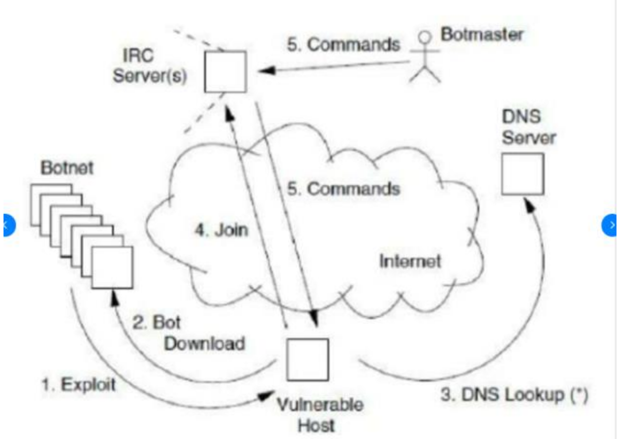


Fig 6. Command and Control Architecture

Command and Control Architeture

- When the attacker issues control commands to the host organization (hacker), the IRC controls the communication with the victim machine. The next step, the hacker will distribute the malicious code sample created on C2 - Accordingly, downloading the malicious code sample will cause an error for the user and be forwarded to the DNS server. This is one of the steps to deploy on C2's infrastructure.

4.2. Existing software

4.2.1. Cobalt Strike

Cobalt Strike is a penetration testing framework that allows a hacker to deploy a Beacon on a victim machine (Beacon is a direct link to the network, controlled by the hacker, and executes malicious behaviors and scripts) and can remote system access. Although known as a threat simulation platform for the Red team (the team that performs security penetration testing), cracked versions of the software have been used by many as exploiters. different groups of hackers.

Favorite Features of Cobalt Strike:

- Reconnaissance
- Post Exploitation
- Attack Packages
- Covert Communication
- Browser Pivoting

4.3. What's new in our system

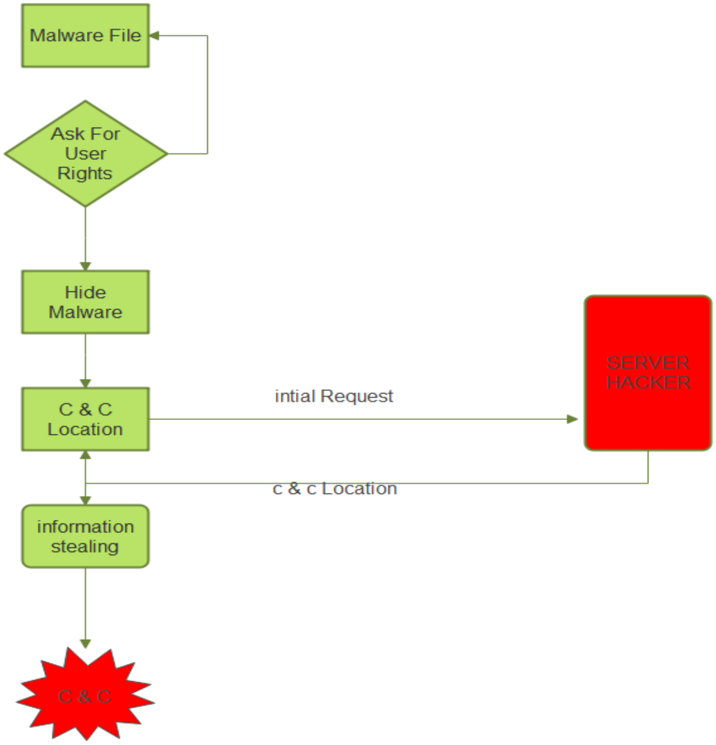


Fig 7. Malware in C2 flowchart

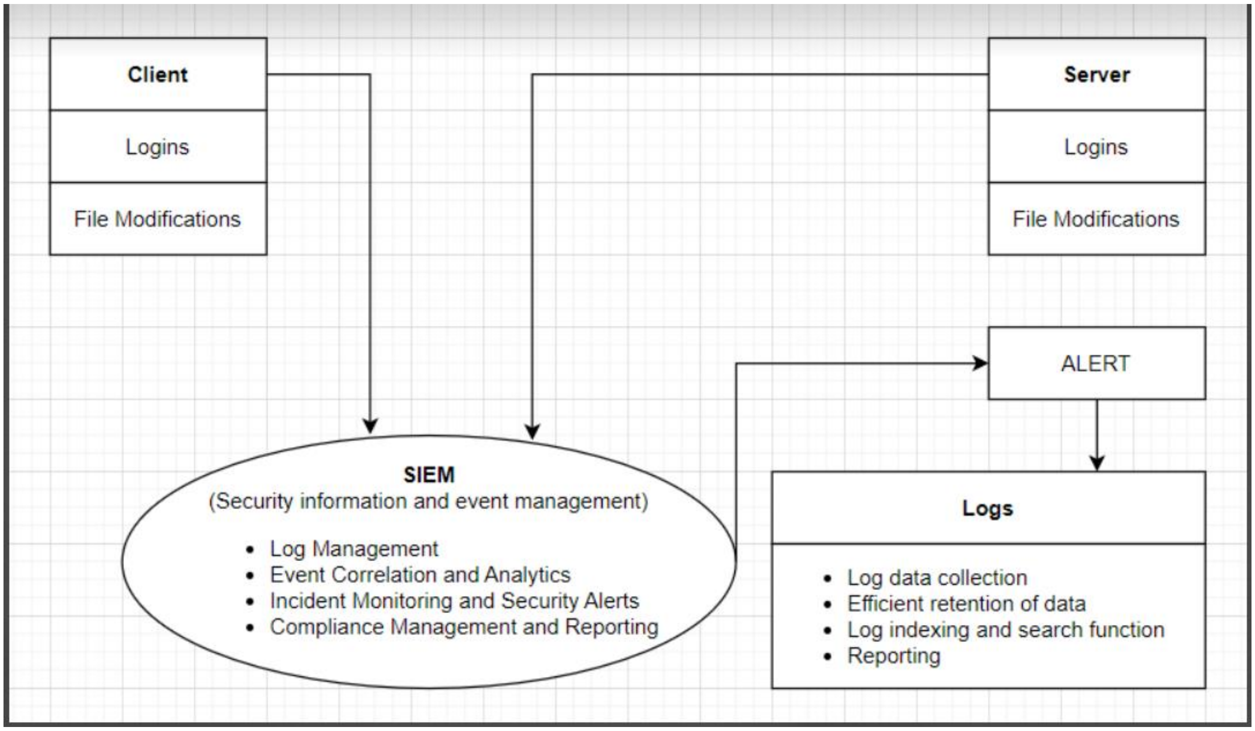

Client
Logins
File Modifications
Server
Logins
File Modifications
ALERT
SIEM
(Security information and event management)
Log Management
Event Correlation and Analytics
Incident Monitoring and Security Alerts
Compliance Management and Reporting
Logs
Log data collection
Efficient retention of data
Log indexing and search function
Reporting

Fig 8. Dataflow diagram for SIEM

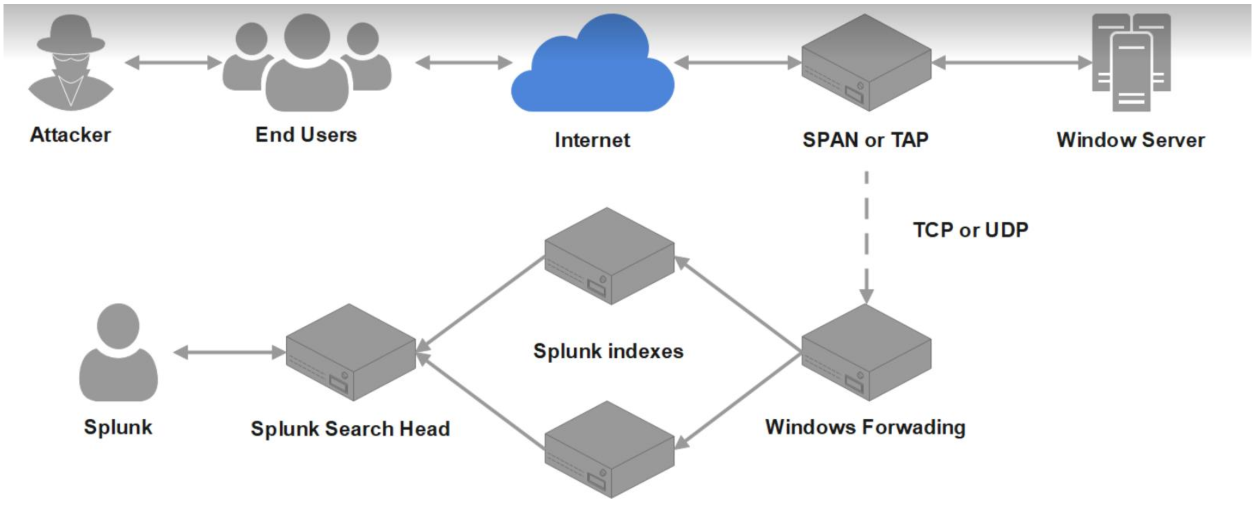


Fig 9. Our topology network

SIEM can be compared to a complex machine where the SIEM has a number of moving parts, each of which does a specific job, that need to work properly together, otherwise the whole system will faulty. There are variations on the standard SIEM, with additional specific sections, but a simple SIEM can be broken down into six separate parts or processes. These individual parts are the source device, log collection, log parsing/normalizing, rule engine, log storage, and event monitoring and retrieval. Each of these components can function independently of the others, but without them all working together, the whole SIEM will not function properly:

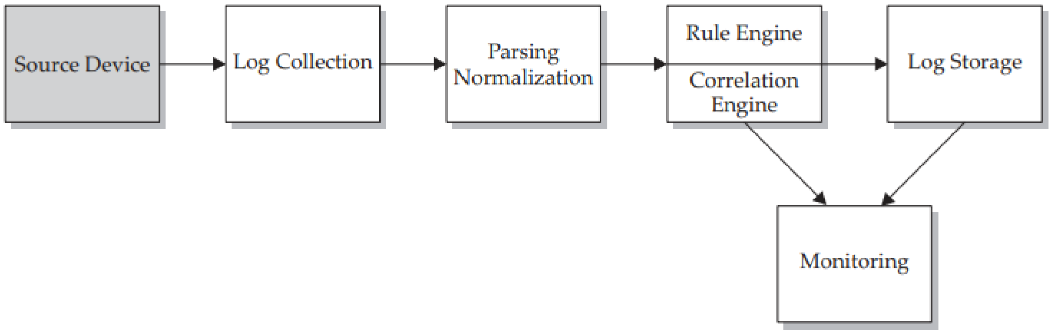


Fig 10: Source Device

A. Source Device

The first part of the SIEM is the source device that feeds the information into the SIEM. A source device is a device, application, or some other type of data that you want to log logs from, which you then store and process in your SIEM. The source device can be a physical device on your network, such as a router, switch, or some kind of server, but it can also be captured from an application or any data. other that you can obtain. The source device is not a real part of SIEM when looking at SIEM as an application you buy, but it is an important part of the entire SIEM process. All the systems on your network are there to process some kind of information for you and your users. Your web service, email, and directory servers all process information generated by your users. Without the source device and the information these devices generate, your SIEM is just a great app with no effect.

Understanding what's available in your environment will be important during your SIEM deployment. Know what sources you want to retrieve logs from in.

B. Log Collection

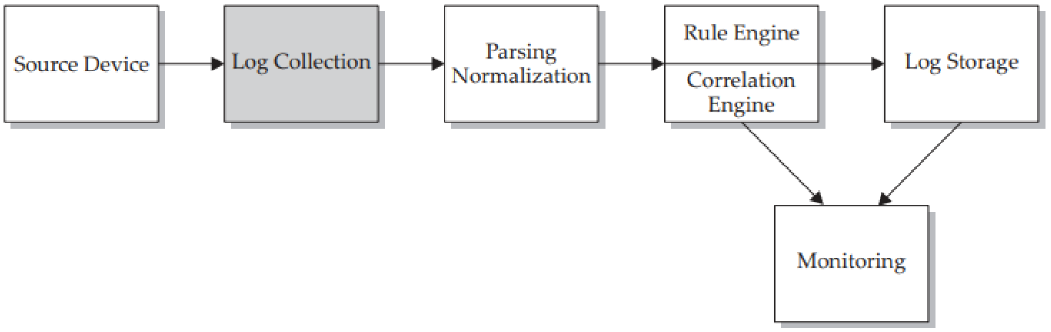


Fig 11: Log Collection

The next step in the device or application log flow is to somehow get all these different logs from their native devices to the SIEM. The actual mechanics of how the logs are retrieved vary depending on the specific SIEM that you are using, but at its most basic, the log collection processes can be broken down into two fundamental methods of collection: Either the source device sends its logs to the SIEM, which is called the push method, or the SIEM reaches out and retrieves the logs from the source device, which is called the pull method. Each of these methods has positives and negatives when used in your environment, but they both succeed in getting the data from the source device into the SIEM.s

C. Parsing Normalization

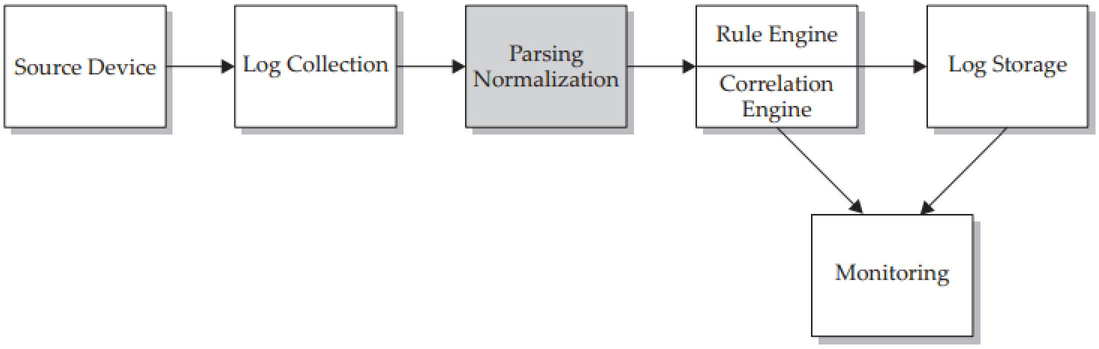


Fig 12: Parsing Normalization

Now that the logs from the multitude of devices and applications in your environment are being forwarded to the SIEM, what happens next? At this point, the logs are all still in their native format so you have not really gained anything, other than a centralized repository for your logs. What needs to happen in order to make these logs useful in the SIEM is to reformat them into a single standard format that is usable by the SIEM. The act of changing all these different types of logs into a single format is called normalization. Each type of SIEM will handle the act of normalization in different ways, but the end result is to have all the logs, no matter what type of device or manufacturer, look the same in the SIEM.

D. Rule Engine/ Correlation Engine

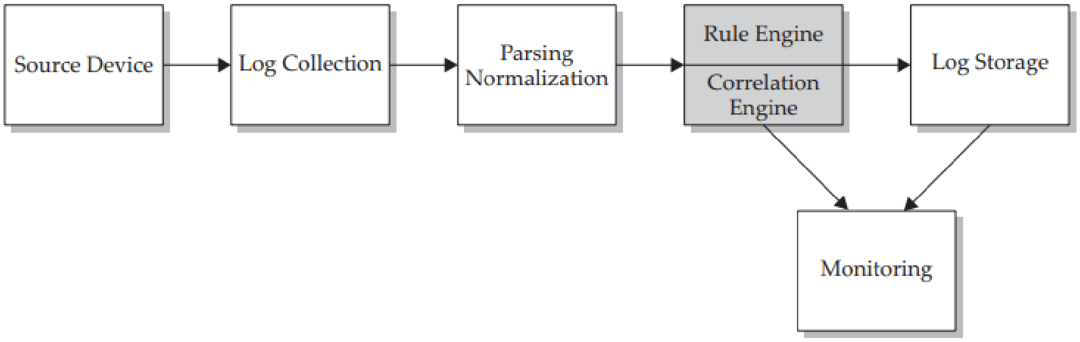


Fig 13: Rule Engine/ Correlation Engine

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 method of writing the SIEM rules usually starts off fairly simply, but can become extremely complex. You typically write the rules using a form of Boolean logic to determine if specific conditions are met and examine pattern matching within the data fields.

E. Log Storage

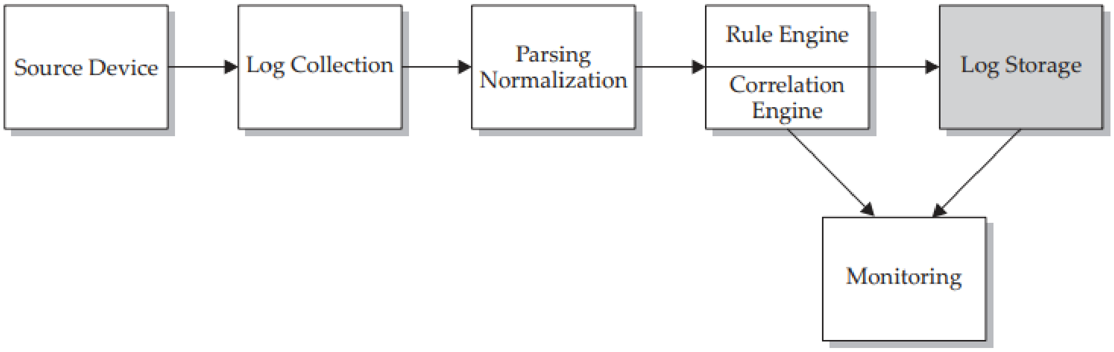


Fig 14: Log Storage

To work with the volumes of logs that come into the SIEM, you need a way to store them for retention purposes and historical queries. There are typically three ways that the SIEM can store its logs: in a database, a flat text file, or a binary file.

F. Monitoring

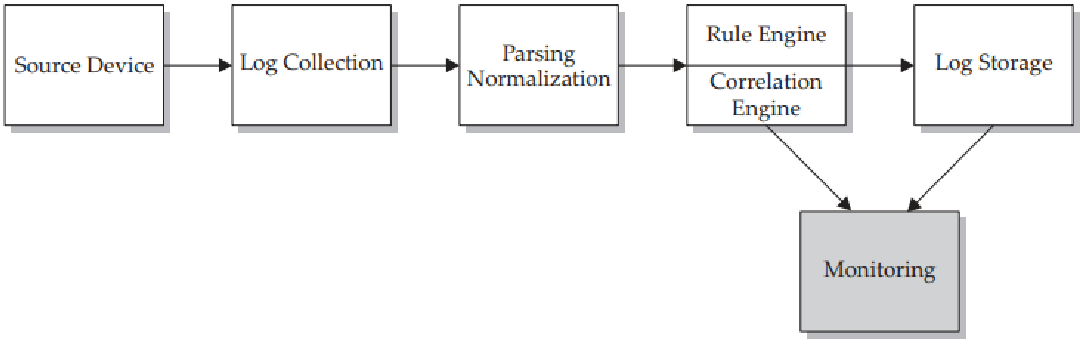


Fig 14: Monitoring

The final stage in the anatomy of a SIEM is the method of interacting with the logs stored in your SIEM. Once you have all the logs in the SIEM and the events have been processed, you need a way to do something useful with the information—otherwise the logs are just in the SIEM for storage purposes. A SIEM will have an interface console, which will either be web-based or application-based and loaded on your workstation.

Both interfaces will allow you to interact with the data stored in your SIEM. This console, be it web- or application-based, will also be used to manage your SIEM.

5. SIEM data processing techniques

SIEM brings together records and events from a variety of organizational sources. Each organization device generates an event. SIEM collects data from different sources around. It tries to collect data from an agent installed on the device. This is the most common source of data collection. It can also connect directly to devices using API calls or network protocols. It can also access log files directly from storage. It follows the Syslog format. Another way to collect data is through the event transfer protocol. Examples of such protocols are as follows- SNMP, Net flow or IPFIX. SIEM as a Data Collection Service and saves the data in a format that makes it easy to analyze it.

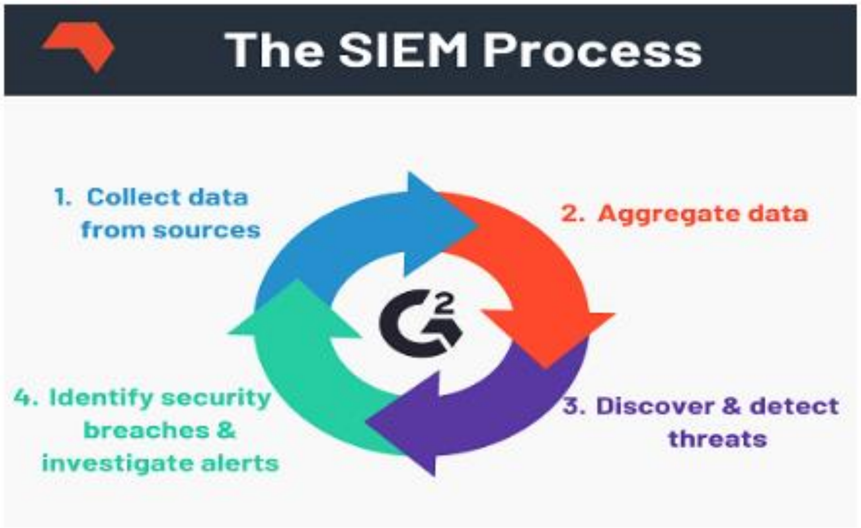

The SIEM Process
1. Collect data from sources
2. Aggregate data
3. Discover & detect threats
4. Identify security breaches & investigate alerts

Fig 10: SIEM Process

Steps to be followed in SIEM Process

- The first stage is to collect data from multiple surrounding sources.
- Then it combines all such collected data.
- In the next process, it starts examining the data to discover threats.
- Identify security breaches and alert organizations to such threats.

6. Conclusion

Choosing an attack model and a SIEM model for deployment in an environment may seem simple, however, given the different components, types, and classifications, such a decision is quite complex. There have been many attempts to categorize SIEM features as a means to facilitate the selection of better solutions. In this paper, we have classified SIEM according to the data processing techniques applied to the input information. Careful SIEM design can enable precise SIEM implementation. However, the practical advantages and limitations of each method, also discussed in this article, indicate that it is not possible to achieve complete security and different desired system characteristics by using only use some sort of implementation method.

7. References

https://www.comodo.com/what-is/the-siem-process.php

https://www.zscaler.com/blogs/security-research/android-malware-targeting-south-korean-mobile-users

https://www.cobaltstrike.com

https://www.pdfdrive.com/security-information-and-event-management-d185596433.html

https://www.scirp.org/journal/paperinformation.aspx?paperid=97094&fbclid=IwAR3vyJdTzlmkt32xeDfBdpn9K-6GUB3qKKFdvXuaHB1m6M_PwABcXuc-Hn0

https://www.logsign.com/blog/security-information-and-event-management-architecture/

https://attack.mitre.org/techniques/T1071/001/

https://attack.mitre.org/software/S0154/