Created by

Niraj Sangraula

CUID: 10176391

Cyber Threat Monitoring System- CybersecureUP

CybersecureUP
Make Security Better

Introduction

A Cyber Threat Monitoring System is a type of solution that monitors your network, infrastructure and so on to determine whether abnormal behavior such as security threats is taking place or not. Security threats refer to data exfiltration or such as DoS attacks. This system not only monitors and detects threats targeted at your organization but also can respond to those threats by sending real-time alerts and messages to administrators. But suppose there are low-level threats such as low-risk viruses. In that case, the system automatically does security patches on the vulnerability part in an attempt to remove it without human intervention. But later, this activity report is sent to the concerned authority. This system that we have made is named **"CybersecureUP."**

Infrastructure (Hardware, Software)

Our team has tested this system in a test environment, and it runs efficiently without error. But there are specific requirements that client infrastructure needs to follow to run efficiently. This system can only run-on windows and Linux but not macOS.

Hardware requirements

Linux x64

Microsoft Windows Server 2019

Software requirements

Splunk- Splunk Enterprise 8.0.0 and later

QRadar- IBM QRadar v7.2.5 or later

Supported browsers

Google Chrome 68 or later

Microsoft Edge 42 or later

CPU requirements

Can be operated in 32- and 64-bit machine

RAM and hard drive space requirements

OS	HDD (min)	RAM
Windows	6gb	16gb
Linux	4gb	16gb

Network requirements

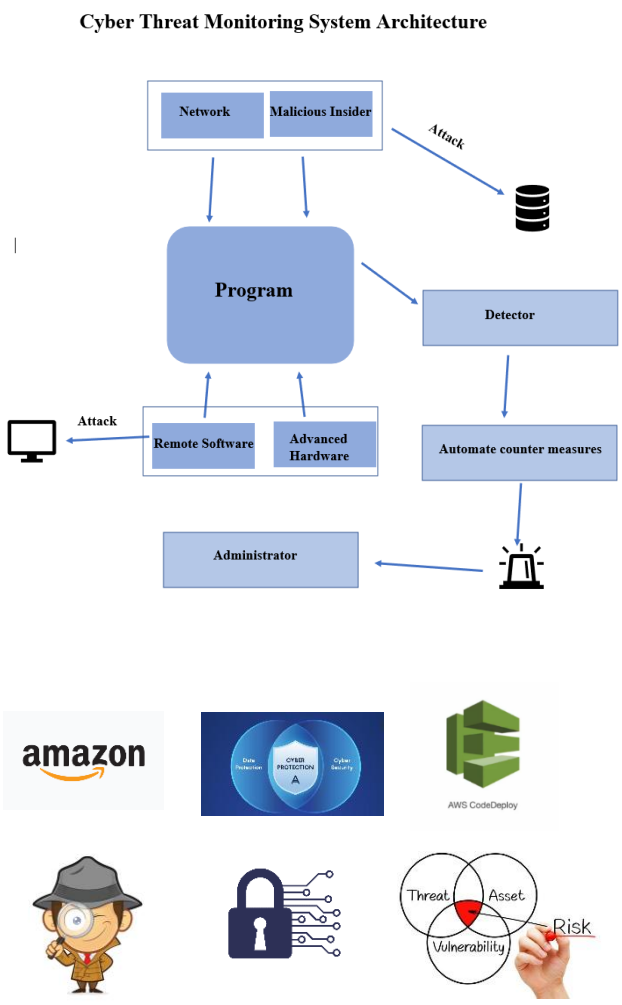
10 Mbps internet

Technology and Security

This system has been developed by our team using a different-different programming languages such as python, JavaScript, PHP and so on. Likewise, the MYSQL database is used for storing information. Furthermore, different technology has been integrated into this system, which has functionality.

- Login and Authentication Monitoring-
- Operating System Monitoring
- Server Monitoring
- Vulnerability Monitoring
- Email & Communications Monitoring
- Remote Access Monitoring

Architectural Diagram



Roles and Responsibility

System engineers

- identify system, implement the system.

System administrators

- Work on the system implemented by the system engineer, do upgrades.

Incident Responder

- The first person to be alerted, work on it to minimize the breach and damage.

Cyber security Analyst

- Implement robust plans and solutions, be informed about the new tools and technologies.

SOC Analyst

- Suppose the threat is more significant and can't be solved by the incident responder. In that case, SOC analysts are informed.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

Identify	Assets are identified which can be systems, data, applications and so on.
Protect	Assets are protected through encryption, backing up the data, training employees, managing endpoints, access control.
Detect	log files will be checked to find malware.
Respond	Responding to minimize the threat by changing passwords, locking all admin accounts.
Recover	lost data is recovered, restore systems and restore application.

The process

CybersecureUP will be deployed on the on-premise server of Up Link company using Amazon **AWS CodeDeploy**. The process of how the system **(CybersecureUP)** works will be discussed in this section taking its architecture as a medium. We can use a basic threat model to identify all the potential attackers and threats. Following this threat model, there are four types of attackers: Network, malicious insider, remote software and advanced hardware. Network-type attackers conduct man-in-the-middle attacks to hijack communication between two parties communicating over a network. A malicious insider is an attacker working inside the company and can be regarded as an insider threat and has unauthentic access to your network. Remote software users are attackers who breach security by making malicious scripts and doing other types of security attacks to gain control over the device or network. Advanced hardware attacker generally carries out their attacks using social engineering to take over a hardware device of a company to bypass it. These all types of attackers can be detected using our system using various techniques mentioned in the previous section. After detection of threats, the system countermeasures them using automation tools. After the countermeasures are applied, the report is sent to an administrator to remove the threat successfully.

Task

The tasks that can be performed by this system and those tasks that the company should carry out are:

- Update the old version of hardware and software.
- Give employee training on how to use this system and give access according to roles.
- Detect threat and provides countermeasures to solve them completely.
- Alert the administrator or responsible authority immediately if a high level or above threat is detected; the system can't solve high-level threat completely.
- Check known threats or data breach scenarios that occurred with other companies throughout history and provide the developer's implementation solution on the potential risk of not suffering from the same fate.

Structure

Tier 1	Tier 2	Tier 3
Low Access Can view Help desk support	Medium Access Can make small changes System Admins	High Access Can make big changes System engineers, manager

GDPR (GENERAL DATA PROTECTION REGULATION) and ELECTRONIC TRANSACTION ACT 2063 (ETA) compliance

- GDPR Article 5 (1) (f)
  On individual security
- GDPR Article 12
  On informing the individual
- GDPR Article 5 (1) (a)
  On transparency, fairness and law.
- Article 44 of **ETA**, related to Pirate, Destroy or Alter computer source code.

Additional Description

Introduction

Furthermore, we can only increase our chances of quickly detecting threats and mitigating them efficiently by integrating many defensive methods within the cyber threat monitoring system. If there are known threats, there are high chances of mitigating them through the system, but in the case of unknown threats, it isn't easy. So, to minimize the worst-case scenarios, many functions are in-built into the application.

Infrastructure (Hardware, Software)

This infrastructure hasn't been selected randomly by us. Instead, we have followed the Kaspersky CyberTrace model, which is also a SIEM solution. Kaspersky is an authentic company that has been providing this type of solution developed over the last decade.

Technology and Security

In the login and authentication monitoring section, the CybersecureUP detects whether or not unauthenticated login attempts have been made from unknown places. In vulnerability monitoring, the system detects whether or not vulnerable apps are running on the company network. In operating system monitoring, CybersecureUP sees whether or not suspicious activity is happening on the computers connected to the company network. This also applies to BYOD devices. So, all mentioned technology in the poster has its own function. They not only detect those threats but also solve them to save the company from data breach scenarios and protect the company hardware, software, employee and architecture.

Roles and Responsibility

System engineers

identify system, make a blueprint and design the system, implement the system

System administrators

Work on the system implemented by the system engineer, do upgrades, maintain the system and provides support to other departments on how to use the system.

Incident Responder

The first person to be alerted by the system if a security breach occurs, work on it to minimize the breach and damage, locate the source of the attack and inform higher up.

Cyber security Analyst

Implement robust plans and solutions if the attacker carries out a successful attack. Be informed about the new tools and technologies to create a strong defense for the company.

SOC Analyst

Suppose the threat is more significant and can't be solved by the incident responder. In that case, SOC analysts are informed and provide remedy approaches to minimize the damage, monitoring, and vulnerability management. (SANS, n.d.).

GDPR (GENERAL DATA PROTECTION REGULATION) and ELECTRONIC TRANSACTION ACT 2063 (ETA) compliance

Since the employee is one of the significant insider threats that can damage the company, they need to be monitored using the threat monitoring system. So, if any compromise in their privacy is made, then the company is subjected to GDPR though which the company might need to suffer from substantial financial losses. So, GDPR guidelines are followed strictly by the company. These are rights provided to employees or individuals concerning their privacy through GDPR:

1. GDPR Article 5 (1) (f) ensures that when the company processes data, it should be processed in such a manner that it shouldn't neglect individual security.
2. GDPR Article 12 ensures that whenever individual data is being examined, they should be informed.
3. GDPR Article 5 (1) (a) ensures that the data collected should be processed by the company in a manner that shouldn't neglect transparency, fairness and law.

Not only employee company can also benefit from compliances. Such compliance is **Article 44 of ETA, related to Pirate, Destroy or Alter computer source code.** This article says that if an individual or company is found to be pirating, destroying and modifying source code from any computer program or computer network, they are liable to imprisonment and fine. The imprisonment is three years, and the fine is 200 thousand rupees.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

All organizations, big or trim, need a specific framework or guideline to protect their assets from modern security attacks. This is where the NIST cybersecurity framework comes in. Through this framework, the organization can efficiently identify and detect cyber threats, provide security measures, and respond to prevent security incidents.

This framework has five core functions they are:

Identify: In this stage, it is identified what assets of the company will be protected. These assets can be systems, data, applications and so on, which are essential for the function of an organization.

Protect: After identifying, the assets will be protected by determining their importance level. The assets are protected through encryption, backing up the data, training employees, managing endpoints, access control, and so on.

Detect: In this stage, log files will be checked to find malware. If malware is detected, then mitigating approaches are initiated.

Respond: If a successful attack is carried out on the organization's network, it needs to be responded to minimize the threat. This can be done by changing passwords, locking all admin accounts or even shutting down the network.

Recover: In this last stage, according to the importance level, the lost data is recovered, restore systems and restore application. After all, this is done eliminate undetected malware that survived from the respond phase from the system completely.

References

20 Coolest Cyber Security Careers | SANS Institute. Sans.org. Retrieved 1 July 2022, from https://www.sans.org/cybersecurity-careers/20-coolest-cyber-security-careers/.

Bharathy, A. (2017). A Hybrid Intrusion Detection System Cascading Support Vector Machine and Fuzzy Logic. *Researchgate*, *1*, 104-109. https://doi.org/10.5829/idosi.wasj.2017.104.109

Callahan, D. (2022). Get Started with the NIST Cybersecurity Framework [Blog]. Retrieved 3 July 2022, from https://cgnet.com/blog/get-started-with-nist-cybersecurity-framework/.

Cyber Security Monitoring. Atlant Security. Retrieved 10 July 2022, from https://atlantsecurity.com/cyber-security-monitoring/.

Dhamankar, R. (2021). *5 steps to implement threat modeling for incident response*. SearchSecurity. Retrieved 15 July 2022, from https://www.techtarget.com/searchsecurity/post/5-steps-to-implement-threat-modeling-for-incident-response.

General Data Protection Regulation (GDPR) – Official Legal Text. General Data Protection Regulation (GDPR). Retrieved 21 July 2022, from https://gdpr-info.eu/.

Hardware and software requirements. Support.kaspersky.com. Retrieved 23 July 2022, from https://support.kaspersky.com/CyberTrace/1.0/en-US/162509.htm.

Lord, N. (2020). What is Threat Monitoring? [Blog]. Retrieved 25 July 2022, from https://digitalguardian.com/blog/what-threat-monitoring.

Technology, D. *Resources || Department Of Information Technology || ETA*. Doit.gov.np. Retrieved 30 July 2022, from https://doit.gov.np/en/resources/2.