MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Govt. of India)

NAAC Accredited A++ with Grade

PROJECT REPORT

ON :

CUSTOMIZATION OF-
CYBER SECURITY TOOL - SIEM

Submitted By:

Anshita Singh

(0901CA221015)

Industry Mentor:

Mr. Ankush Vilhekar, Senior Manager – Security Administration,

India Post Payments Bank, New Delhi

Faculty Mentor:

Dr. R.S. Jadon (Professor)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE
Gwalior – 474005(MP) estd.1957

January – June 2024

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Govt. of India)

NAAC Accredited A++ with Grade

PROJECT REPORT

ON :

CUSTOMIZATION OF -
CYBER SECURITY TOOL - SIEM

A Project report submitted in partial fulfillment of the requirement for the degree

Submitted By:

Anshita Singh

(0901CA221015)

Industry Mentor:

Mr. Ankush Vilhekar, Senior Manager – Security Administration,

India Post Payments Bank, New Delhi

Faculty Mentor:

Dr. R.S. Jadon (Professor)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

Gwalior – 474005(MP) estd.1957

January – June 2024

इंडिया पोस्ट पेमेंट्स बैंक India Post Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

TO WHOMSOEVER IT MAY CONCERN

To,

Ms. Anshita Singh,

MITS Gwalior,

Subject: Completion of Internship,

Reference: Internship Completion Certificate dated 12.03.2024 issued by the India Post Payments Bank,

In connection with subject noted matter, on the specific request of the intern, this internship, which aimed in developing a customized software for the security of the system, was extended till April 15, 2024 under the guidance of Sh. Neeraj Kumar Jha, Chief Human Resource Officer and the same was completed on 15.04.2024.

With best wishes,

Neer Kumar Jha
22/4/24

(Neeraj Kumar Jha),
Chief Human Resource Officer,
India Post Payments Bank

नीरज कुमार झा
NEERAJ KUMAR JHA (I.Po.S)
मुख्य मानव संसाधन अधिकारी
Chief HR Officer
इंडिया पोस्ट पेमेंट्स बैंक लिमिटेड
India Post Payments Bank Ltd.

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Govt. of India)

NAAC Accredited A++ with Grade

CERTIFICATE

This is certify that **Anshita Singh (0901CA221015)** has submitted the project report titled **cyber security tools** under the mentorship of **Mr. Ankush Vilhekar,** (Senior Manager at Security Administration), in partial fulfilment for the requirement for the award of degree of **Master in Computer Applications** in Computer Science and Engineering from **Madhav Institute of Technology and Science, Gwalior**.

26/4/24

Dr. R.S. Jadon
(Professor and Project Coordinator)
Computer Science and Engineering

26/4/24

Dr. Manish Dixit
(Professor and Head)
Computer Science andEngineering

Dr. Manish Dixit
Professor & HOD
Department of CSE
M.I.T.S. Gwalior

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Govt. of India)

NAAC Accredited A++ with Grade

DECLARATION

I hereby declare that the work being presented in this project report, for the partial fulfilment of requirement for the degree of Master of Computer Application in Computer Science and Engineering at **Madhav Institute of Technology & Science, Gwalior** is an authenticated and original record of my work under the mentorship of **Mr. Ankush Vilhekar (senior manager – security administration)**, New Delhi.

I declare that I have not submitted the matter embodied in this report for the award of any degree or diploma anywhere else.

Anshita Singh

Anshita Singh

0901CA221015

II Year (IV SEM)

2022-2024

Master of Computer Application,

Computer Science and Engineering

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Govt. of India)

NAAC Accredited A++ with Grade

ACKNOWLEDGEMENT

The full semester project has proved to be pivotal to my career. I am thankful to my institute, **Madhav Institute of Technology and Science** to allow me to continue my disciplinary project. I extend my gratitude to the Director of the institute, **Dr. R. K. Pandit** and Dean Academics, **Dr. Manjaree Pandit** for this.

I would sincerely like to thank my department, **Department of Computer Science and Engineering**, for allowing me to explore this project. I humbly thank **Dr. Manish Dixit**, Professor and Head, Department of Computer Science and Engineering, for his continued support during the course of this engagement, which eased the process and formalities involved.

I am extremely grateful to **India Post Payment Bank**, New Delhi for providing me this opportunity to undertake this project training and allowing me to apply the knowledge gained in the classroom to real-world scenarios.

I would like to express my heartfelt gratitude to **Mr. Ankush Vilhekar**, Senior Manager-Security Administration, New Delhi for their valuable guidance, unwavering support, and motivation throughout the development of the cyber security tools project.

I am very thankful for my project guide **Shankar sir,** who provided me with constant support and encouragement throughout the project training. His timely advice and suggestions have been very helpful in shaping the direction of the project.

I am sincerely thankful to my faculty coordinator. I am grateful to the guidance of **Dr. R.S. Jadon**, (Professor), Computer Science and Engineering, for her continued support and guidance throughout the project. I am also very thankful to the faculty and staff of the department.

Anshita Singh

Anshita Singh
0901CA221015

2022-2024

Master of Computer Application

Computer Science and Engineering

ABSTRACT

We are in the age of any time and anywhere access to banking. Technology innovation has moved banking to desktops, laptops, tablets and mobiles. The customer has grabbed banking in the user's palm. Yet, there has been issues with the new era digital banking because of the increasing trend in failed or fraudulent transactions. A few of the recent incidents in the banking sector have shaken the confidence. Banks have suffered financial losses on a few occasions, but their reputation loss is a matter of greater concern. The trust the customers need to have in banks for parking in their hard-earned funds is critical for banking. After all, banking is based on trust and it is the responsibility of the banks too. So to avoid such activities banks have moved towards adopting the SIEM under(Security Information and Event Management) ISOC (Information Security Operation Centre); a superstructure that identifies abnormalities early and alerts stakeholders immediately.

This project aims to improve the efficiency and transparency of complaint-handling procedures, there by providing a better experience to customers while using digital banking services. Additionally, the software provides an opportunity for the banks to improve their services and address the grievances in a timely and effective manner sometimes even before the occurrence of the issue.

This project takes care of the security aspect by ensuring that only authenticated users can access the system. It provides a secure login for users to ensure data confidentiality and user privacy. Users are authenticated by cross-checking the details submitted to the bank hence a mutual trust stays between the user and the bank.

Trend Micro's Deep Discovery Inspector etc are the types of device product which gets activated when traffic reaches DDI, we receive an alert. It detects malicious content, communications, and behaviour that could point to advanced malware or attacker activity at any point in the attack process. Thus, when malicious traffic reaches Trend Micro's DDI, an alert titled "High Priority Alert on DDI" is generated based on a high level of severity.

Therefore, we have worked on the operational and customisation aspect of software and also developed an user friendly API for same. The most innovative contribution is implementation of API looking for vulnerabilities and authenticity of IP addresses. Fetch these to the system which in turn initiates the protective action.

सार

हम किसी भी समय और कहीं भी बैंकिंग तक पहुंच के युग में हैं। प्रौद्योगिकी नवाचार ने बैंकिंग को डेस्कटॉप, लैपटॉप, टैबलेट और मोबाइल पर स्थानांतरित कर दिया है। ग्राहक ने उपयोगकर्ता की हथेली में बैंकिंग पकड़ ली है। फिर भी, विफल या धोखाधड़ी वाले लेनदेन की बढ़ती प्रवृत्ति के कारण नए युग की डिजिटल बैंकिंग में कुछ समस्याएं आई हैं। बैंकिंग क्षेत्र में हाल की कुछ घटनाओं ने विश्वास को हिला दिया है। कुछ मौकों पर बैंकों को वित्तीय नुकसान हुआ है, लेकिन उनकी प्रतिष्ठा में गिरावट अधिक चिंता का विषय है। ग्राहकों को अपनी मेहनत की कमाई को जमा करने के लिए बैंकों पर जो भरोसा होना चाहिए, वह बैंकिंग के लिए महत्वपूर्ण है। आख़िरकार, बैंकिंग विश्वास पर आधारित है और यह बैंकों की ज़िम्मेदारी भी है। इसलिए ऐसी गतिविधियों से बचने के लिए बैंक (सुरक्षा सूचना और इवेंट प्रबंधन) आईएसओसी (सूचना सुरक्षा संचालन केंद्र) के तहत एसआईईएम को अपनाने की ओर बढ़ गए हैं; एक अधिरचना जो असामान्यताओं की शीघ्र पहचान करती है और हितधारकों को तुरंत सचेत करती है।

इस परियोजना का उद्देश्य डिजिटल बैंकिंग सेवाओं का उपयोग करते समय ग्राहकों को बेहतर अनुभव प्रदान करके शिकायत-निपटान प्रक्रियाओं की दक्षता और पारदर्शिता में सुधार करना है। इसके अतिरिक्त, सॉफ्टवेयर बैंकों को अपनी सेवाओं में सुधार करने और कभी-कभी समस्या उत्पन्न होने से पहले भी समय पर और प्रभावी तरीके से शिकायतों का समाधान करने का अवसर प्रदान करता है।

यह प्रोजेक्ट यह सुनिश्चित करके सुरक्षा पहलू का ध्यान रखता है कि केवल प्रमाणित उपयोगकर्ता ही सिस्टम तक पहुंच सकें। यह डेटा गोपनीयता और उपयोगकर्ता गोपनीयता सुनिश्चित करने के लिए उपयोगकर्ताओं को एक सुरक्षित लॉगिन प्रदान करता है। उपयोगकर्ताओं को बैंक में जमा किए गए विवरणों को क्रॉस-चेक करके प्रमाणित किया जाता है, इसलिए उपयोगकर्ता और बैंक के बीच आपसी विश्वास बना रहता है।

ट्रेंड माइक्रो के डीप डिस्कवरी इंस्पेक्टर आदि डिवाइस उत्पाद के प्रकार हैं जो ट्रैफिक डीडीआई तक पहुंचने पर सक्रिय हो जाते हैं, हमें एक अलर्ट प्राप्त होता है। यह दुर्भावनापूर्ण सामग्री, संचार और व्यवहार का पता लगाता है जो हमले की प्रक्रिया में किसी भी बिंदु पर उन्नत मैलवेयर या हमलावर गतिविधि की ओर इशारा कर सकता है। इस प्रकार, जब दुर्भावनापूर्ण ट्रैफ़िक ट्रेंड माइक्रो के डीडीआई तक पहुंचता है, तो उच्च स्तर की गंभीरता के आधार पर "डीडीआई पर उच्च प्राथमिकता अलर्ट" नामक एक अलर्ट उत्पन्न होता है।

इसलिए, हमने सॉफ्टवेयर के परिचालन और अनुकूलन पहलू पर काम किया है और इसके लिए एक उपयोगकर्ता के अनुकूल एपीआई भी विकसित किया है। सबसे नवीन योगदान आईपी पते की कमजोरियों और प्रामाणिकता की तलाश में एपीआई का कार्यान्वयन है। इन्हें सिस्टम में लाएँ जो बदले में सुरक्षात्मक कार्रवाई शुरू करता है।

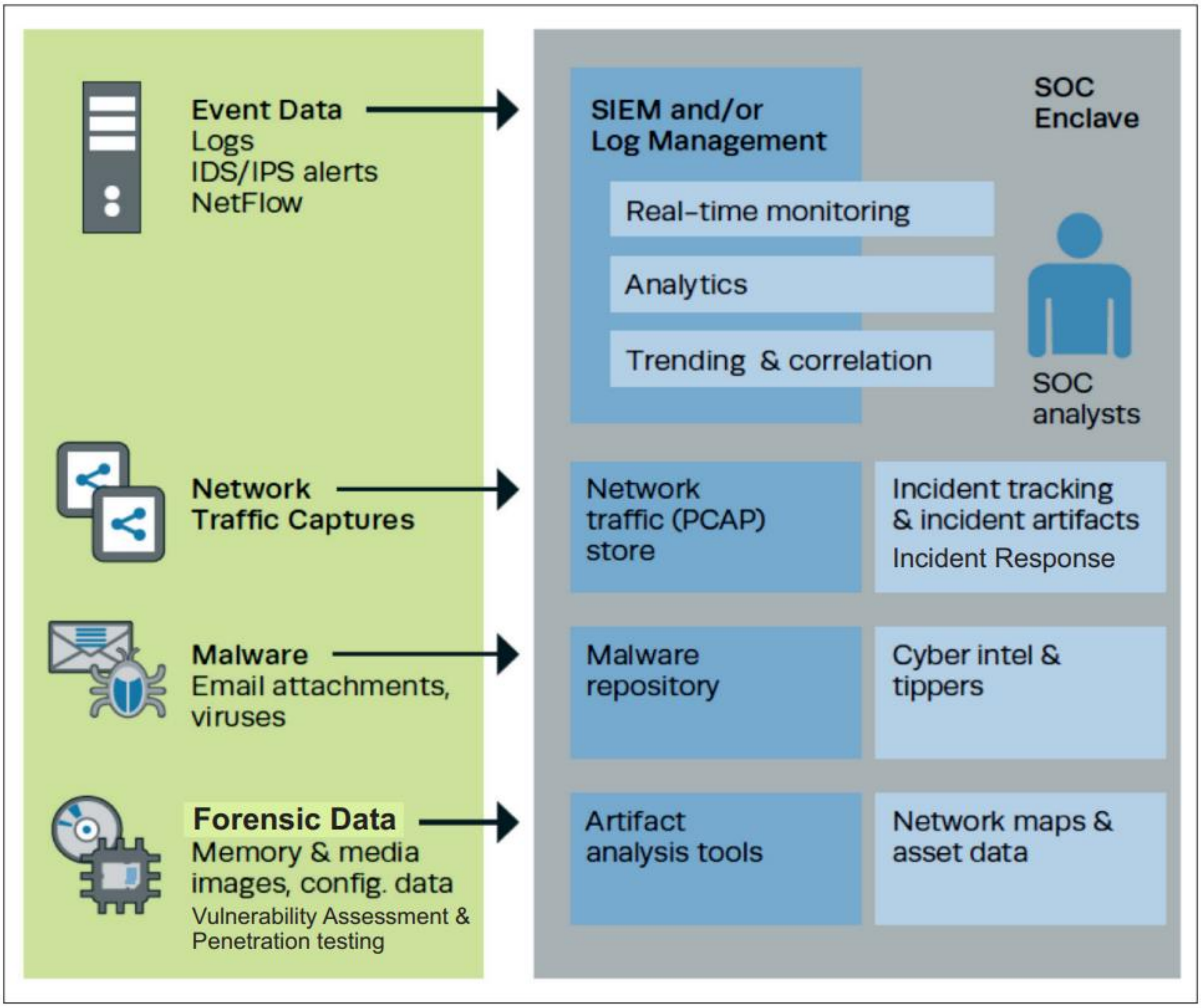
TABLE OF CONTENTS

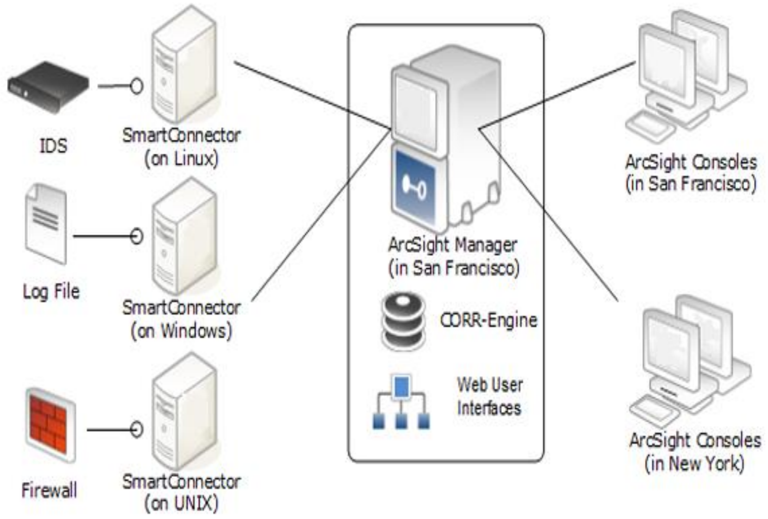
1. INTRODUCTION

Information Security Operations Center (ISOC) – "The ISOC is responsible for monitoring, detecting, and isolating incidents and the management of the organisation's security products, network devices, end-user devices, and systems. This function is performed seven days a week, 24 hours per day. The ISOC is the primary location of the staff and the systems dedicated for this function," defines Wikipedia

The recent attacks prove that financial systems deploying defensive technologies like perimeter security and encryption, etc., are not sufficient and one needs to constantly monitor the security. Security is not a product that can be deployed and forgotten, rather it is a process that needs to be continuous.

The picture below shows the security features that became part of the overall IT security of a matured business organization. This section provides insight into how each of the security-specific points found their place in the organization. The Logical Security framework presents the defence-in-depth, layered approach to security. It is broken down into five main groups: **Operations, data, hosts, network, identity and access control.**

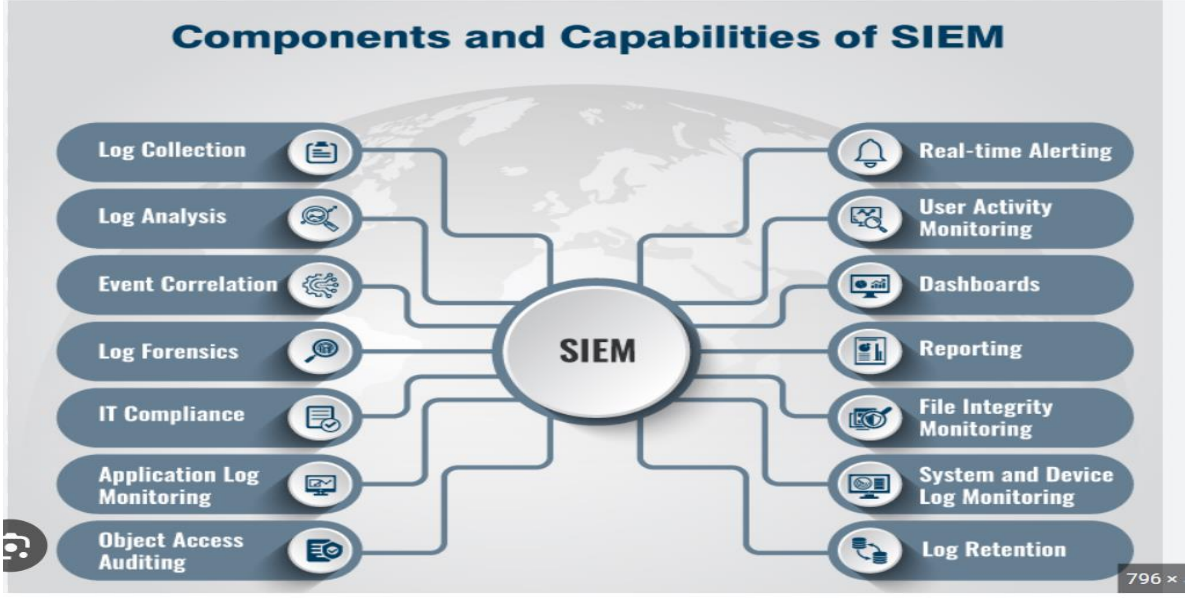



IDS
SmartConnector (on Linux)
Log File
SmartConnector (on Windows)
Firewall
SmartConnector (on UNIX)
ArcSight Manager (in San Francisco)
CORR-Engine
Web User Interfaces
ArcSight Consoles (in San Francisco)
ArcSight Consoles (in New York)

Data collection - Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as Event Collectors or Flow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format. The core functionality of SIEM is focused on event data collection, and flow collection. Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs. Flow data is network activity information or session information between two hosts on a network, which translates in to flow records. It translates or normalizes raw data in to IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the Incident Forensics component.

Data processing- After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage. Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Data searches - In the third or top layer, data that is collected and processed by is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the Console. In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance. In distributed environments, the Console does not perform event and flow processing, or storage. Instead, the Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.



1.1 Recognition of need

The issues with the new era of digital banking because of the increasing trend in failed or fraudulent transactions. A few of the recent incidents in the banking sector have shaken her confidence. Banks have suffered financial losses on a few occasions, but their reputations on loss are a matter of greater concern. The trust the customers need to have in banks for parking with their hard-earned funds is crucial for banking. After all, banking is based on trust. It is the responsibility of the banks to put in place all necessary infrastructure and systems to ensure that digital banking is safe and secure. They have to ensure confidentiality, integrity and availability, the three key requirements of secured banking.

1.2 Problem Identification:

There are a lot of viruses present in the environment at various IP protocol. But they are not interconnected and hence attack on any one part of the system goes unrecognised. Therefore there is immediate need to monitor the real time functioning of logs. Since SIEM () under ISOC is responsible for real time tracking and monitoring of the security of various layers of network and devices and ISOC being a team of experts monitoring the real time security plays a crucial role. Therefore, by integrating various security devices and connecting them with SIEM under ISOC will lead to the effective solution for banking related safety of various network layers and devices.

1.3 Strategy for determining information:

a. **Research:** a research over the various safety tools were undertaken from the research paper available with the bank.

b. **Application based study:** a detailed analysis of various logs was performed to understand the security issues associated on each level of network.

c. **Acknowledgement of tools:** a set of tools such as Antivirus *trend* etc, were chosen for performing the study.

1.4 Advantages of our project:

Any virus or malicious activity performed in any device and at any network level or at host or server can be very efficiently and effectively be identified and acknowledged by the ISOC by using the SIEM. It is because by coordinating the logs with the security tools and then these with the SIEM helps the ISOC team to very efficiently track the malfunctioning performed as the ISOC team monitors the security activity 24x7.

Chapter 2. FEASIBILITY STUDY

A. Economic feasibility :

The Economic feasibility of the cyber security tools project is quite favourable. Since it is web based system, it can be accessed by both students and department personnel from anywhere and anytime, thus providing a great deal of convenience. Additionally, the cost of the system is relatively low, as it requires few members such as engineers, data analyst, and certain hardware and software tools such as end user devices, servers , network equipment, or other security system firewalls and antivirus.

PERSONAL			
Serial No.	Specification	Description	Amount
1	System Analyst		80000
2	Programmer	40 days per man (in 2 months)	15000
3	Database Specialist	16 (in 2 months)	7000
OTHER EXPENSE			
1	Electricity	For systems	400 unit @8rs /unit = 3200
2	Stationary	For documentations	3000
3	Workspace facilities	Electricity. tables , chairs	10000
4	Systems	For process	30000
Total			**145200**

B. Technical Feasibility:

The proposed system is build on User and Entity behaviour Analytics (UEBA) and security Orchestration and automation response (SOAR) technology which is a popular and widely used technology for building modern web applications. It provides developers with a comprehensive set of tools and libraries for building scalable and robust applications. Relational database are the databases that are used which provide high -performance data storage and retrieval capabilities. While Java is a web application framework that provides developers with necessary tools to build web applications.

These technologies are widely used and have excellent community support, making it easy to find resources and documentation to solve any technical challenges that may arise during development.
In conclusion, the cyber security tools project build using Java is technically feasible and provides a reliable and secure platform for users to manage their security. The use of modern web development technologies and libraries made its development, deployments and working easier.

System Requirements

ThehardwarerequirementsforESM7.5areasfollows

	Maximum	Mid - range	High performance
Processors	8 Cores	32 Cores	40 cores
Memory	48 GB RAM	192 GB RAM	512 GBRAM
Hard disk	Six 600 G disks (1.5 Tb) (B 10000 RPM	201 TB disks (10 Tb) 15000 rpm	12 TB Solid state

System Storage- non – event storage, for example resources, trends, amd lists.
Event storage- storage for events
Event archive size- archive for online events

	Recommended	Manimum	Maximum
System storage size	The default about one sixth of usable space, from atleast 3 GB a maximum of 15000 Gb during installation, it is recommended that you can accept the default.	3 GB	1500 GB
Event storage size	Specify about two thirds of the usable space shown during installation	10 GB	12 TB
Event archive size	You may specify the remaining the space after the systemand storage have been allocated	1 GB	Limit is predicated on your file system size.

Final Cost of our Project = 145200

Total Completion time of our Project = 2 months

C. Behavioural Feasibility :

Behavioural feasibility refers to the extent to which the system is accepted and used by its intended users. In the case of the Complaint Management System, it is designed to cater to the needs of Bank users and department personnel. The system is user-friendly and intuitive, which means that users will find it easy to navigate and use. Additionally, the system is designed to provide a quick and efficient resolution of complaints related to various issues.

The system is also designed to maintain transparency and provide regular updates to users regarding the status of their complaints. This helps in building trust and confidence among the users, which is critical for the success of any system.

Moreover, the system provides a secure login process mechanism. This ensures that only authorized users can access the system, thus ensuring data privacy and security. Additionally, the system provides an option to view their profile details, which is helpful for users to check and validate their information on the system.

Overall, the cyber security tools is highly feasible from a behavioral perspective as it addresses the needs of its users while providing a secure and user-friendly interface.

The project aims at maximizing the security and data breach along with user authentication . This is intended to overcome the threats that go unnoticed . The user can easily use the system software as the software does not need any special guidance.

The following measures are being taken to ensure the same:

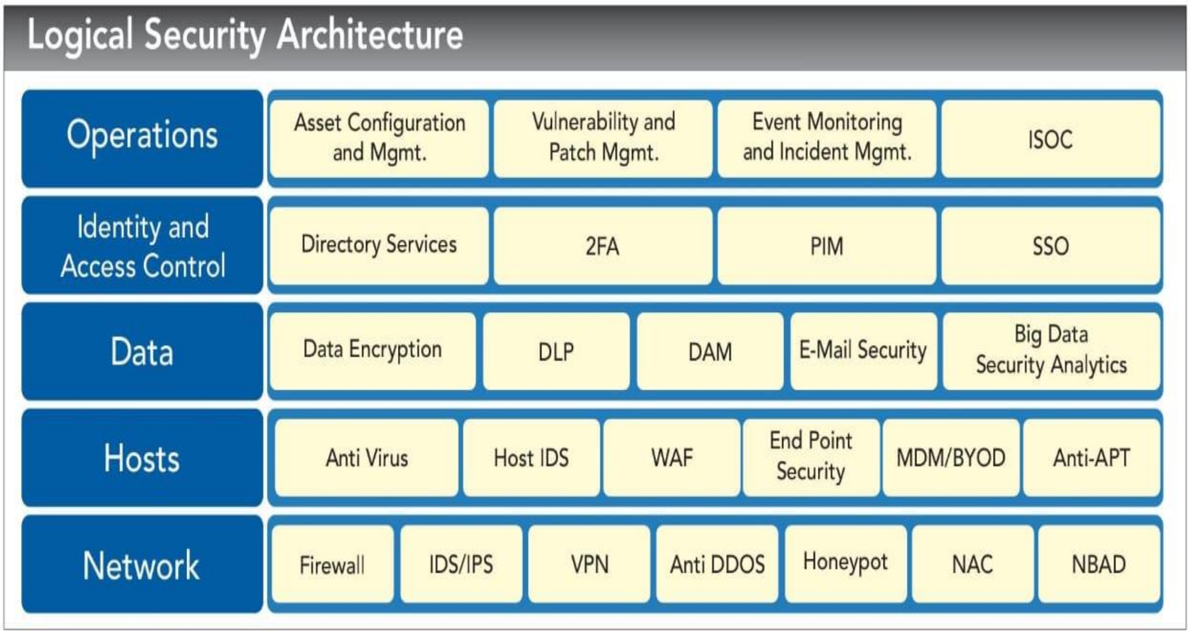
i. The platform will be as much easy to use as possible, convenient, and provide value to users and will be also addressing any concerns that users may have about security, privacy, and trust.

ii. To maintain user engagement, system software can encourage user for participation and foster a sense of community among users. This could include features such as user reviews and ratings, forums for discussion, and social media integration.

iii. It is receptive to user feedback and be willing to make changes and improvements based on user suggestions. This can help to build trust and improve safety concerns .

iv. We would be providing user training modules/sessions so as to facilitate easier adaptation of the system.

1. System Analysis



Logical Security Architecture

Operations	Asset Configuration and Mgmt.	Vulnerability and Patch Mgmt.	Event Monitoring and Incident Mgmt.	ISOC			
Identity and Access Control	Directory Services	2FA	PIM	SSO			
Data	Data Encryption	DLP	DAM	E-Mail Security	Big Data Security Analytics		
Hosts	Anti Virus	Host IDS	WAF	End Point Security	MDM/BYOD	Anti-APT	
Network	Firewall	IDS/IPS	VPN	Anti DDOS	Honeypot	NAC	NBAD

The entire system consists of 5 layers starting from Network, Hosts, Data, Identity and Access Control, and ending on Operations. They are also further classified into the various subcategories as mentioned in above figure.

1. **Network Security:** Network security is a basic necessity today. Network Security Appliances help in protecting the computer systems and other IT infrastructure inside the network from unwanted intrusions or attacks**.**

   1.1 Firewall : Network security started its journey with basic firewalls and is now capable of filtering based on content of the packet instead of just packet headers. Not able to go beyond the layer 4 intelligence of TCP/IP stack, firewalls just remained as main entrance security gateways in the entire enterprise security space.

   1.2 IDS/IPS: Intrusion detection and prevention systems detect/prevent network attacks by: detecting threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations. The IDS/IPS systems lack the visibility into application layer of TCP/IP stack and hence may not protect from application specific attacks.

   1.3 VPN: *Virtual Private Network*; VPN creates private confidential networks on top of shared public networks like Internet. VPNs by encrypting the data, provide secure tamper-proof remote employee log-in and remote branch office connection to the enterprise resources.

   1.4 Anti DDOS: Distributed Denial of Service (DDoS) is the fastest growing threat. It aims at bringing down the critical IT resources, by sending malicious traffic and thereby exhausting the critical resource capacity. The solutions also vary at each layer. T ISPs (Internet Service Providers) offer layer 3 and layer 4 DDoS protection services, guaranteeing clean pipes o However, to from volumetric DD S attacks. prevent layer 7 DDoS attacks on mise DDoS , -pre detection and prevention devices need to be put in place.

1.5 **Honeypot:** These are traps set up inside the network waiting for someone to attack. They work on simple concept; alert the security administrator the moment a contact is made to them.

1.6 **Network Access Control (NAC):** Non- compliant devices can be denied access to enterprise network using NAC isolating these insecure devices , from infecting the rest of nodes in the network. Examples of non-complaint devices include unauthorized - devices, un patched and not updated devices, etc.

1.7 **NBAD:** Network Behaviour Anomaly Detection (NBAD): Preventative security measures are often defeated, by new polymorphic malware, and zero day exploits. Therefore, it's important to be on the eye watch for intruders. NBAD analyses the flow of data across all devices to understand the deviations from normal traffic. For example, certain type of traffic, say Skype from normal users can be acceptable, but the same type of traffic from servers is very suspicious. NBAD is useful in detecting the suspicious behaviour and can guide the security experts in forming rules to prevent such events to occur in future.

2. **Host Security:** Hosts are the main access points to the critical assets of the enterprise and hence it is imperative to secure the hosts.

2.1. **Antivirus:** The most common basic security deployed on every host is anti-virus.

2.2 **Host IDS:** As anti-virus systems work based on signature verification and cannot protect hosts from zero-day malware, the servers are protected by another layer of security, which is host based IDS. The main goal of host IDS is to keep the integrity of the server intact. It keeps monitoring the suspicious operations like configuration changes, registry changes, log re-writes, file deletes, etc. and immediately alerts and blocks as per policy.

2.3 **WAF** : Web Application Firewall (WAF): The fastest growing categories of attacks and data breaches are those that target applications. There are countless possibilities to exploit code vulnerabilities and application modules.

2.4 **Endpoint Security**: For overall enterprise security is essential keep endpoint devices clean, malware free and up-to-date with all required patches.

2.5 Mobile Device Management (MDM): MDM software strengthens security through remote monitoring and control of security configurations, policy enforcement and patch pushes to mobile devices. Further, these systems can remotely lock lost, stolen, or compromised mobile devices and, if needed, wipe all stored data.

2.6 Anti-APT: Advanced Persistent Threats (APT) are custom-made targeted attacks. They are capable of compromising the targeted systems with advanced coding techniques that circumvent the traditional signature virus detection

3. **Data :** Data being one of the most critical assets, keeping the enterprise data safe and secure through various means is important.

   3.1 Cryptographic Techniques : Cryptographic techniques address two major security challenges – confidentiality and integrity. PKI (Public Key Infrastructure) is able to in addition address authentication non-repudiation. While and the cryptographic techniques are good at safeguarding the data at rest and data in motion, they are weak in protecting the data being in operation.

   3.2 Data Leakage Prevention: According to "Intel Security 2016 Data Protection Benchmark Study", over 25% of organisations do not monitor access to employee or customer information.

   3.3 Database Activity Monitoring (DAM): Monitoring database activity is a critical component of database security, especially as information that is more sensitive is consolidated into larger databases. Database Activity Monitor involves the capturing and recording of all Structured Query Language (SQL) activity in real-tme or near real-time. They can monitor database administrator activity, across multiple database platforms; and can generate alerts on policy violations. There are five features distinguish Database Activity Monitoring tools.

   3.4 E-Mail : Security E-mail is a popular attack vector and hence individual and business accounts need to be protected. E-mail acts as a launchpad for attacks like spam, phishing and spreading malware, etc. Secure e-mail gateway that scans all e-mails and filters the malicious e-mails is now common across all enterprises.

4. **Identity and Access Control:** Identity and access management solution with central directory of identities are integrated with applications and its underlying platform with "need to know/access" policy defined by the business layer.

   4.1 Directory Services : Directory is like a registry where all information about users, groups, computers, servers, printers, network shares, and more are stored.

   4.2 Two actor Authentication (2FA) : is an extra security layer that authenticates the user with one more factor over and above the usual password. Usually the second factor is a dynamic OTP (One-time Password) communicated with the customers (external users) over a different device they own and on a different channel, like OTPs sent over mobile for Internet Banking.

   4.3 Privileged Identity Module (PIM) : Called privileged identities, they are allow unrestricted access to view and change data, and alter configuration settings, and run programs.

   4.4 Single Sign-on (SSO) : SSO allows user to login once with ingle-I to access s D all applications and platforms. The user is authorised to access, and eliminates further prompts when they switch applications during a particular session. Single sign of allows logging out from all the systems f with single log-out. However, logging of a particular application does n t log them out of all applications they were accessing.

5. **Operations :** Operating a security program requires the necessary tools to support change control, and track assets based on classification framework.

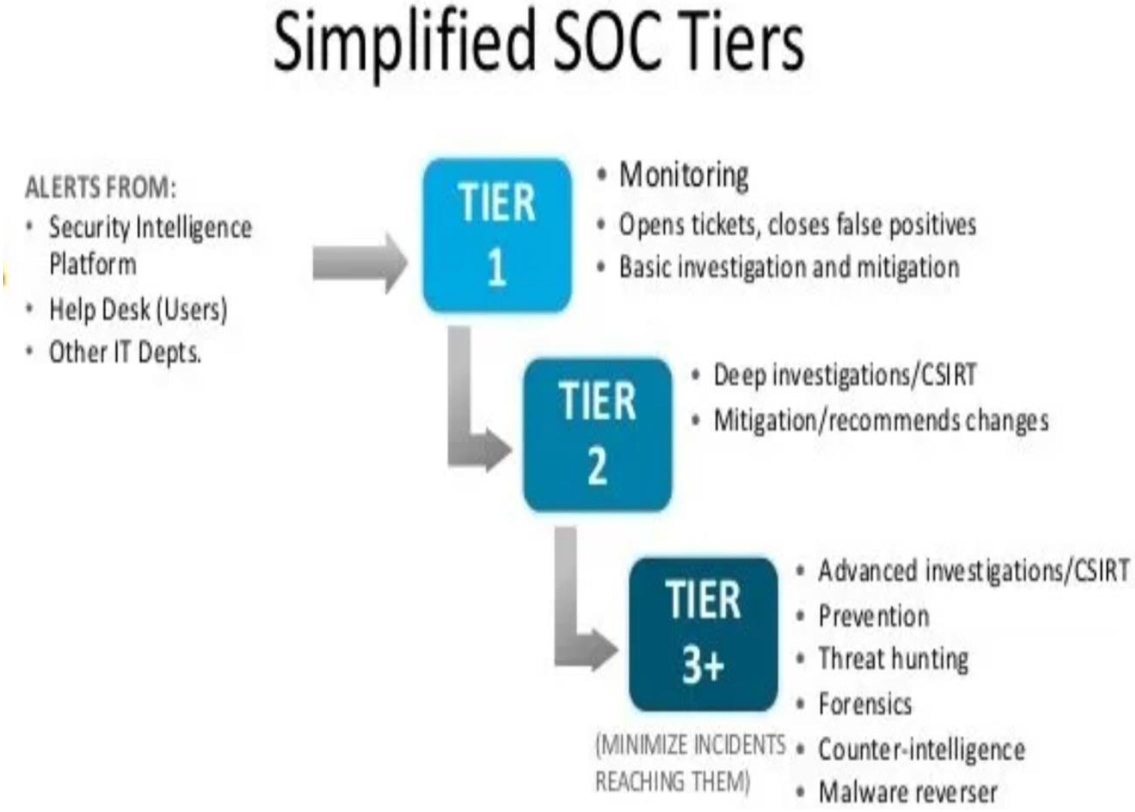
5.1 ServiceAsset Configuration andManagement (SACM) :According to ITIL, SACM is the process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed.

5.2 Vulnerability and Patch Management: It has become very common for vendors of hardware, software, network devices, security solutions, etc., to keep releasing patches to close the vulnerabilities. Not patching the systems leave the enterprise in a greater risk. Manual patching takes too long a time and leaves no audit trail of the whole exercise. Modern enterprises are automating the process of vulnerability and patch management through centralised tools.

5.3 Security Incident and Event Management (SIEM): SIEM is a tool that collects logs and events from various security infrastructure, systems and applications and stores it centrally. It also helps in normalizing the logs/events from of different types different nodes to a standard pattern. The collection and storing are done in a compressed form to save the network and stor e. Once collected, age resources these logs/event are analysed correlate and meaningful intelligence is provided on a central console with various customizable dashboards for faster reaction and identification of root cause of the incident.

5.4 Security Operations Center: Security Operations Center is a generic term describing a platform set up for the purpose of providing detection and timely reactive services to security incidents. ISOC solution is an integrated deployment of advanced cyber security products/services, expert human resources, and industry best practices and processes. ISOC implementation and operationalization play a crucial role in achieving the objective of providing in-depth centralized visibility into organization's IT infrastructure to monitor, detect, prevent and mitigate security incidents. Organizations need to focus more on rapid detection and response mechanisms, apart from technologies that prevent intrusions. Quick detection and remediation is possible only by automating the security operations. Such automation frees up analysts from mundane tasks and allows them to concentrate on higher-priority risks affecting the most critical assets and data. ISOC automation capability is going to be a major distinguishing factor in assessing an ISOC product/technology. An advanced implementation of the Information Security Operations Center

(ISOC) may have the following additional components. Upon implementation of a basic version of ISOC, organizations may build these functionalities in their ISOC.



Simplified SOC Tiers

ALERTS FROM:
- Security Intelligence Platform
- Help Desk (Users)
- Other IT Depts.

TIER 1
- Monitoring
- Opens tickets, closes false positives
- Basic investigation and mitigation

TIER 2
- Deep investigations/CSIRT
- Mitigation/recommends changes

TIER 3+
- Advanced investigations/CSIRT
- Prevention
- Threat hunting
- Forensics
- Counter-intelligence
- Malware reverser

(MINIMIZE INCIDENTS REACHING THEM)

3.2 Basics of SIEM deployment

SIEM is Implemented in 4 Steps

A successful SIEM implementation requires careful planning, execution, and ongoing review to ensure that the system meets the organization's security and compliance needs. Here's a discussion of the key steps involved in the process:

1. Establish Requirements

Before implementing a SIEM solution, it's crucial to identify the organization's specific security and compliance requirements. This involves:

- **Regulatory landscape:** Research the relevant industry-specific regulations (e.g., GDPR, HIPAA, PCI-DSS) and internal policies that dictate your organization's security and compliance requirements.
- **Data sources:** Identify all data sources to be monitored, such as firewalls, intrusion detection systems, endpoint security tools, authentication systems, and application logs. Prioritize them based on their criticality and risk levels.
- **Desired outcomes:** Clearly articulate the goals of implementing a SIEM solution, such as reducing incident response time, ensuring compliance with specific regulations, or use case priorities such as gaining insights into user behavior.

2. Implementation Planning

Once the requirements are established, a detailed implementation plan should be developed. This plan should cover:

- **SIEM selection:** Evaluate various SIEM solutions in the market based on factors like functionality, scalability, ease of use, integration capabilities, and cost. Consider conducting a proof-of-concept to help make an informed decision.
- **Project scope and timeline:** Outline the scope of the SIEM implementation project, including the number of data sources, required integrations, and customizations. Establish a realistic timeline with milestones for each phase of the project.
- **Stakeholder involvement:** Engage key stakeholders from IT, security, and compliance teams to ensure collaboration, communication, and alignment of goals. Assign specific roles and responsibilities to the team members.

- **Training plan:** Develop a training program to educate team members on using and managing the SIEM system effectively. This should cover topics like system administration, incident response, reporting, and troubleshooting.

3. Deployment and Review

The deployment phase involves installing, configuring, and integrating the SIEM solution with the organization's IT infrastructure. Key tasks include:

- **SIEM installation:** Set up the SIEM solution by installing the required software or hardware, as well as necessary agents or connectors on the relevant devices.
- **Configuration:** Define the data normalization and correlation rules to ensure that events from different sources are accurately analyzed and correlated. Create custom rules, alerts, and dashboards tailored to your organization's needs.
- **Security policies and workflows:** Develop and implement security policies to govern the use of the SIEM system. Establish response workflows for handling alerts and incidents, including escalation procedures and communication channels.
- **Testing:** Conduct thorough testing of the SIEM system to validate its functionality, effectiveness, and accuracy in detecting threats, generating alerts, and providing context for incident response.
- **Review and refinement:** Gather feedback from stakeholders and end-users to identify areas for improvement. Refine the system configuration, rules, and alerts to address any gaps or issues discovered during the testing and review phase.

4. Post-Implementation

Following the deployment and initial review, the SIEM system should be continuously monitored, maintained, and optimized. This includes:

- **Policy and rule updates:** Regularly review and update security policies, rules, and alerts to ensure they remain relevant and effective in the face of evolving threats and changing business requirements.
- **Performance optimization:** Monitor the SIEM system's performance and resource utilization, and make necessary adjustments to ensure optimal efficiency.
- **Threat intelligence:** Integrate the SIEM solution with external threat intelligence feeds to stay updated on the latest security threats, vulnerabilities, and trends.
- **Ongoing training and support:** Provide continuous training, documentation, and support to team members to ensure they can effectively manage and use the SIEM system.

- **Periodic reviews and audits:** Conduct regular reviews and audits of the SIEM system to assess its effectiveness, compliance, and alignment with the organization’s security and compliance needs. Use these findings to make data-driven decisions for further optimization and improvement.

3.3 Factors to consider while deploying SIEM

1. Map your company data flows.
2. Align to the company's regulatory compliance needs.
3. Identify your assets to select the necessary log data sources.
4. Select the right SIEM technology for your IT environment.
5. Configure your SIEM effectively.

- **Map your company's data flows:**

  You must consider your business information, and that related to your IT (authentication, security, infrastructure) to map your corporate data flows in order to find your assets. You need to identify where the information flows, where it is stored, and how you can access it, both from inside and outside the company network, in order to protect it.

  Your last risk assessment, if available, will provide you with specific indications relating to your critical systems, and your security priorities and, indirectly, support the configuration of the SIEM use cases.

- **Be aligned with your company's regulatory compliance needs (GDPR, PCI DSS, ISO 27001, etc.) and your recent risk evaluation:**

  We live in Europe, and the GDPR includes several useful references to be taken. It also includes many other useful references to be taken into account in the design of a SIEM platform including the need to establish a log data retention policy, the need to differentiate access to log information in compliance with the least privilege, and the need to know principles, protection of logs at rest and in transit, among other things.

  It is important to consider any other compliance with security frameworks and guidelines required by your business, e.g., ISO 27001, PCI DSS, COBIT for SOX compliance, etc.

Some frameworks like PCI DSS (requirements 10. x) contain detailed indications of how to configure auditing settings and retain system logs for compliance. The SIEM project team must take into account these various needs during implementation, correctly identifying the certification perimeter.

- **Identify your assets to select the log data sources:**

  Once you have considered your data flows and compliance needs, you will have a clear picture of the possible assets and select the data sources for your log collection. Data sources are important and not all the logs are equal: some are written in open format (like the Common Event Format), and others must be interpreted and parsed by the platform.

  So, how do you decide on what to feed your SIEM? The SANS Institute published a short guide, "Top 6 SANS Essential Categories of Log Reports" to help organizations identify the most common security controls which should be considered when customizing SIEM reports. While the guide is many years in existence now it still offers useful guidance on where to start. It suggests reports that have the highest likelihood of identifying suspicious activity, in order to keep the number of false positives low. The top report categories are listed below:

  1. Authentication and Authorization Reports
  2. Systems and Data Change Reports
  3. Network Activity Reports
  4. Resource Access Reports
  5. Malware Activity Reports
  6. Failure and Critical Error Reports

  Your organization can use these as a starting point. Additionally, don’t forget to also consider other sources that you may have to improve threat detection. For example:

  A. Cloud platforms
  B. Endpoint detection and response (EDR)
  C. Network detection and response (NDR)
  D. Mobile device management (MDM)
  E. File integrity monitoring (FIM)
  F. DHCP logs and databases

G. DNS logs

Each organization is unique and prioritizes its data differently so while setting up your own SIEM instance you need to use your own judgment on what matters most to your organization. Your organization may choose to prioritize compliance frameworks adherence, risk assessment results, MITRE ATT&CK's techniques detection section, MITRE Cyber Analytics Repository, Sigma rules, incident report outcomes, etc

- **Select the right SIEM technology for your IT environment:**

  Once you’ve identified your assets, you should be able to determine the most appropriate deployment models and SIEM solutions that fit your needs: on-premise, cloud-native, SIEM-as-a-service (using a third-party supplier), self orhybrid-managed.

  A SIEM-as-a-service (Managed SIEM) option can offer several benefits to your organization including reducing SIEM deployment cost (simply paying a subscription fee), leveraging the existing infrastructure of the provider to speed up deployment, service scalability, gaining access to the SIEM provider’s skilled staff for tuning, and limiting internal personnel requirements.

  To support your technology decision-making, you can use resources such as Gartner's "RFP for Security Information and Event Management" toolkit, the Gartner Magic Quadrant/Market Guide for SIEM, or other free online user reviews and comparisons of the industry-leading marketplace vendors.

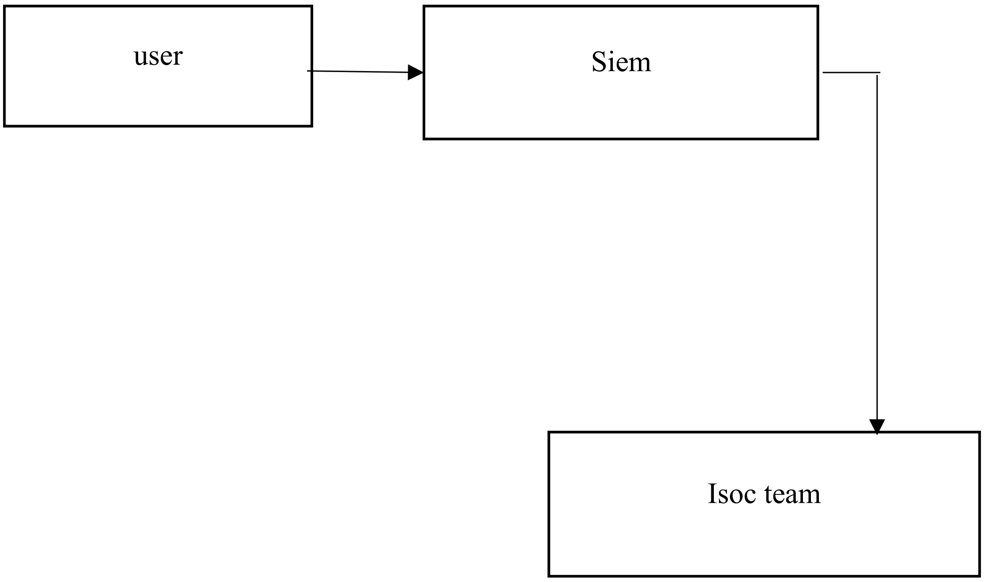
- **Configure your SIEM (log collection, parsing, correlation rules, behavior analysis, use cases, alarms, etc.), as well as a regular review of security events (establish a security monitoring process based on your SIEM platform):**

  Configuration of the data sources (e.g., the servers that generate logs) is as important as configuring the SIEM platform itself.

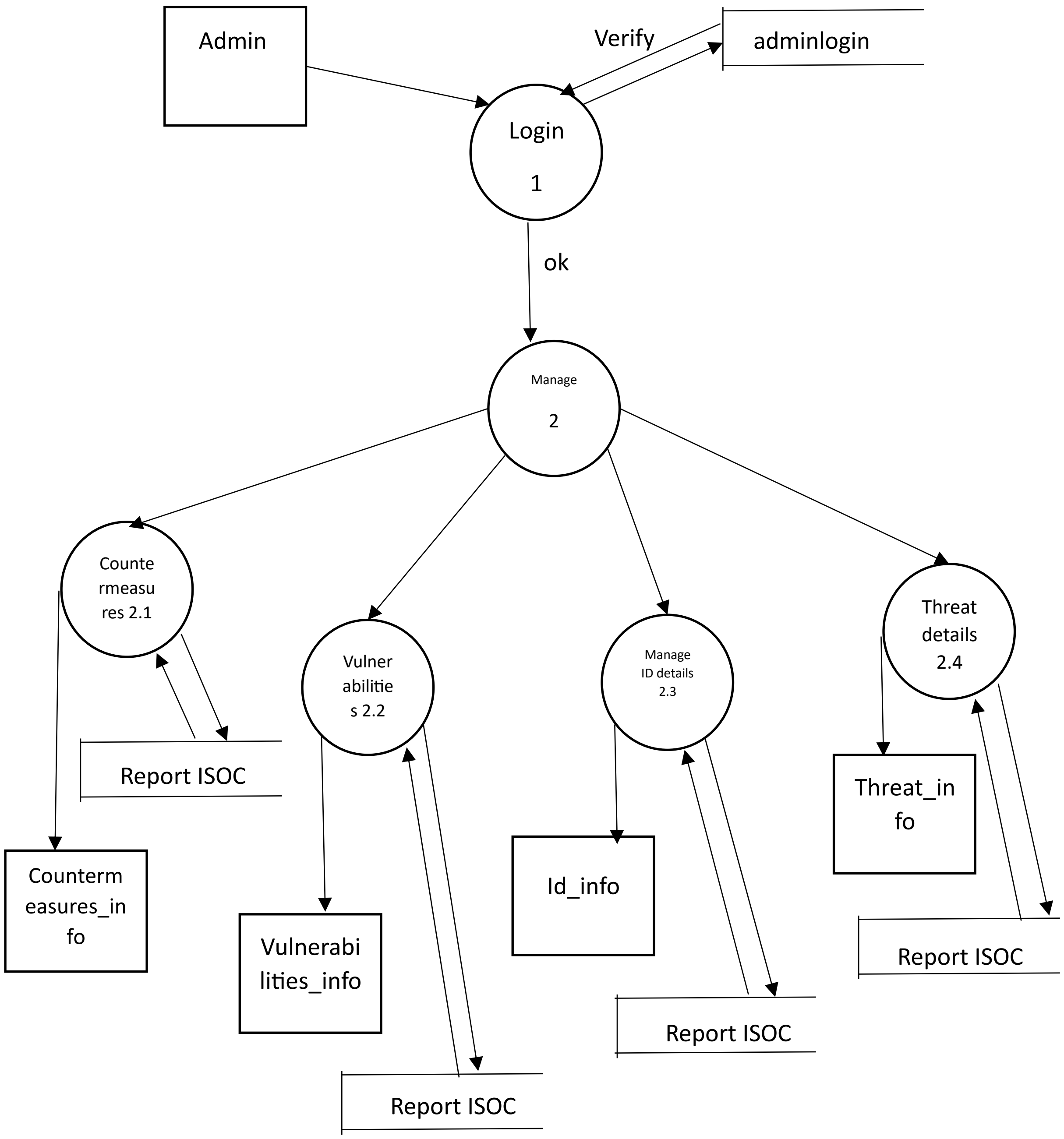
  SIEM solutions are first and foremost containers of information from selected sources. The more complete this information is, the more it will increase the efficiency of the monitoring process. To that end, correct hardening policies are paramount, since systems and applications must provide accurate and meaningful auditing information while minimizing the impact on performance. For example, use Windows advanced audit policy settings only, do not rely on default, and explicitly configure the desired value for each setting.

Do not forget to involve your internal teams (DBAs, systems engineers, application owners, etc.) to correctly choose the auditing parameters without compromising the functioning of the production systems and consequentially your business. Make daily security log reviews a routine for your staff and improves automation. Use threat intelligence feeds and user entity behavior analytics (UEBA) features, if available.

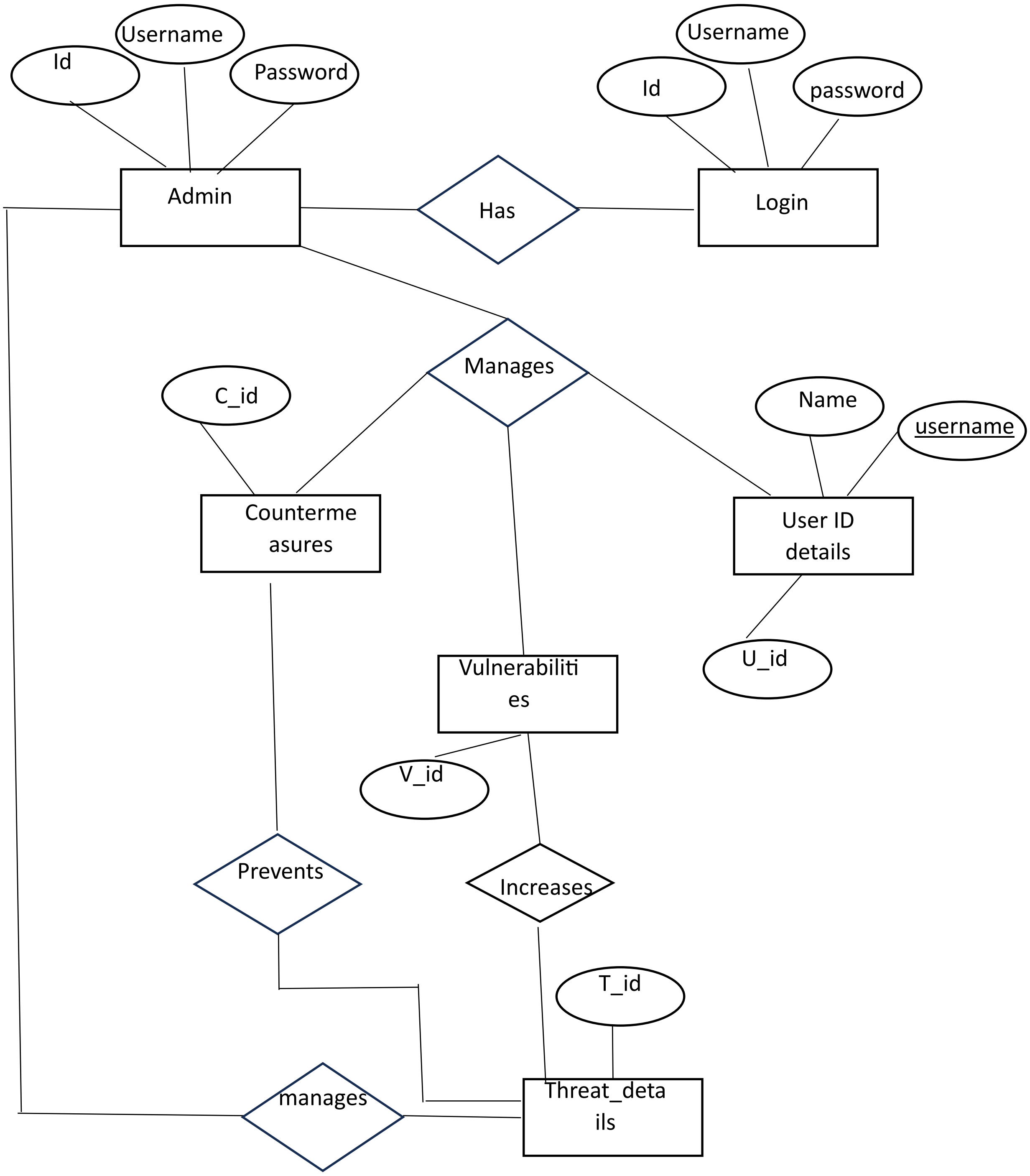
3.4 Data Flow Diagram (Level- 0)



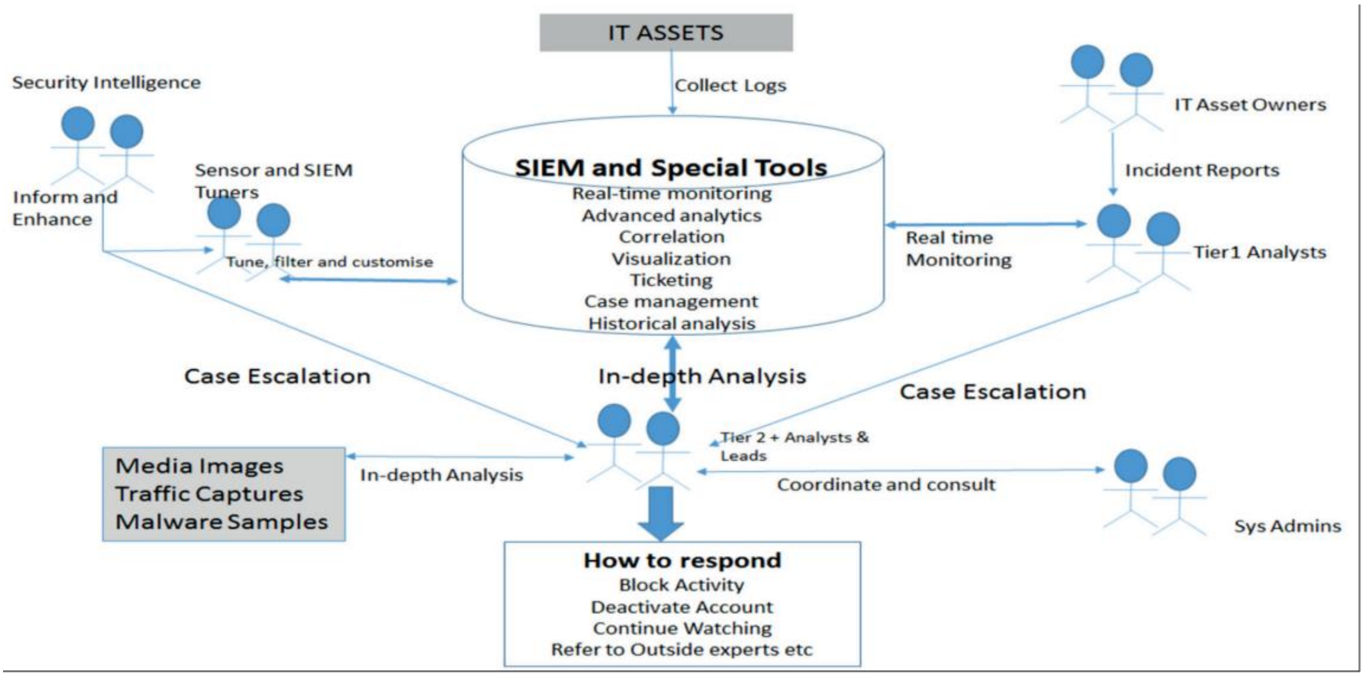
3.4.1 DFD for Admin(Level- 1)



3.5 ER Diagram



Chapter 4: Testing



The testing was performed on SIEM under ISOC team supervision by passing in various use cases. A total of 5 use cases were considered in arriving to the conclusion.

During testing the data from various devices, networks, sensors etc were collected. And the data collected was sent to the SIEM which was now joined with various host and server end security tools . The activities performed on the system end security devices were being regularly monitored by the ISOC team. In this way our software efficiently detected all the malicious activities as soon as they as occur.

A list of results that were generated on testing the software is as under.

Serial no.	Classification	Description	Severity
1.	Compromise	Logs reporting on a successful system or a network compromise	High
2.	Attack	Logs reporting on an activity indicating system or network attack. Attack is known to have originated from a "Bad Guy" source.	High
3.	Denial of service	Logs reporting on activity indicating denial of service where it is assumed to have succeeded to have failed.	High
4.	Malware	Logs reporting on activity indicative of malware installation, propagation or use which is specifically targeting the organisation and can be aligned with any Indicators of Compromise	High
5.	Suspicious	Logs reporting on an activity that is only suspicious but not known to be a legitimate attack	Medium
6.	Reconnaissance	Logs reporting on an activity indicative of or directly indicating system or network reconnaissance.	Medium
7.	Misuse	Logs reporting on an activity indicating network or system misuse	Medium
8.	Activity	Logs reporting on general system or network activity	Medium

9.	Risk	Logs reporting on potential vulnerability weaknesses.	Medium
10.	Authentication	Logs reporting on unusual authentication attempts and account modifications	Medium
11.	Access	Logs reporting on general system access activity	Medium
12.	Application	Logs reporting on application specific activity	Medium
13.	Failed attack	Logs reporting on attack activity that was not successful, possibly due to preventive measures	Low
14.	Failed denial of service	Logs reporting on denial of service activity that was not successful, possibly due to preventative measures.	Low
15.	Failed malware	Logs reporting on malware activity that was not successful, possibly due to preventative measures	Low
16.	Failed suspicious	Logs reporting on suspicious activity that was not successful, possibly due to preventative measures.	Low
17.	Failed activity	Logs reporting on general system or network activity that was not successful, possibly due to preventative measures	Low
18.	Other security	Logs reporting on security activity not otherwise classifiable.	Low

4.2 Integration Testing :- In integration testing, system consists different modules, where in each module can arise problems during the testing. Integration testing is the process of testing the interaction between different components/modules of the system to ensure that they are working properly when combined. It helps to identify defects or issues that may arise when the components are integrated. Integration testing should be developed from the system specification. Firstly, a minimum configuration must be integrated and then tested

4.3 Validation Testing :- Validation testing provides final assurance that software meets all behavioral and performance requirements. It helps to identify defects or issues that may arise when the components are integrated. Validation can be defined in many ways but a simple definition is that validation succeeds when software function in a manner that can be reasonably used by the customer. In this testing we had tested the connectivity or data transfer between couple of unit testing modules. Validation testing will involve testing the overall system to ensure that it meets the requirements of the user such as ease of use, security, and reliability. This will involve testing various scenarios such as registration of complaints, updating complaint status, and generating reports to ensure that the system is functioning as intended. Overall, integration and validation testing are critical to ensuring the success of the Complaint Management System and providing a reliable and efficient tool for the students and department admins of Indian Post Payment Banks.

Chapter 5: Implementation

Toinstall the time zone update package before installation:

1. Unpack the package and upload it to your server (for example, to /opt/work/).

2. As user root, run the following command: rpm-Uvh /opt/work/

3. Tocheck the time zone setting, run the following command: timedatectl

4. If the time zone is not correct or it is not the desired time zone, run the following commandtospecify another time zone:

timedatectl set-timezone

For example: timedatectl set-timezone America/Los_Angeles

To install the time zone update package after you complete the ESM installation:

1. Use the procedure above to install the correct time zone update package.

2. As user arcsight, shut down all ArcSight services:
/etc/init.d/arcsight_services stop all

3. As user arcsight, run the following command (all on one line):
/opt/arcsight/java/esm/current/jre/bin/java-jar /opt/arcsight/manager/lib/jre-tools/tzupdater/ziupdater-1.1.1.1.jar-V

4. As user arcsight, start all ArcSight services:
/etc/init.d/arcsight_services start all Set Directory Sizes Make sure that the partition in which your /tmp directory resides has at least 6 GB of space.

Set Directory Sizes

Installation Guide Installing Software ESM Make sure that the partition in which your /opt/arcsight directory resides has at least 100 GB of space.

Sizing Guidelines for CORR-Engine

When installing ESM 7.5, the default CORR-Engine storage sizes are automatically calculated based on your hardware according to the default values in the table below. These are the recommended sizing guidelines. You can change any of the default storage sizes in the “CORR Engine Configuration” panel of the wizard, but when doing so, be sure that you take the minimum and maximum values into consideration when changing storage sizes.

Note: Any events that are brought from an offline archive into the online archive count as part of the total 12 TB (or license determined) storage limit. You do not want the offline archives that you bring back online to encompass the entire storage limit. Use discretion when bringing offline archives online, and be sure to make them offline again when you are done working with them.

Port	Flow	Description
8443/TCP	Inbound	Smart Connector sand Consoles Note:This port is only necessary in compact mode or for communication to the persist or node.
25/TCP	Out bound	SMTP to mail server Note: ESM only requires email in compact mode or on the persist or node
1100/TCP	Out bound	POP3to mail server Note:ESM only requires email in compact mode or on the persist or node
143/TCP	Out bound	IMAP to mail server Note: ESM only requires email in compact mode or on the persist or node
1645/UDP	Out bound/ Inbound	RADIUS Note:This port is only necessary in compact mode or for communication to the persist or node.
1812/UDP	Out bound/ Inbound	RADIUS,if applicable Note:This port is only necessary in compact mode or for communication to the persist or node.
389/UDP	Out bound	LDAP to LDAP server,if applicable
636/UDP	Out bound	LDAP over SSL to LDAP server, if applicable
9000/UDP	Out bound/ Inbound	Logger peering, if a pplicable Note:This port is only necessary in compact mode or for communication to the persist or node.

Chapter 6: Sample Forms

5.1 Logic- High Priority Alert in DDI

Monitor the alert for high priority alert in DDI

Description: Trend Micro's Deep Discovery Inspector is a device product.

When traffic reaches DDI, we receive an alert. It detects malicious content, communications, and behaviour that could point to advanced malware or attacker activity at any point in the attack process. Thus, when malicious traffic reaches Trend Micro's DDI, an alert titled "High Priority Alert on DDI" is generated based on a high level of severity.

Impact: It can do encrypt files on the endpoint, threatening to erase files, or blocking system access, creating backdoor.

Action taken by SOC Team

a. Verify the IP address's reputation (good or malicious), and if the IPS or firewall permitted it, block it. Verify whether the IP address is public, private, or outsourced.
b. Verify logs to identify the traffic and source address with high priority allowed by DDI
c. If malicious IP is available to the public, then brought the incident up with the team so they may be blocked if IP is private so SOC team do the communicate with the Concern team (through mail) and try to find out it is legitimate action or not.

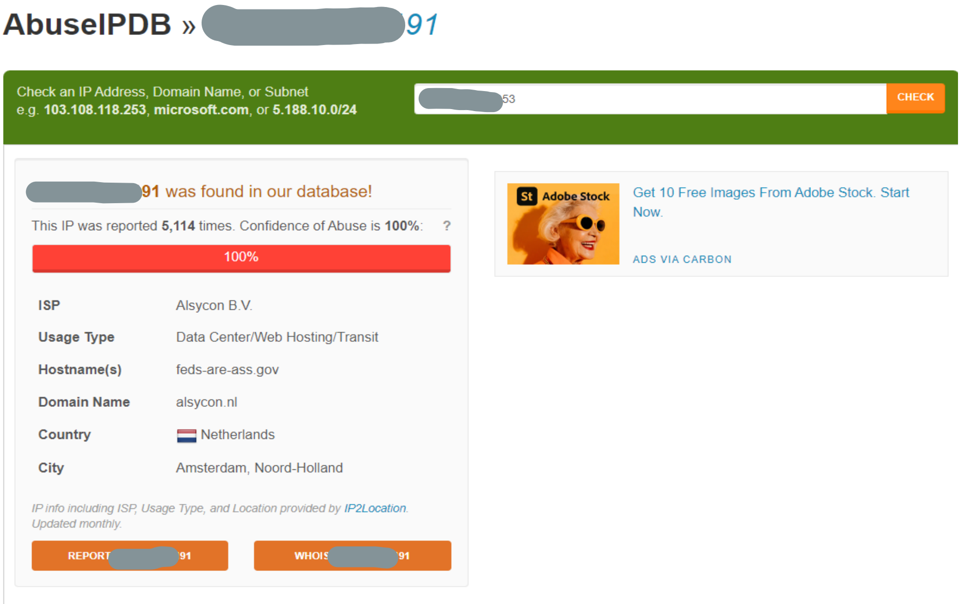
Practical Steps:-

a. Verify the IP address's reputation (good or malicious), and if the IPS or firewall permitted it, block it. Verify whether the IP address is public, private, or outsourced.

- Check the IP Reputation (Malicious or good)

  Use below URL to get check the IP Reputation.

  https://www.abuseipdb.com



AbuseIPDB » [redacted]91

Check an IP Address, Domain Name, or Subnet
e.g. **103.108.118.253**, **microsoft.com**, or **5.188.10.0/24**

[redacted]53 CHECK

[redacted]**91** was found in our database!

This IP was reported **5,114** times. Confidence of Abuse is **100%**: ?

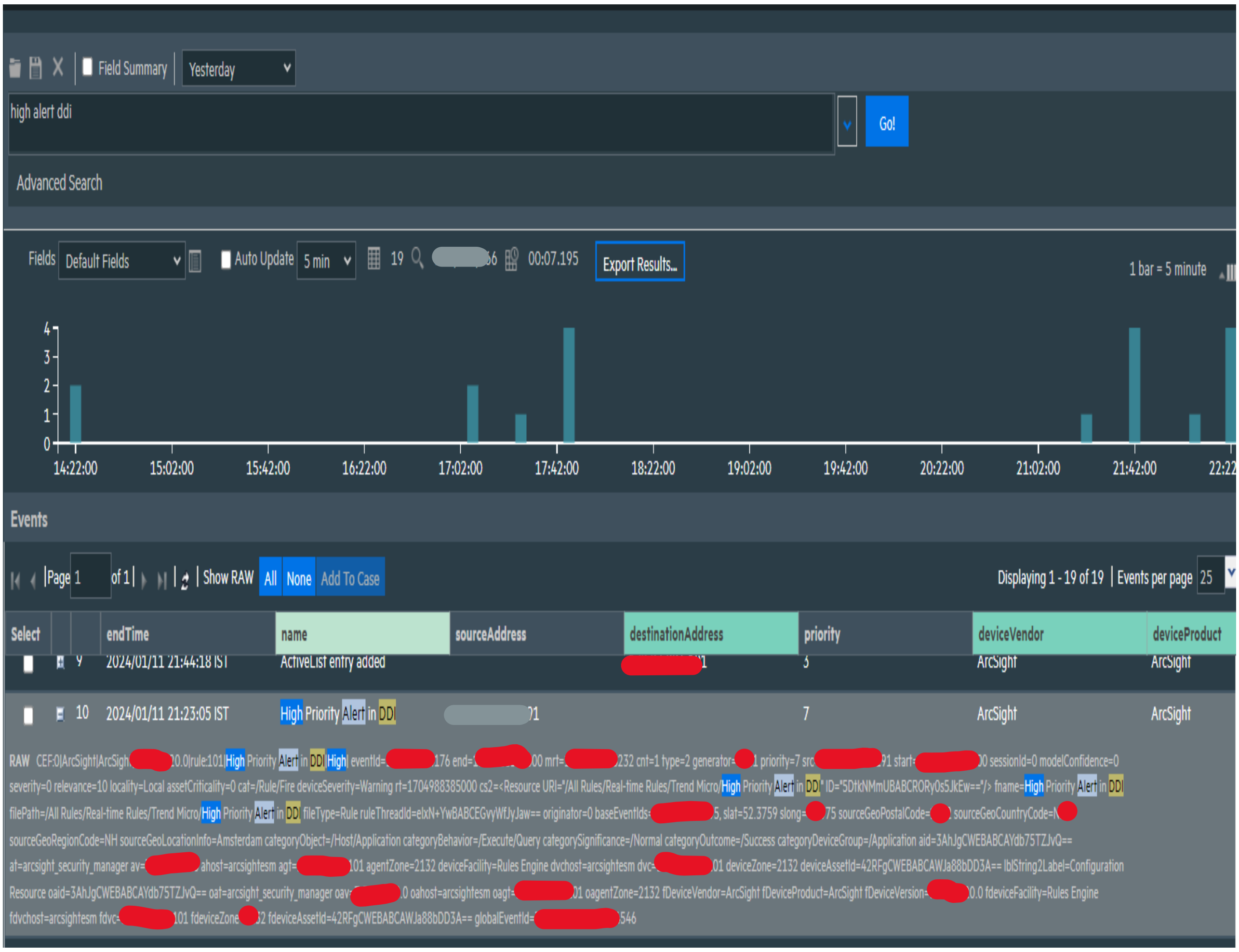
100%

ISP	Alsycon B.V.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	feds-are-ass.gov
Domain Name	alsycon.nl
Country	Netherlands
City	Amsterdam, Noord-Holland

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT [redacted]91 WHOIS [redacted]91

b. Verify logs to identify the traffic and source address with high priority allowed by DDI



high alert ddi

Select			endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct
□	⊞	9	2024/01/11 21:44:18 IST	ActiveList entry added		[redacted]1	3	ArcSight	ArcSight
□	⊟	10	2024/01/11 21:23:05 IST	High Priority Alert in DDI	[redacted]91		7	ArcSight	ArcSight

```
RAW  CEF:0|ArcSight|ArcSigh[redacted]0.0|rule:101|High Priority Alert in DDI|High| eventId=[redacted]176 end=[redacted]00 mrt=[redacted]232 cnt=1 type=2 generator=[redacted]1 priority=7 src[redacted]91 start=[redacted]00 sessionId=0 modelConfidence=0
severity=0 relevance=10 locality=Local assetCriticality=0 cat=/Rule/Fire deviceSeverity=Warning rt=1704988385000 cs2=<Resource URI="/All Rules/Real-time Rules/Trend Micro/High Priority Alert in DDI" ID="5DtkNMmUBABCRORy0s5JkEw=="/> fname=High Priority Alert in DDI
filePath=/All Rules/Real-time Rules/Trend Micro/High Priority Alert in DDI fileType=Rule ruleThreadId=elxN+YwBABCEGvyWfJyJaw== originator=0 baseEventIds=[redacted]5, slat=52.3759 slong=[redacted]75 sourceGeoPostalCode=[redacted] sourceGeoCountryCode=N[redacted]
sourceGeoRegionCode=NH sourceGeoLocationInfo=Amsterdam categoryObject=/Host/Application categoryBehavior=/Execute/Query categorySignificance=/Normal categoryOutcome=/Success categoryDeviceGroup=/Application aid=3AhJgCWEBABCAYdb75TZJvQ==
at=arcsight_security_manager av=[redacted] ahost=arcsightesm agt=[redacted]101 agentZone=2132 deviceFacility=Rules Engine dvchost=arcsightesm dvc=[redacted]01 deviceZone=2132 deviceAssetId=42RFgCWEBABCAWJa88bDD3A== lblString2Label=Configuration
Resource oaid=3AhJgCWEBABCAYdb75TZJvQ== oat=arcsight_security_manager oav=[redacted].0 oahost=arcsightesm oagt=[redacted]01 oagentZone=2132 fDeviceVendor=ArcSight fDeviceProduct=ArcSight fDeviceVersion=[redacted]0.0 fdeviceFacility=Rules Engine
fdvchost=arcsightesm fdvc=[redacted]101 fdeviceZone[redacted]2 fdeviceAssetId=42RFgCWEBABCAWJa88bDD3A== globalEventId=[redacted]546
```

c. <u>If malicious IP is available to the public, then brought the incident up with the team so they may be blocked</u>

d. <u>After getting response from concern soc team update activity on the ITSM tool as</u> per analysis

e. <u>Response from Concern team</u>

5.2 Potential High-Risk File Founded

Monitor and alert when potential high-risk file founded.

Description: When traffic touched our device, "Trend Micro," on the Deep Device Analyzer product, we received an alert. "Deep Discovery Analyzer is a turnkey appliance that analyzes and detects targeted attacks using virtual images of endpoint configurations**.** "it is executed when traffic hit on Trend Micro with severity risk high

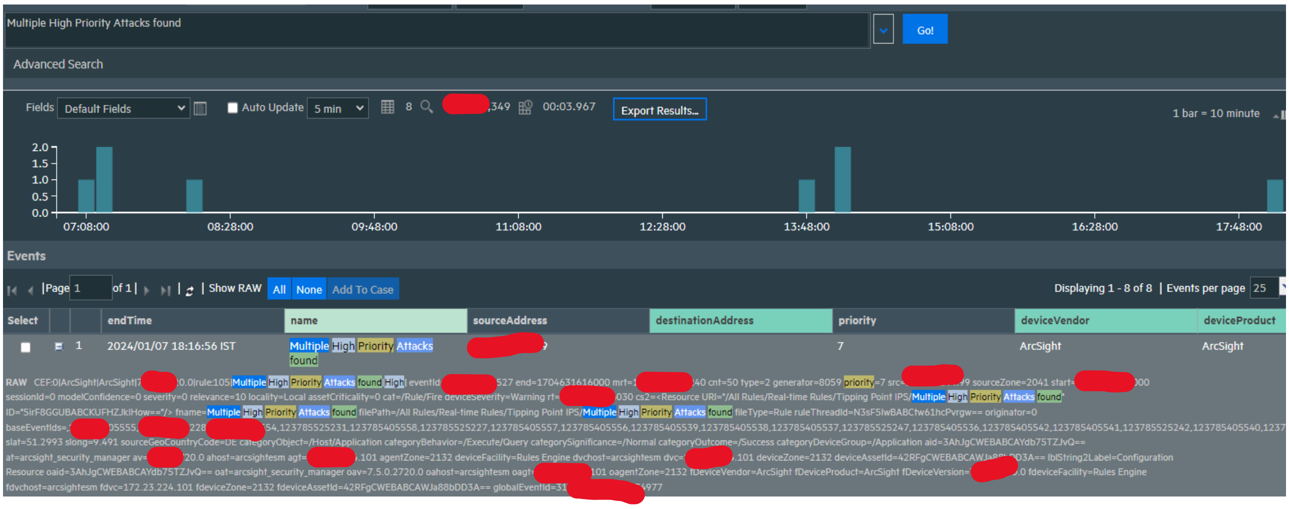
Impact: It can do encrypt files on the endpoint, threatening to erase files, or blocking system access, creating backdoor.

<u>Action taken by SOC Team</u>

a. Soc will verify logs for high risk file.
b. Discuss with AV team and try to understand the high-risk file and action taken by the antivirus on that.
c. Soc team will create incident and assign to AV team.
d. Soc team Put their remark if activity is legitimate then ticket will be resolved

<u>Practical Steps:-</u>

a. Soc will verify logs for high risk file



Multiple High Priority Attacks found

Fields Default Fields | □ Auto Update 5 min | 8 | [redacted],349 | 00:03.967

|Page 1 of 1| | Show RAW | Displaying 1 - 8 of 8 | Events per page 25

Select			endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct
□	▤	1	2024/01/07 18:16:56 IST	Multiple High Priority Attacks found	[redacted]9		7	ArcSight	ArcSight

```
RAW  CEF:0|ArcSight|ArcSight|7[redacted]0.0|rule:105|Multiple High Priority Attacks found|High| eventId=[redacted]527 end=1704631616000 mrt=1[redacted]40 cnt=50 type=2 generator=8059 priority=7 src=[redacted]99 sourceZone=2041 start=[redacted]000
sessionId=0 modelConfidence=0 severity=0 relevance=10 locality=Local assetCriticality=0 cat=/Rule/Fire deviceSeverity=Warning rt=[redacted]030 cs2=<Resource URI="/All Rules/Real-time Rules/Tipping Point IPS/Multiple High Priority Attacks found"
ID="5irF8GGUBABCKUFHZJklHow=="/> fname=Multiple High Priority Attacks found filePath=/All Rules/Real-time Rules/Tipping Point IPS/Multiple High Priority Attacks found fileType=Rule ruleThreadId=N3sF5IwBABCtw61hcPvrgw== originator=0
baseEventIds=,[redacted]05555,[redacted]228[redacted]54,123785525231,123785405558,123785525227,123785405557,123785405556,123785405539,123785405538,123785405537,123785525247,123785405536,123785405542,123785405541,123785525242,123785405540,1237
slat=51.2993 slong=9.491 sourceGeoCountryCode=DE categoryObject=/Host/Application categoryBehavior=/Execute/Query categorySignificance=/Normal categoryOutcome=/Success categoryDeviceGroup=/Application aid=3AhJgCWEBABCAYdb75TZJvQ==
at=arcsight_security_manager av=[redacted]20.0 ahost=arcsightesm agt=[redacted].101 agentZone=2132 deviceFacility=Rules Engine dvchost=arcsightesm dvc=[redacted].101 deviceZone=2132 deviceAssetId=42RFgCWEBABCAWJa8[redacted]DD3A== lblString2Label=Configuration
Resource oaid=3AhJgCWEBABCAYdb75TZJvQ== oat=arcsight_security_manager oav=7.5.0.2720.0 oahost=arcsightesm oagt=[redacted]101 oagentZone=2132 fDeviceVendor=ArcSight fDeviceProduct=ArcSight fDeviceVersion=[redacted].0 fdeviceFacility=Rules Engine
fdvchost=arcsightesm fdvc=172.23.224.101 fdeviceZone=2132 fdeviceAssetId=42RFgCWEBABCAWJa88bDD3A== globalEventId=31[redacted]4977
```

a. Discuss with AV team and try to understand the high-risk file and action taken by the anti-virus on that
b. Soc team will create incident and assign to AV team in ITSM.
c. Soc team Put their remark if activity is legitimate then ticket will be resolved

5.3 Log into Multiple Systems in Short Period

This rule triggered by login into multiple systems in short time period.

Description: When the user login in short time on the multiple System the alert will triggered

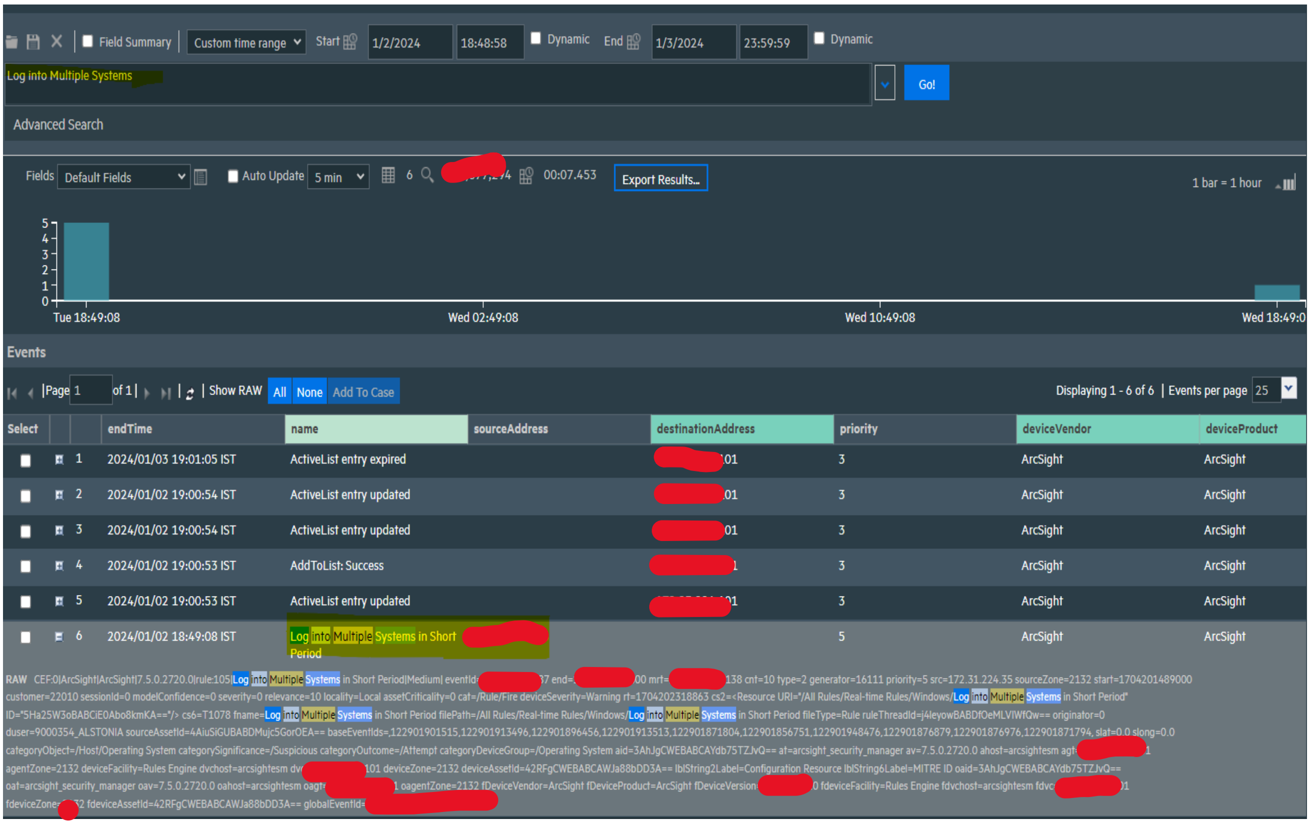
Impact: Unauthorized users can download and run malicious software to elevate their privileges.

Action taken by SOC Team

a. Verify in logs and identify the target Username which is logged in multiple system in short period of time
b. Raise concern with the respective team assigning a ticket for the justifications.
c. If this is not a valid activity, immediately inform respective team to disable the user
d. Soc team updated their analysis after ticket would be resolved

Practical Steps:-

a. Verify in logs and identify the target Username which is logged in multiple system in short period of time



Log into Multiple Systems

Select		endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct
□	1	2024/01/03 19:01:05 IST	ActiveList entry expired		[redacted]	3	ArcSight	ArcSight
□	2	2024/01/02 19:00:54 IST	ActiveList entry updated		[redacted]	3	ArcSight	ArcSight
□	3	2024/01/02 19:00:54 IST	ActiveList entry updated		[redacted]	3	ArcSight	ArcSight
□	4	2024/01/02 19:00:53 IST	AddToList: Success		[redacted]	3	ArcSight	ArcSight
□	5	2024/01/02 19:00:53 IST	ActiveList entry updated		[redacted]	3	ArcSight	ArcSight
□	6	2024/01/02 18:49:08 IST	Log into Multiple Systems in Short [redacted] Period			5	ArcSight	ArcSight

```
RAW  CEF:0|ArcSight|ArcSight|7.5.0.2720.0|rule:105|Log into Multiple Systems in Short Period|Medium| eventId=[redacted]37 end=[redacted]00 mrt=[redacted]138 cnt=10 type=2 generator=16111 priority=5 src=172.31.224.35 sourceZone=2132 start=1704201489000
customer=22010 sessionId=0 modelConfidence=0 severity=0 relevance=10 locality=Local assetCriticality=0 cat=/Rule/Fire deviceSeverity=Warning rt=1704202318863 cs2=<Resource URI="/All Rules/Real-time Rules/Windows/Log into Multiple Systems in Short Period"
ID="5Ha25W3oBABCiE0Abo8kmKA=="/> cs6=T1078 fname=Log into Multiple Systems in Short Period filePath=/All Rules/Real-time Rules/Windows/Log into Multiple Systems in Short Period fileType=Rule ruleThreadId=j4leyowBABDfOeMLVIWfQw== originator=0
duser=9000354_ALSTONIA sourceAssetId=4AiuSiGUBABDMujc5GorOEA== baseEventIds=,122901901515,122901913496,122901896456,122901913513,122901871804,122901856751,122901948476,122901876879,122901876976,122901871794, slat=0.0 slong=0.0
categoryObject=/Host/Operating System categorySignificance=/Suspicious categoryOutcome=/Attempt categoryDeviceGroup=/Operating System aid=3AhJgCWEBABCAYdb75TZJvQ== at=arcsight_security_manager av=7.5.0.2720.0 ahost=arcsightesm agt[redacted]1
agentZone=2132 deviceFacility=Rules Engine dvchost=arcsightesm dv[redacted]101 deviceZone=2132 deviceAssetId=42RFgCWEBABCAWJa88bDD3A== lblString2Label=Configuration Resource lblString6Label=MITRE ID oaid=3AhJgCWEBABCAYdb75TZJvQ==
oat=arcsight_security_manager oav=7.5.0.2720.0 oahost=arcsightesm oagt[redacted]1 oagentZone=2132 fDeviceVendor=ArcSight fDeviceProduct=ArcSight fDeviceVersion[redacted]0 fdeviceFacility=Rules Engine fdvchost=arcsightesm fdvc[redacted]01
fdeviceZone=[redacted]32 fdeviceAssetId=42RFgCWEBABCAWJa88bDD3A== globalEventId=[redacted]
```

b. Raise concern with the respective team assigning a ticket for the justifications.
c. Soc team updated their analysis after ticket would be resolved

5.4 Juniper: Configuration Deletion

Monitors alert for the configuration deletion in Juniper Firewall

Description: This rule takes effect when a configuration is changed or removed from the device. Juniper Firewall.

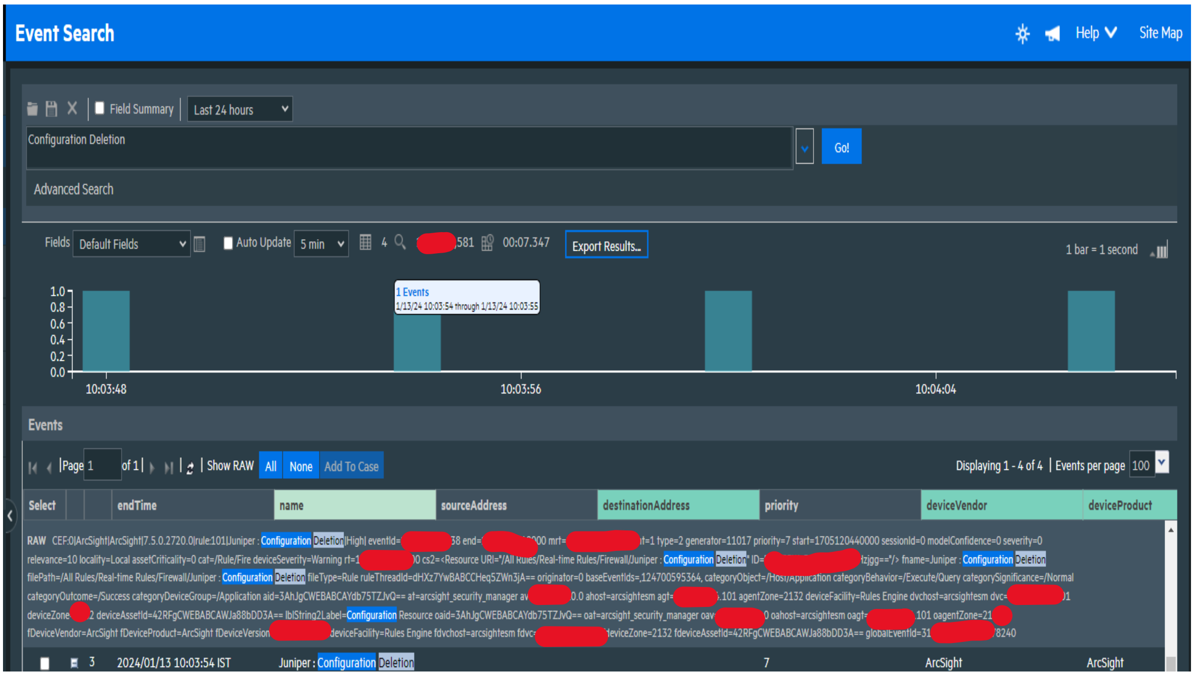
Impact: Critical policies that are deleted may prevent legitimate users from using the application, disrupt internal communications, and have an impact on crucial transactions.

Action taken by SOC Team

a. Verify whether it is a legitimate action or not from log or concern with team.
b. After identifying the installed/Edited/Deleted policy no, User, and Fortinet device,
c. immediately raise a concern with the Network/Firewall team to get the justification (Like, CR details and required approval).
d. Following ticket resolution, the SOC team updated their analysis. After ticket would be resolved successfully
e. If not Identify the reason and take appropriate action.

Practical Steps:-

a. Review logs to know which policy has been deleted.



Configuration Deletion

4 [redacted]581 00:07.347

Select			endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct

```
RAW  CEF:0|ArcSight|ArcSight|7.5.0.2720.0|rule:101|Juniper : Configuration Deletion|High| eventId=[redacted]38 end=[redacted]000 mrt=[redacted]t=1 type=2 generator=11017 priority=7 start=1705120440000 sessionId=0 modelConfidence=0 severity=0
relevance=10 locality=Local assetCriticality=0 cat=/Rule/Fire deviceSeverity=Warning rt=1[redacted]0 cs2=<Resource URI="/All Rules/Real-time Rules/Firewall/Juniper : Configuration Deletion" ID=[redacted]zjgg=="/> fname=Juniper : Configuration Deletion
filePath=/All Rules/Real-time Rules/Firewall/Juniper : Configuration Deletion fileType=Rule ruleThreadId=dHXz7YwBABCCHeq5ZWn3jA== originator=0 baseEventIds=,124700595364, categoryObject=/Host/Application categoryBehavior=/Execute/Query categorySignificance=/Normal
categoryOutcome=/Success categoryDeviceGroup=/Application aid=3AhJgCWEBABCAYdb75TZJvQ== at=arcsight_security_manager av[redacted]0.0 ahost=arcsightesm agt=[redacted].101 agentZone=2132 deviceFacility=Rules Engine dvchost=arcsightesm dvc=[redacted]01
deviceZone[redacted]2 deviceAssetId=42RFgCWEBABCAWJa88bDD3A== lblString2Label=Configuration Resource oaid=3AhJgCWEBABCAYdb75TZJvQ== oat=arcsight_security_manager oav[redacted]0 oahost=arcsightesm oagt=[redacted].101 oagentZone=21[redacted]
fDeviceVendor=ArcSight fDeviceProduct=ArcSight fDeviceVersion[redacted]deviceFacility=Rules Engine fdvchost=arcsightesm fdvc=[redacted]deviceZone=2132 fdeviceAssetId=42RFgCWEBABCAWJa88bDD3A== globalEventId=31[redacted]8240
```

Select			endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct
□		3	2024/01/13 10:03:54 IST	Juniper : Configuration Deletion			7	ArcSight	ArcSight

a. Check with Network team and raise an incident and assign to network team.
b. C. Get CR no from network team to verify in ITSM for the same.
c. Following ticket resolution, the SOC team updated their analysis. After ticket would be resolved successfully

5.5 Multiple High Priority Attacks found

Monitors the alerts when multiple high priority attacks found

Description: This rule executes when traffic goes to Tipping Point (IPS) with high priority volume

Impact: Multiple high-priority attacks can affect an organization's operations by interfering with its services and preventing authorized users from accessing them at critical moments.

Action taken by SOC Team

a. Soc will identify from which IP/IPs high priority alert is coming in large volume.

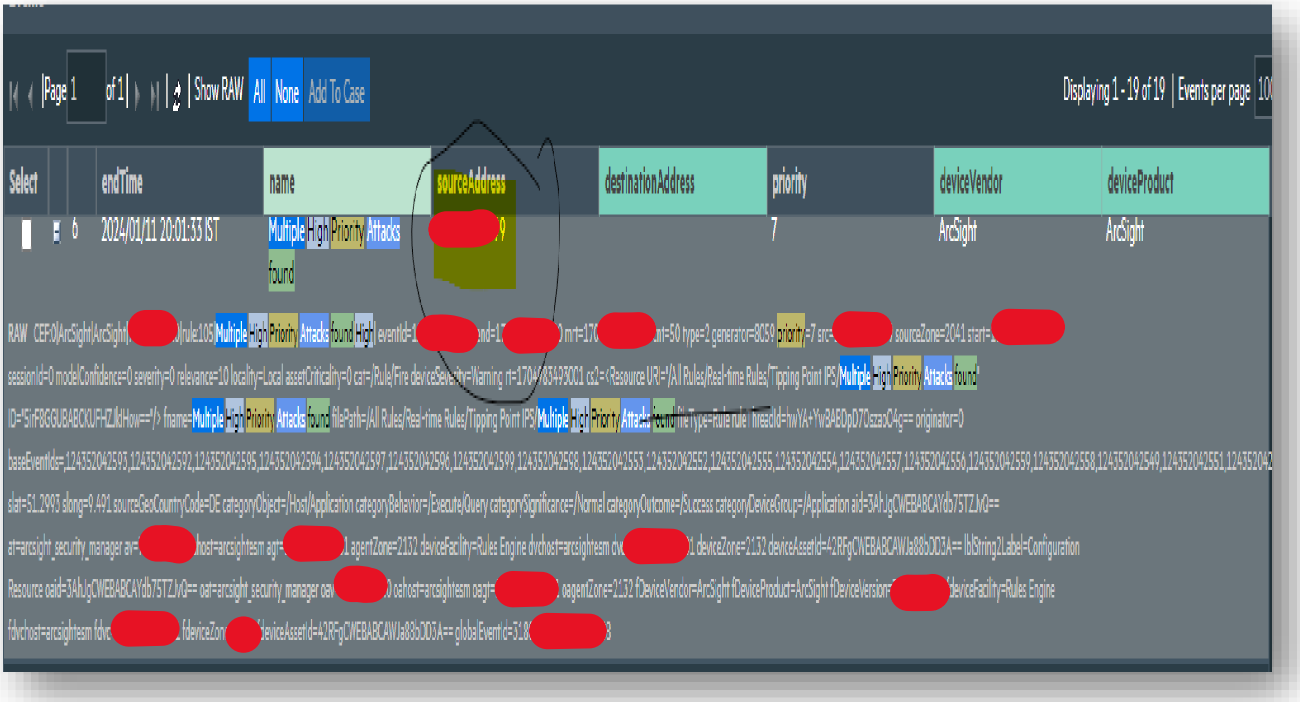
b. Check the IP address for the IP reputation.

c. Check in logs the IP address is blocked or not in Firewall.

d. If IPs address is not blocked, Soc will notify network team and raise one incident to block in perimeter firewall.

Practical Steps:-

a. Soc will identify from which IP/IPs high priority alert is coming in large volume.

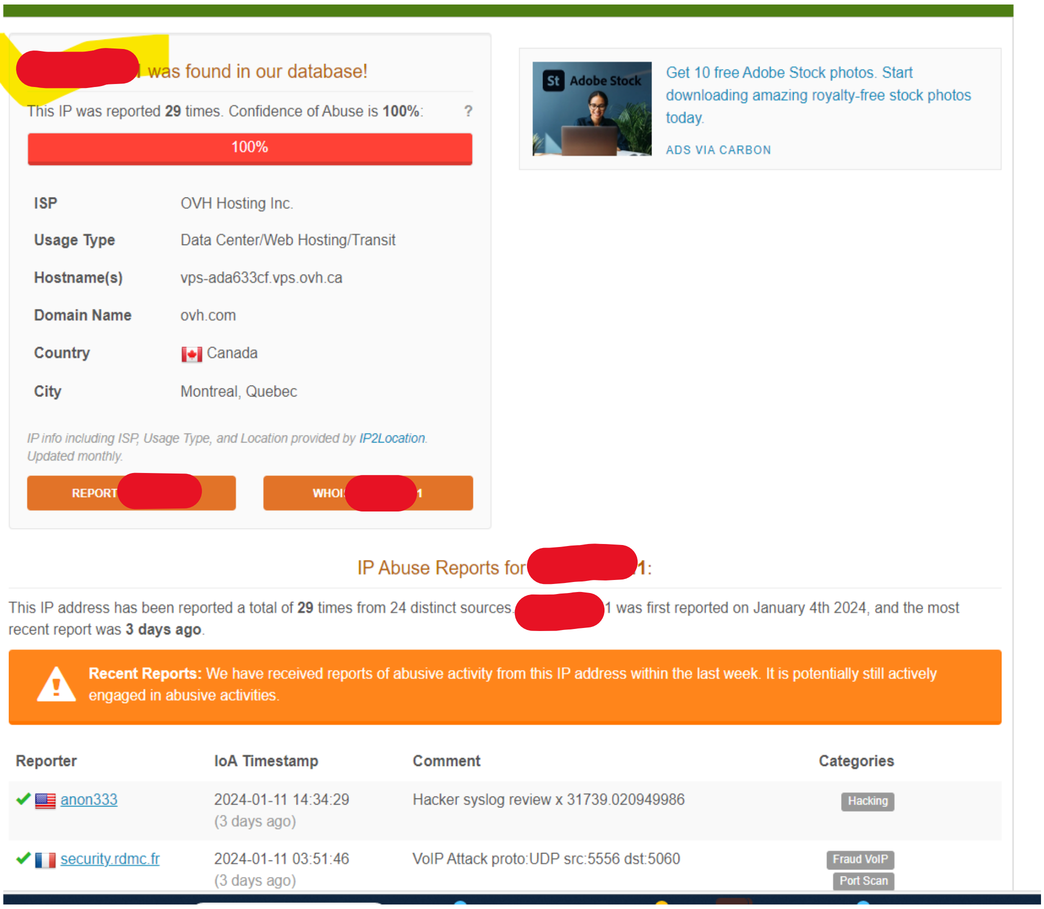


|◀ ◀ |Page 1 of 1| ▶ ▶| | Show RAW All None Add To Case — Displaying 1 - 19 of 19 | Events per page 10

Select			endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct
□		6	2024/01/11 20:01:33 IST	Multiple High Priority Attacks found	[redacted]9		7	ArcSight	ArcSight

```
RAW  CEF:0|ArcSight|ArcSight|[redacted]|rule:105|Multiple High Priority Attacks found|High| eventId=1[redacted]nd=1[redacted] mrt=170[redacted]nt=50 type=2 generator=8059 priority=7 src=[redacted] sourceZone=2041 start=1[redacted]
sessionId=0 modelConfidence=0 severity=0 relevance=10 locality=Local assetCriticality=0 cat=/Rule/Fire deviceSeverity=Warning rt=1704983493001 cs2=<Resource URI='/All Rules/Real-time Rules/Tipping Point IPS/Multiple High Priority Attacks found'
ID="5irF8GGUBABCKUFHZJkHow=="/> fname=Multiple High Priority Attacks found filePath=/All Rules/Real-time Rules/Tipping Point IPS/Multiple High Priority Attacks found fileType=Rule ruleThreadId=hwYA+YwBABDpD7OszaO4g== originator=0
baseEventIds=124352042593,124352042592,124352042595,124352042594,124352042597,124352042596,124352042599,124352042598,124352042553,124352042552,124352042555,124352042554,124352042557,124352042556,124352042559,124352042558,124352042549,124352042551,12435204
slat=51.2993 slong=9.491 sourceGeoCountryCode=DE categoryObject=/Host/Application categoryBehavior=/Execute/Query categorySignificance=/Normal categoryOutcome=/Success categoryDeviceGroup=/Application aid=3AhJgCWEBABCAYdb75TZJvQ==
at=arcsight_security_manager av=[redacted]host=arcsightesm agt=[redacted]1 agentZone=2132 deviceFacility=Rules Engine dvchost=arcsightesm dv[redacted]1 deviceZone=2132 deviceAssetId=42RFgCWEBABCAWJa88bDD3A== lblString2Label=Configuration
Resource oaid=3AhJgCWEBABCAYdb75TZJvQ== oat=arcsight_security_manager oav[redacted]0 oahost=arcsightesm oagt=[redacted] oagentZone=2132 fDeviceVendor=ArcSight fDeviceProduct=ArcSight fDeviceVersion=[redacted]fdeviceFacility=Rules Engine
fdvchost=arcsightesm fdvc[redacted] fdeviceZon[redacted]fdeviceAssetId=42RFgCWEBABCAWJa88bDD3A== globalEventId=318[redacted]8
```

b. Check the IP address for the IP reputation



[redacted] was found in our database!

This IP was reported **29** times. Confidence of Abuse is **100%**: ?

100%

ISP	OVH Hosting Inc.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	vps-ada633cf.vps.ovh.ca
Domain Name	ovh.com
Country	Canada
City	Montreal, Quebec

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

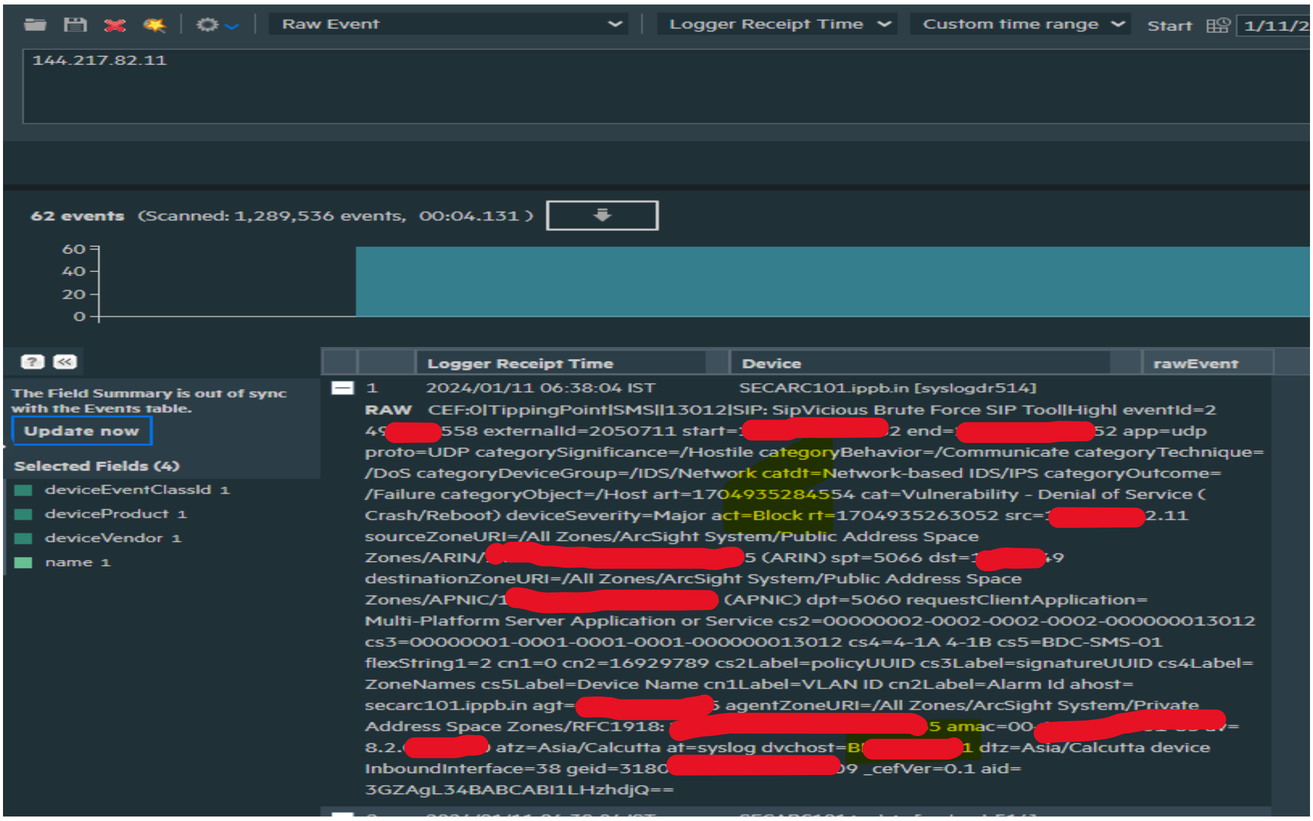
IP Abuse Reports for [redacted]1:

This IP address has been reported a total of **29** times from 24 distinct sources. [redacted]1 was first reported on January 4th 2024, and the most recent report was **3 days ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
✓ anon333	2024-01-11 14:34:29 (3 days ago)	Hacker syslog review x 31739.020949986	Hacking
✓ security.rdmc.fr	2024-01-11 03:51:46 (3 days ago)	VoIP Attack proto:UDP src:5556 dst:5060	Fraud VoIP Port Scan

c. Check in logs the IP address is blocked or not in Firewall



```
144.217.82.11
```

62 events (Scanned: 1,289,536 events, 00:04.131)

The Field Summary is out of sync with the Events table.

Selected Fields (4)

- deviceEventClassId 1
- deviceProduct 1
- deviceVendor 1
- name 1

```
   Logger Receipt Time        Device                               rawEvent
1  2024/01/11 06:38:04 IST    SECARC101.ippb.in [syslogdr514]
RAW  CEF:0|TippingPoint|SMS||13012|SIP: SipVicious Brute Force SIP Tool|High| eventId=2
49[redacted]558 externalId=2050711 start=[redacted]2 end=[redacted]52 app=udp
proto=UDP categorySignificance=/Hostile categoryBehavior=/Communicate categoryTechnique=
/DoS categoryDeviceGroup=/IDS/Network catdt=Network-based IDS/IPS categoryOutcome=
/Failure categoryObject=/Host art=1704935284554 cat=Vulnerability - Denial of Service (
Crash/Reboot) deviceSeverity=Major act=Block rt=1704935263052 src=[redacted]2.11
sourceZoneURI=/All Zones/ArcSight System/Public Address Space
Zones/ARIN/[redacted]5 (ARIN) spt=5066 dst=[redacted]9
destinationZoneURI=/All Zones/ArcSight System/Public Address Space
Zones/APNIC/1[redacted] (APNIC) dpt=5060 requestClientApplication=
Multi-Platform Server Application or Service cs2=00000002-0002-0002-0002-000000013012
cs3=00000001-0001-0001-0001-000000013012 cs4=4-1A 4-1B cs5=BDC-SMS-01
flexString1=2 cn1=0 cn2=16929789 cs2Label=policyUUID cs3Label=signatureUUID cs4Label=
ZoneNames cs5Label=Device Name cn1Label=VLAN ID cn2Label=Alarm Id ahost=
secarc101.ippb.in agt=[redacted]5 agentZoneURI=/All Zones/ArcSight System/Private
Address Space Zones/RFC1918: [redacted]5 amac=00[redacted]=
8.2.[redacted] atz=Asia/Calcutta at=syslog dvchost=B[redacted]1 dtz=Asia/Calcutta device
InboundInterface=38 geid=3180[redacted]09 _cefVer=0.1 aid=
3GZAgL34BABCABI1LHzhdjQ==
```

d. If IPs address is not blocked, Soc will notify network team and raise one incident to block in perimeter firewall.

Chapter 7: Conclusion

Since then, the cyber security threat has led to a huge loss in terms of consumer loyalty, security, confidentiality, credibility, and accessibility for many organisations, in the Industrial Internet of Things (IIOT). To initiate a cyber-attack is progressed, organisations need a more proactive strategy for detecting and retrieving potential events. The results of the project would allow any organisation to create their own software, while mitigating the impact of cyber-attacks, to improve the framework for future analysis. For future work, the SIEM system engine is used to model a threat to real life by designing some correlation rules that will be integrated into the system.

The main objective of this work is to identify and compile the current state of the art of SOCs along with their components. We used the relevant literature and defined state of the art to identify major challenges that hinder further developments and innovations for SOC's. The challenges can also serve as a guidelines for future research aiming to improve SOC's.

Therefore, SIEM is a technology that aggregates logs via data correlation allowing security analyst to shift through tonnes of information by network devices. Security concerns can be sorted by risk factor providing immediate action to reduce the attack surface and provide network health. Splunk is armed with features and capabilities to combat suspicious network activity while generating report to logs to adhere to industry policies and procedures.

Hence, the implementation of a SIEM solution is crucial for organisations seeking to ensure robust network security. By leveraging the capabilities of SIEM, organisation can detect threats proactively, meet compliance requirements, and enhace their overall security posture in todays's complex threat landscape.

Chapter 8 : Future Works

Predictive analysis represents the future of cybersecurity. By using machine learning algorithms to analyse data, organisations can detect potential threats before they occur and stay ahead of the game. SIEM solutions that utilise predictive analytics offer several benefits over traditional SIEM, using early detection of threats, better accuracy, increased efficiency and scalability.

However, as threats become more sophisticated, SIEM solutions must evolve to keep up. The future of SIEM lies in predictive analytics and machine learning, which can help organizations prevent attacks before the occur.

What is predictive analysis?

Predictive analysis is a type of advanced analytics that uses statistical modeling, data mining techniques and ML to forecast future outcomes based on historical data. Companies use it to identify risks and oppurtunities by finding patterns in data.

Predictive analytics is linked with big data and data science. Nowdays, organisations have a large amount of data in different repositories, and data scientists extracts insights using deep learning and ML algorithms. Techniques such as logistic and linear regression models, neural networks and decision trees are used to make predictions. These modelling techniques use initial predictive learnings to make additional predictive insights.

Benefits of predictive analysis in SIEM

There are several benefits of predictive analytics in SIEM over traditional SIEM solutions:

Early detection of threats: By using machine learning algorithm to analyse data, predictive analytics can identify potential threats before they occur. This allows organisations to take proactive measures to not only prevent attacks but also minimise the impact of security incidents.

Better accuracy : with predictive analytics, SIEM solutions can analyse large volumes of data and identify patterns that may be missed by human analysts or traditional SIEM solutions. This improves the accuracy of threat detection and reduces false positives significantly.

Increased efficiency: By automating data science and data engineering tasks, predictive analytics can free up IT and security teams to focus on more strategic tasks, such as incident planning and threat hunting.

Examples of predictive analytics in SIEM

User end entity behaviour analytics (UEBA)

UEBA is a type of security software designed to identify abnormal and potentially harmful user end device behaviour using behavioural analytics, ML algorithms and automation. UEBA is especially effective at detecting insider threats, which might go unnoticed by other security tools since they mimic authorised network traffic.
SIEM solutions collect security event data from multiple internal security tools, aggregate it into single log and analyse it to identify unusual behaviour and potential threats. UEBA can enhance SIEMs visibility into the network by detecting insider threat and analysing user behaviour.

Network detection and response(NDR)

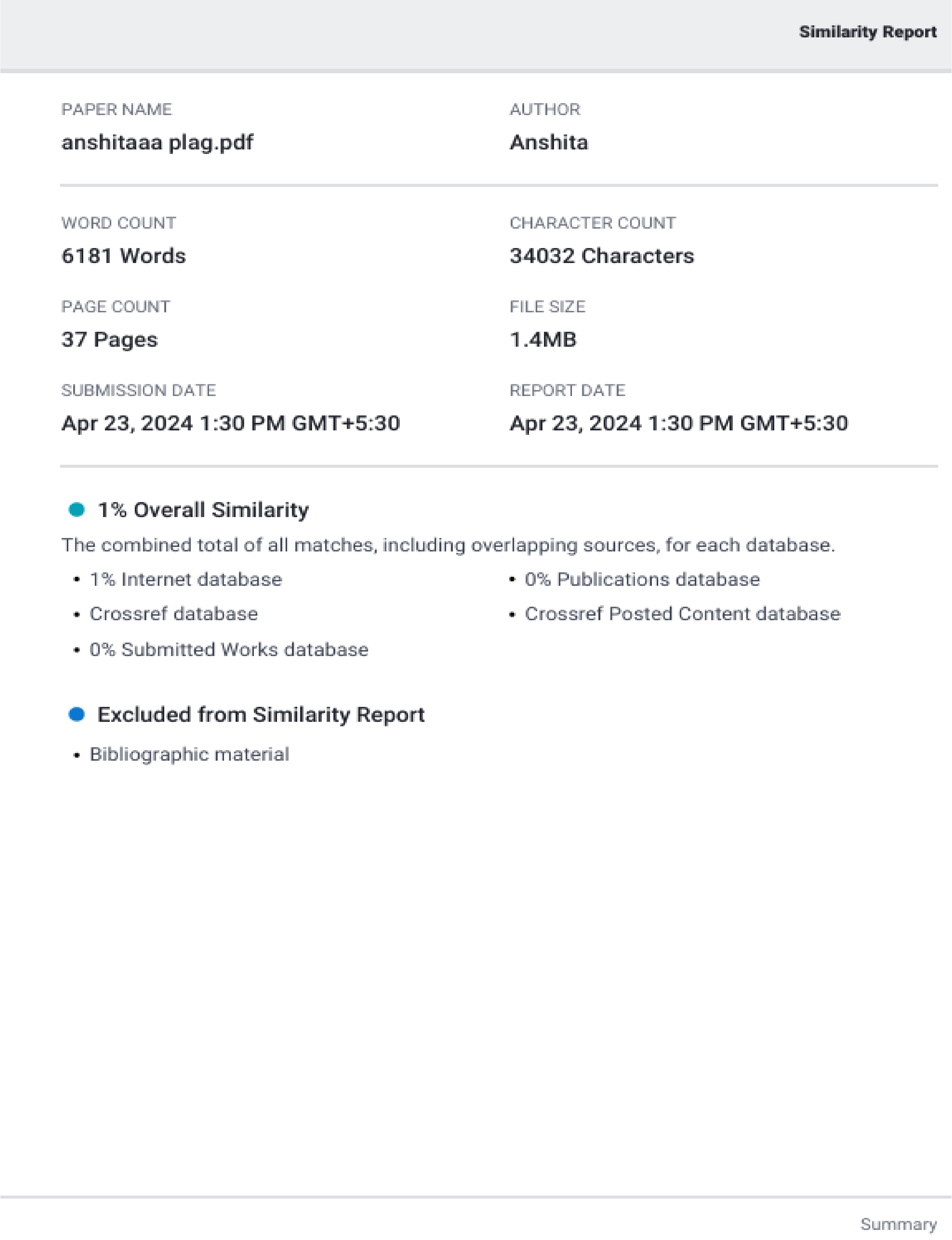
NDR is a cybersecurity event data that employs non signature based methods, including AI, ML and behavioural analytics, to detect and respond to suspicious or malicious activities in identifying threats that might go unnoticed by traditional security tools that rely on signature based detection.

By integrating NDR tools with SIEM, organisations can enhance their security and regulatory compliance workflows. NDR tools can stream network traffic data and analysis to a SIEM, providing valuable insights.

References

Sno.	References
1.	ESM install guide
2.	Implementation step logics web
3.	Research paper- 09296846
4.	IJNAA Volume 12 issue 2 Pages 869-895
5.	ISOC handbook
6.	www.postman.com

Plagiarism Report



Similarity Report

PAPER NAME

anshitaaa plag.pdf

AUTHOR

Anshita

WORD COUNT

6181 Words

CHARACTER COUNT

34032 Characters

PAGE COUNT

37 Pages

FILE SIZE

1.4MB

SUBMISSION DATE

Apr 23, 2024 1:30 PM GMT+5:30

REPORT DATE

Apr 23, 2024 1:30 PM GMT+5:30

● 1% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 1% Internet database
- Crossref database
- 0% Submitted Works database
- 0% Publications database
- Crossref Posted Content database

● Excluded from Similarity Report

- Bibliographic material

Summary

इंडिया पोस्ट पेमेन्ट्स बैंक

India Post Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

FORTNIGHTLY PROGRESS REPORT (FPR) FROM INDUSTRY MENTOR

Name of student	Anshita Singh		Department		
Industry/Organization	IPPB		Date/Duration	~~12/01/24 -12/03/24~~ 12/01/24 — 27/01/24	
Criterion	Poor	Average	Good	Very Good	Excellent
Punctuality/Timely completion of assigned work			Good		
Learning capacity/Knowledge upgradation					Excellent
Performance/Quality of work					Excellent
Behaviour/Discipline/Teamwork				Very Good	
Sincerity/Hard work				Very Good	
Comment on the nature of work done/Area/Topic	Security Operation Center- Overview and understanding				
OVERALL GRADE (Any one)	**VERY GOOD**				
Name of Industry Mentor	Ankush Vilhekar				
Signature of Industry Mentor	Vilhkar				

Receiving Date	22/2/24	Name of Faculty Mentor	DR.R.S.Jadon	Sign	

इंडिया पोस्ट पेमेन्ट्स बैंक

India Post Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

FORTNIGHTLY PROGRESS REPORT (FPR) FROM INDUSTRY MENTOR

Name of student	Anshita Singh		Department		
Industry/Organization	IPPB		Date/Duration	~~12/01/24 -12/03/24~~ 28/01/24 TO 14/02/24	
Criterion	Poor	Average	Good	Very Good	Excellent
Punctuality/Timely completion of assigned work			Good		
Learning capacity/Knowledge upgradation					Excellent
Performance/Quality of work					Excellent
Behaviour/Discipline/Teamwork				Very Good	
Sincerity/Hard work				Very Good	
Comment on the nature of work done/Area/Topic	Security Operation Center- Overview and understanding				
OVERALL GRADE (Any one)	**VERY GOOD**				
Name of Industry Mentor	Ankush Vilhekar				
Signature of Industry Mentor	AVilhkar				

Receiving Date	22/2/24	Name of Faculty Mentor	DR. R.S. Jadon	Sign	

इंडिया पोस्ट पेमेन्ट्स बैंक

India Post Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

FORTNIGHTLY PROGRESS REPORT (FPR) FROM INDUSTRY MENTOR

Name of student	Anshita Singh		Department		
Industry/Organization	IPPB		Date/Duration	15/02/24 -29/02/24	
Criterion	Poor	Average	Good	Very Good	Excellent
Punctuality/Timely completion of assigned work				Very Good	
Learning capacity/Knowledge upgradation					Excellent
Performance/Quality of work					Excellent
Behaviour/Discipline/Teamw ork					Excellent
Sincerity/Hard work				Very Good	
Comment on the nature of work done/Area/Topic	Security Operation Center- Cyber security tools				
OVERALL GRADE (Any one)	VERY GOOD				
Name of Industry Mentor	Ankush Vilhekar				
Signature of Industry Mentor					

Receiving Date	14/03/24	Name of Faculty Mentor	DR. R.S. Jadon	Sign	

इंडिया पोस्ट पेमेन्ट्स बैंक
India Post Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

FORTNIGHTLY PROGRESS REPORT (FPR) FROM INDUSTRY MENTOR

Name of student	Anshita Singh		Department		
Industry/Organization	IPPB		Date/Duration	01/03/24 -12/03/24	
Criterion	Poor	Average	Good	Very Good	Excellent
Punctuality/Timely completion of assigned work				Very Good	
Learning capacity/Knowledge upgradation					Excellent
Performance/Quality of work					Excellent
Behaviour/Discipline/Teamw ork				Very Good	
Sincerity/Hard work					Excellent
Comment on the nature of work done/Area/Topic	Security Operation Center- connecting and implementing SIEM with tools				
OVERALL GRADE (Any one)	VERY GOOD				
Name of Industry Mentor	Ankush Vilhekar				
Signature of Industry Mentor					

Receiving Date	14/03/24	Name of Faculty Mentor	DR. R. S. Jadon	Sign	

इंडिया पोस्ट पेमेन्ट्स बैंक

India Post Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

FORTNIGHTLY PROGRESS REPORT (FPR) FROM INDUSTRY MENTOR

Name of student	Anshita Singh		Department		
Industry/Organization	IPPB		Date/Duration	13/03/24 -31/03/24	
Criterion	Poor	Average	Good	Very Good	Excellent
Punctuality/Timely completion of assigned work					Excellent
Learning capacity/Knowledge upgradation					Excellent
Performance/Quality of work					Excellent
Behaviour/Discipline/Teamw ork				Very Good	
Sincerity/Hard work					Excellent
Comment on the nature of work done/Area/Topic	Security Operation Center- connecting and implementing SIEM with tools				
OVERALL GRADE (Any one)	VERY GOOD				
Name of Industry Mentor	Ankush Vilhekar				
Signature of Industry Mentor	Vilhkar				

Receiving Date	24/04/24	Name of Faculty Mentor	R.S. Jadon	Sign	

इंडिया पोस्ट
पेमेन्ट्स बैंक

India Post
Payments Bank

[भारत सरकार का उपक्रम | A Govt. of India undertaking]

FORTNIGHTLY PROGRESS REPORT (FPR) FROM INDUSTRY MENTOR

Name of student	Anshita Singh		Department		
Industry/Organization	IPPB		Date/Duration	01/04/24 -15/04/24	
Criterion	Poor	Average	Good	Very Good	Excellent
Punctuality/Timely completion of assigned work					Excellent
Learning capacity/Knowledge upgradation					Excellent
Performance/Quality of work					Excellent
Behaviour/Discipline/Teamw ork				Very Good	
Sincerity/Hard work					Excellent
Comment on the nature of work done/Area/Topic	Security Operation Center- connecting and implementing SIEM with tools				
OVERALL GRADE (Any one)	VERY GOOD				
Name of Industry Mentor	Ankush Vilhekar				
Signature of Industry Mentor	Vilhkar				

Receiving Date	24/04/24	Name of Faculty Mentor	R.S. Jadon	Sign	