AN INTELLIGENT CYBER SECURITY DETECTION AND RESPONSE PLATFORM

Song Zhuo[1]*, Yang Yu Hong[2], Thelma D. Palaoag[3]

[1,2,3]University of the Cordilleras*

Corresponding Author: -
songzhuo360@gmail.com

ABSTRACT:

To further solve the cyber security challenges faced by the digital transformation of the Philippines university industry. This paper designed and proposed a cyber-security detection and response platform (CSDRP), which can deal with traditional network security problems, improve the network security management capabilities of universities, and provide a method for real-time monitoring of network status and network security response in universities. With the outbreak of the epidemic, many universities in the Philippines have launched online courses and online services. These online courses and online services continue to proliferate, and with them come a host of cyber security risks and hidden dangers.

CSDRP extracts logs through the traffic probes, and the platform performs correlation analysis on many security logs, combines relevant models and machine learning algorithms and generates response logs, which can be responded to and linked with policies, and finally presents relevant threats visually. This study deploys the platform in the actual network environment. The experimental results show that it provides accurate threat warnings, as well as good real-time detection and visualization of cyber threats, and can collect logs from different data sources in real time. Linkage of safety equipment.

KEYWORDS: *Cyber security; Security detection; Security response; Risk assessment; CSDRP;*

1. INTRODUCTION

Nowadays, the scale of campus network construction in universities continues to expand, the network scale is huge while the cyber security protection is inconsistent. The security awareness of campus network users is weak, and the security risks of the campus network are prominent. With the outbreak of covid-19, the use of online systems has also become more common at many universities in the Philippines. At the same time, cyber security threats and hidden dangers at all levels are also increasing. The threats and losses caused by network viruses and DOS/DOS attacks are immeasurable [1]. Cybersecurity attacks are quite complex, and the IT department of universities are hard to take measures to protect their network. Most of the network administrator only rely on a single network security device or single protection technology, such as a firewall, anti-virus software, and other network security facilities, it can no longer adapt to the current complex network security work. The administrators also lack a good cyber threat visualization tool to help them better monitor the threats.

Through comparing and studying the related research papers, it can be seen that the traditional attack and defense methods are single and fragile [2]. While the cybercrimes and cyberattacks are by nature borderless [3]. The traditional cyber security defense of the administrator is mainly to set up security devices such as a firewall between the internal LAN and the external Internet. Subconsciously, the internal network of the LAN is considered safe, as long as attacks from the Internet are prevented, the normal operation of the network can be guaranteed, only few information can be used to detect and prevent attacks [4]. However, once the intranet host is infected, the attack will expand horizontally, causing the entire intranet host to be paralyzed and causing serious losses to intranet services [5]. The traditional network security architecture has the problem of lagging network risk perception [6]. Traditional defenses focus on cyber-attack issues discovered after detecting hits in databases of known static signatures. When the new trend of cyber threats such as a 0-day attack, APT attacks, and dynamic signature viruses appear, traditional security defense methods will not be able to cope. Once a new threat or mutant virus breaks through the border defense, the network lacks effective detection and response capabilities, making it difficult to quickly find out them [7][8]. Various network security devices exist independently in the server system, and each has its security protection strategy, such as abnormal network behavior management tools, intrusion detection, and endpoints security platform [9]. When a cyber-security attack happens, the administrators need to log in to the different network security devices by themselves and check them one by one, which is cumbersome, time-consuming, and laborious work [10]. The traditional Net Flow method lacks an intuitive display of the running status [11]. The operation of traditional network security devices only supports command lines or simple webpage operations and lacks a friendly interactive interface or visual display interface in the display of operation effects. To address the challenging issues, this paper proposed a Cyber Security Detection and Response Platform (CSDRP) based on security logs detection and analysis of core switch traffic. The research data collection part is based on the deployment of Shenxinfu SIP products for relevant log acquisition and analysis. The CSDRP is like a security commander for end users, it aims to design and propose a security event analysis platform that integrates detection, analysis, and response processing. To visualize the threat data and provide more meaningful information, this platform can also provide corresponding threat alarms and a visualized threat platform, and at the same time, it also can support having a correlation response with other related security devices inside the network.

2. Methodology

The CSDRP architecture includes three parts: the logs collection layer, the data analysis layer, and the data visualization layer.

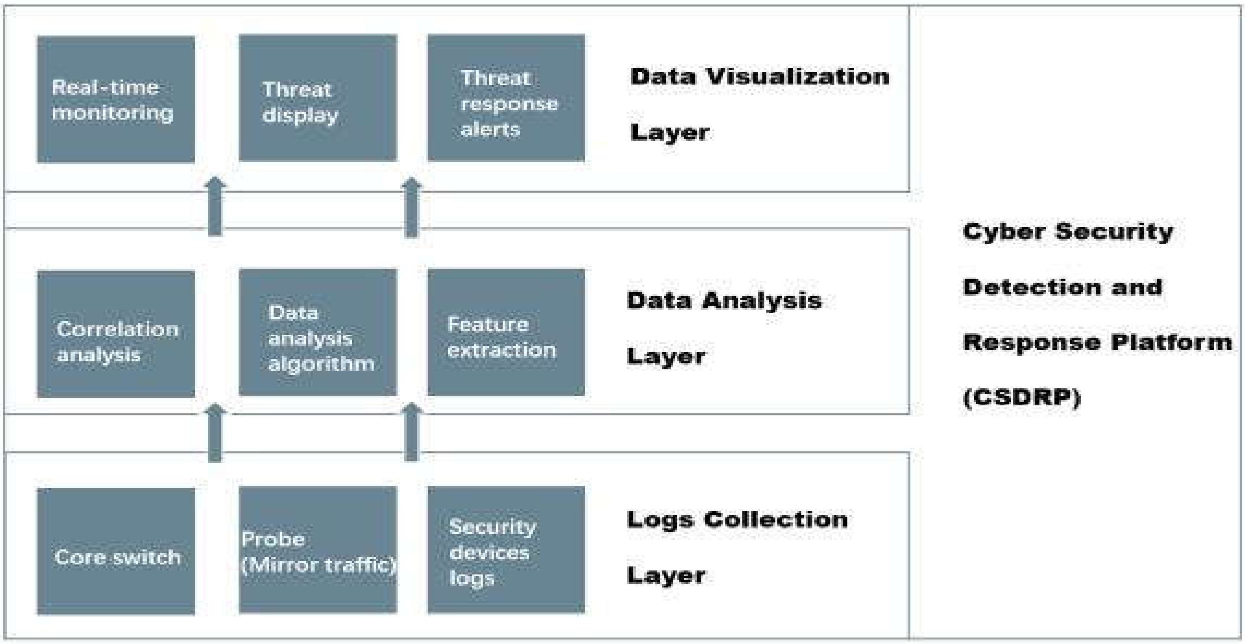


Fig. 1. The CSDRP platform architecture design

A. Logs collection layer

The most important component of the data collection layer is the traffic monitoring probe. As a traffic collection device, the probe is connected with devices that have bypass mirroring functions such as switches and processes the mirrored traffic and inputs data to the platform. And mirror all core switch traffic. The entire network environment generally includes many terminal devices, such as servers, hosts, firewalls, IoT devices, and so on. Various devices in the network environment generate a large amount of log information in real-time, and the traffic of the core switch is mixed with a lot of noise traffic. After the probe is deployed, it can directly obtain all the traffic passing through the switch, capture log data from multi-level, multi-angle, and multi-granularity, and obtain all security information that affects campus network security as the basis of the second data analysis layer. It is also the prerequisite for the analysis and visualization of the entire platform.

The Logs collection layer is mainly responsible for collecting massive heterogeneous data related to security logs, which are mainly divided into two types: one is device log information, which is characterized by massive and heterogeneous data, including device operating status, running Performance data, various logs, and events, Flow stream data, etc.; the other type is communication log information, including common communication request logs, intranet traffic, media streams, etc. The entire Logs collection layer probes the log data collected mainly from the core switch and goes through data preprocessing, data caching, and other stages；

Log collection stage: For the two types of data described above, probes may obtain terminal data, middleware data, third-party device logs, threat intelligence docking, etc., and finally send them to the platform layer. The probe generally directly obtains the traffic of the switch, but it can also directly interface with different traffic and log data through the API layer and supports collection in Syslog, web service, restful API, and Wmi. The metadata information generated by the probe enters the platform through ETL tools, and the security data of third-party devices enter the platform through logstash collection and processing;

Data preprocessing stage: Since the collected logs are too complex and noisy, the probe will first preprocess the collected data, including log information cleaning, log merging, and data reconstruction. After a series of data filtering operations, the probe platform will convert the processed data into formatted data that the platform can understand, and cache in the form of files. All security data is cached in the probe platform through Kafka's message queue;

Data caching and storage: After the data is processed, it has been cached in the probe platform in a specific format. The next step is to use machine learning techniques and trained machine learning models to analyze these security logs and data in specific formats. MapReduce [12] is used by many security detection platform designs as well.

B. Data analysis layer

After the security logs are analyzed, the data analysis layer will process the collected data. The data analysis layer will process the original data through association analysis, feature extraction, data fusion, etc. The platform will extract useful security data according to the defined keywords and data formats, and obtain an analysis of the overall security situation [13]. The entire data analysis layer will go through the stages of association analysis, machine learning model, big data analysis, data storage, and data call. Through the secondary analysis and processing of data, the functions of data analysis and mining can be finally completed.

Correlation analysis: In the network environment of universities, there are generally many security devices, such as firewalls, WAF, etc. Sometimes, we are faced with multi-source and multi-dimensional attack information, so we need to find correlations and causal links between different subsets and objects through association mining analysis. Analyze based on log rules, log statistics, asset attributes, etc. Inference and attack source tracing is performed according to the set restrictions and threshold associations.

SVM machine learning model: Due to the complexity, inconsistent format, and high noise of the logs collected by the probe. SVM is a good choice in environments flooded with large amounts of different types of security log data. SVM, Support Vector Machine is a machine learning model with fast and high error-tolerant classification performance and noise tolerance. SVM can improve the generalization ability of the model for data processing, and can greatly reduce the error for data samples. At the same time, the SVM machine learning algorithm combined with feature detection is applied to email security, which can more accurately detect threats such as forged emails and spam.

Big data analysis stage: For the processing of massive data, the platform will calculate the relevant data offline, or perform real-time computer calculations by reading ES (Elastic Search) data. The detection model constructed from big data can be used to discover unknown threats and suspicious behaviors, improve the detection rate, and provide a basis for threat tracking/hunting, etc.

Data storage stage: The CSDRP platform will store the analysis data and results in the ES engine (Elastic Search), thus providing fast retrieval capabilities for subsequent data calls. The platform stores the statistical result data that needs to be presented quickly in MongoDB in the next step, which can be read quickly. Compared with the ES engine, it does not require rendering and memory consumption. At the same time, the platform will call the Flink computing engine to process again. The original data such as logs and traffic returned by probes and third-party devices are finally stored in ES, and the security event analysis results of the preliminary analysis are stored in MongoDB;

Data call phase: The relevant logs stored in the platform have been processed into a platform-readable format after multi-layer processing. This processed data is then sent to the next layer for data visualization analysis. In the platform visualization layer, respectively call the above-generated alarm log, threat quantity, asset information, etc.

C. Data visualization layer

The entire data visualization display is based on web design. The first step is to call data from the data analysis layer and read and display relevant data. Secondly, by providing various data security visualization services and external interfaces, the JS framework is the mainstay, ECharts is used as a graphics library, and the Vue architecture is used as the basic design for large-screen visualization. The visualization platform mainly includes the following parts.

Alarm center: The alarm center includes equipment performance monitoring and analysis, traffic monitoring and analysis, user asset number detection, risk host, risk user analysis, historical security status, risk profile, etc.;

Threat monitoring: The threat monitoring module is for real-time monitoring of common security hotspot events, such as a 0-Day attack, ransomware, worms, and Trojan horses. It also includes monitoring of some common Web attack events, denial of service attack events, intrusion and control events, malicious program events, etc.

Asset analysis: asset analysis provides a module for the overview of intranet assets, including automatic statistics of potential assets and risk assets;

Linkage response: Configure linkage with third-party security products through the API interface, and can transmit relevant log information to other devices to realize joint handling of threat response.

3. The KEY model and technology

A. Key Model Analysis

System vulnerability analysis model: Obtain vulnerability scanning behavior characteristics and request characteristics such as vulnerability detection request type, request frequency, request source, vulnerability detection code, etc. by obtaining system host logs, network traffic logs, and other logs[14]. Establish a security analysis model for the attack behavior of system vulnerability scanning, accurately identify the system vulnerability scanning behavior, including the source IP of the attacker, attack time stamp, attack frequency, etc., and then judge whether there is a vulnerability risk based on whether there is a successful access log.

Web vulnerability analysis model: By analyzing IDS logs, web application access logs, network traffic logs, and other logs obtain vulnerability detection request type, request frequency, request source, vulnerability detection code, and other vulnerability scanning behavior characteristics and request characteristics, and accurately identify web application vulnerabilities Scanning behavior, establish a security analysis model for the scanning behavior of web application vulnerability scanning.

DoS/DDoS attack prevention model: By improving the DoS attack algorithm, it can defend against flooding attacks such as packets, IP protocol, TCP protocol, and HTTP-based DoS/DDoS attacks, detect various malformed packet attacks, and defend against IP/port scanning attacks. First, the abnormal TCP packets, IP option attacks, etc. include SYN floods, ICMP floods, UDP floods, and DNS query floods [15][16]. When the frequency of detected SYN packets is too high, ICMP flood attacks and other flood attacks are detected, to achieve Dos/DDos model improvement and network security protection;

SQL injection attack analysis model: establish a security analysis model for the SQL injection attack behavior of web applications, analyze the URL, URL, Input parameters, payload, and whether the attack is successful, etc., and detect successful SQL injection attacks in time to avoid further leakage of sensitive information.

Asset statistical analysis model: There are various devices connected in the network, and the asset statistical analysis model can be based on standardized asset information data (device name, IP address, port security service, operating system fingerprint, middleware, and Web server fingerprint, tripartite component software and hardware asset information such as fingerprints), SMP security management platform data (system and web vulnerability scan results, security configuration baseline verification results, general software version/patch information, etc.) to generate asset statistical reports and trend analysis.

B. Key Technology Analysis

In the entire CSDRP design process, how to obtain valid data from massive security logs and give corresponding alarms and responses is the most important part. This paper studies related key technologies such as User and Entity Behavior Analysis (UEBA) and the use of threat intelligence sharing framework.

a. UEBA

UEBA (User and Entity Behavior Analysis) aims to discover possible anomalies based on user or entity behavior analysis. UEBA is a technology that uses advanced data analysis methods to detect and investigate anomalies based on user and entity network behaviors. Perception (integrated with SIEM, or in SOC), or combined with insider security solutions such as Data Leakage Prevention (DLP) for more precise anomaly location, is an indispensable and important capability [17].

UEBA can identify different types of abnormal user behaviors and can analyze and predict abnormal behaviors based on group behaviors and group relationships. It can treat them as indicators of threats and intrusions, including analyzing anomalous behavior, spotting threats, and more. By analyzing the behavior of internal users and assets, continuous learning and behavior portrait construction are carried out on these objects, and the baseline portrait is used as an entry point to detect abnormal behaviors that are easy to baseline.

(1. Abnormal analysis based on group behavior.

When different types of servers are identified in the same group in the network environment, they may be infected with the same zombie worm to have similar group behavior. Combined with the identification basis, abnormalities can be found and the source of the problem can be located. This model can be extended to a behavior detection model for abnormal accounts.

(2. Predict future risk trends based on group relationship anomalies

For example, through the access relationship in the group, it is predicted whether the abnormal host or the compromised host will affect the core assets in the same group and whether the path to the core assets should be cut off.

b. Threat Intelligence Sharing Framework

Since this platform involves the analysis of related logs and threat warnings in combination with the signature database, it is required to conduct real-time analysis and comparison of traffic metadata collected in the local network, discover known threats and suspicious connection behaviors, and increase the accuracy and accuracy of intelligent analysis technology. The detection rate. For example, through behavior analysis, it is found that the communication behavior of covert tunnels (such as DNS tunnels) is only suspicious, but if the address information of the connection is associated with the zombie and worm intelligence of threat intelligence, it can be detected as remote control behavior through the analysis model. At the same time, the data sources of the platform are diversified, including Google VirusTotal, CnCert's ANVA data sharing, and data exchange and acquisition from other cloud platforms. The CSDRP platform can mine and extract these data to form accurately machine-readable and early warning threat intelligence.

c.Sensible Threat Alert Design

To facilitate operation and maintenance experience and security event analysis, the CSDRP platform innovatively designed perceivable security alarms to make threats easy to identify and understand.

(1. Labeling: In the form of labeling, each security event alarm is represented by a specific label, and each label provides a detailed description.

(2. Descriptive ratings: To make it easier to understand the importance and urgency of security incidents, the platform provides different descriptive ratings for each incident.

4. Deployment and evaluation

This section details the CSDRP implementation process, comprising the performance, functional validation use cases, and the scalability of the solution.

a. Implementation

CSDRP mainly includes two parts: a detection probe and a security log analysis platform. The Traffic Monitor Probe is bypassed to the switch, receives the mirrored traffic of the switch to collect and detect, and transmits the results to the platform through the network link for comprehensive analysis. CSDR Platform is used to receive and analyze logs. The network topology diagram of this implementation and test is as follows：

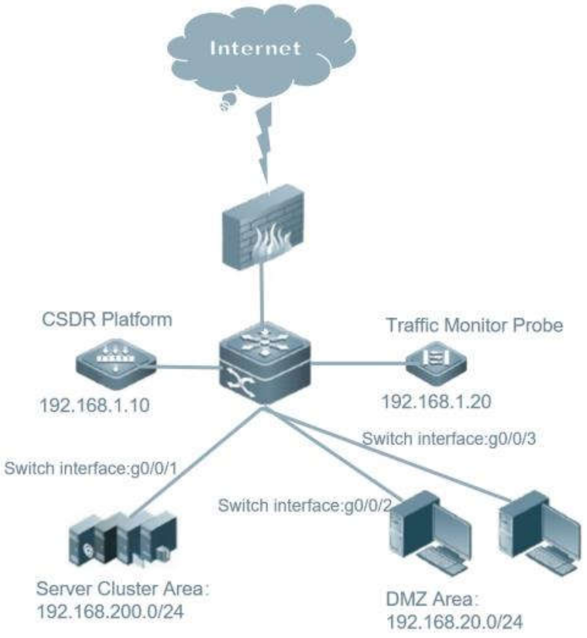


Fig. 2. The platform Implementation topology design

The entire network environment includes firewalls, core switches, user office DMZs, and server business areas. CSDRP is deployed in a virtual machine, The VM host is equipped with an Intel Xeon Silver 4210R CPU running at 2.40GHz, and 32GB RAM. Network connectivity is provided using a core switch, and the traffic monitor probe with the core switch is directly connected. During deployment, ensure that the two platforms are in the same network segment.
The IP address of CSDRP shall be communicated with the IP address of a probe management interface, to receive the data sent by the probe. The configuration IP address of the CSDRP eth0 interface is 192.168.1.100. The configuration IP address of the probe th0 interface is 192.168.1.20.

b. Testing
The test mainly focuses on the three aspects of threat detection and verification, visual display, and response linkage.

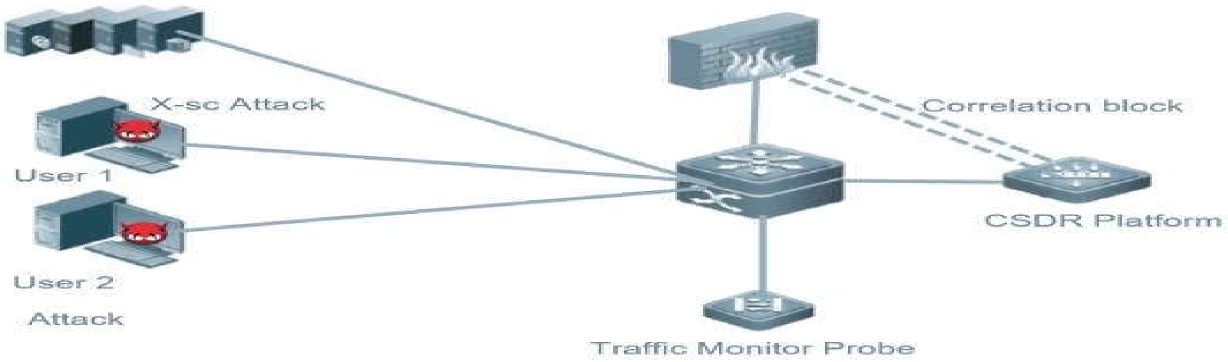
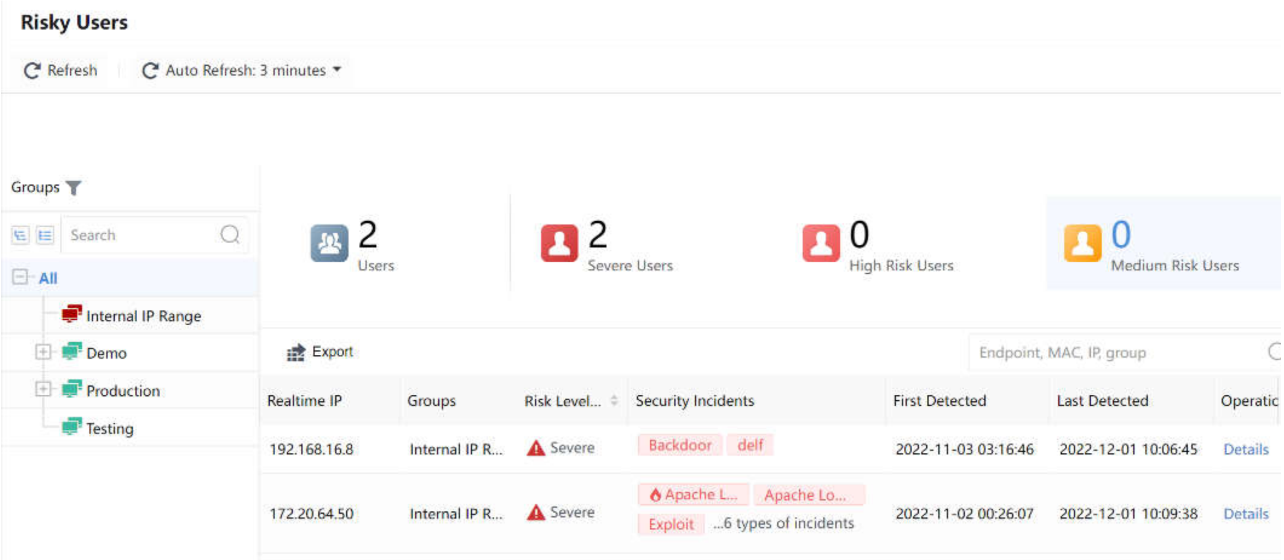


Fig. 3. The platform testing topology design

Threat detection:
To better verify the effectiveness and timeliness of CSDRP for threat virus detection, User 1 and User 2 placed the ransomware X-sc in advance and executed it. After some time, it was found that CSDRP had detected the threat of the ransomware virus and displayed the threat information on the dashboard of the platform。



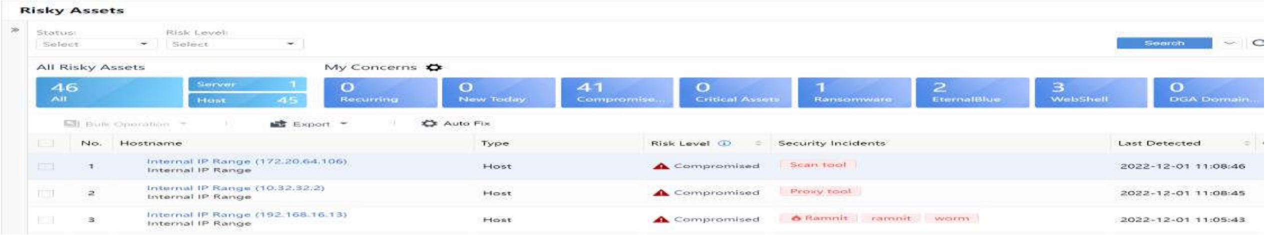
Risky Users

Realtime IP	Groups	Risk Level...	Security Incidents	First Detected	Last Detected	Operatic
192.168.16.8	Internal IP R...	Severe	Backdoor delf	2022-11-03 03:16:46	2022-12-01 10:06:45	Details
172.20.64.50	Internal IP R...	Severe	Apache L... Apache Lo... Exploit ...6 types of incidents	2022-11-02 00:26:07	2022-12-01 10:09:38	Details

Fig. 4. The platform Threat detection part

Visual analysis:

It can display both external and lateral attacks, illegitimate accesses, suspicious activities, and risky accesses initiated by risky hosts to internal hosts. It describes large-scope diffused activities after being controlled by hackers. The impact scope will be further expanded, affecting office effectiveness and service security. The suspicious activities, risky accesses, illegitimate accesses, and lateral attacks initiated by risky hosts to other hosts in the LAN can be viewed. The detailed log information of attacks also can be viewed.



Risky Assets

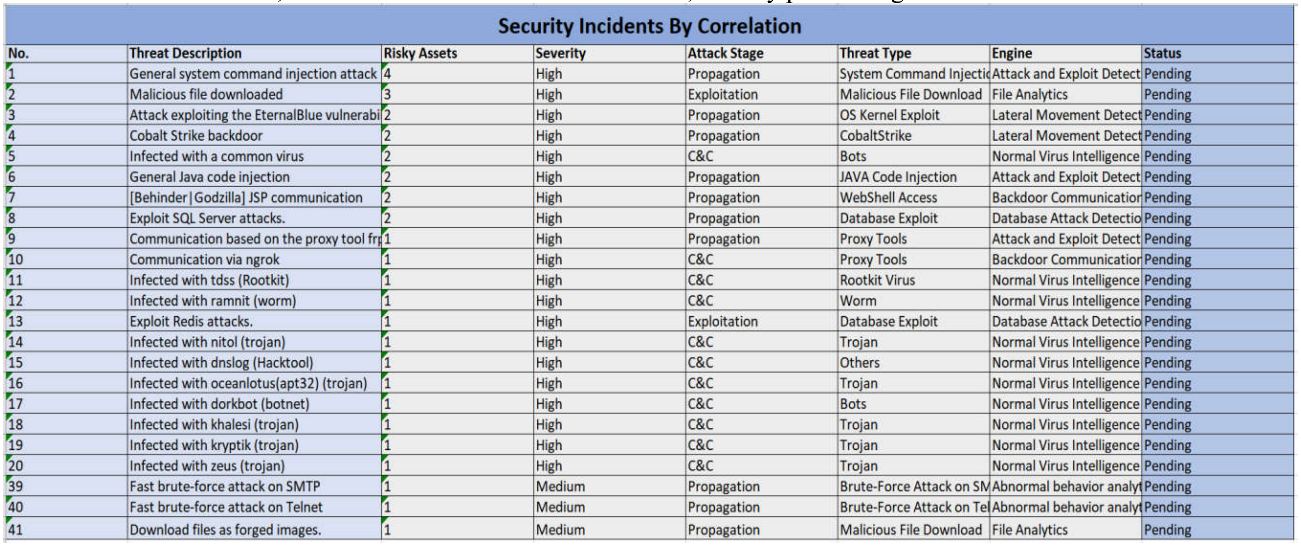
No.	Hostname	Type	Risk Level	Security Incidents	Last Detected
1	Internal IP Range (172.20.64.106) Internal IP Range	Host	Compromised	Scan tool	2022-12-01 11:08:46
2	Internal IP Range (10.32.32.2) Internal IP Range	Host	Compromised	Proxy tool	2022-12-01 11:08:45
3	Internal IP Range (192.168.16.13) Internal IP Range	Host	Compromised	Ramnit ramnit worm	2022-12-01 11:05:43

Fig. 5. The CSDRP platform visual analysis

Response linkage:

Block or perform access control on risky IP addresses through CSDRP and firewall, to alleviate harm to the hosts and server. As shown above, simulated viruses are placed in user hosts 1 and 2. During testing, after the security event occurs, the CSDRP will report the related logs to the firewall to block certain host or WAN IP addresses as a source or destination by using API. In this case, there are two attacks has detected that the

The host is infected with the prevailing External Blue, correlate with the firewall to block to prevent the virus from being transmitted from this host, and block the host as the virus source, thereby prohibiting the external connection behavior.



Security Incidents By Correlation

No.	Threat Description	Risky Assets	Severity	Attack Stage	Threat Type	Engine	Status
1	General system command injection attack	4	High	Propagation	System Command Injectic	Attack and Exploit Detect	Pending
2	Malicious file downloaded	3	High	Exploitation	Malicious File Download	File Analytics	Pending
3	Attack exploiting the EternalBlue vulnerabi	2	High	Propagation	OS Kernel Exploit	Lateral Movement Detect	Pending
4	Cobalt Strike backdoor	2	High	Propagation	CobaltStrike	Lateral Movement Detect	Pending
5	Infected with a common virus	2	High	C&C	Bots	Normal Virus Intelligence	Pending
6	General Java code injection	2	High	Propagation	JAVA Code Injection	Attack and Exploit Detect	Pending
7	[Behinder|Godzilla] JSP communication	2	High	Propagation	WebShell Access	Backdoor Communicatior	Pending
8	Exploit SQL Server attacks.	2	High	Propagation	Database Exploit	Database Attack Detectio	Pending
9	Communication based on the proxy tool fr	1	High	Propagation	Proxy Tools	Attack and Exploit Detect	Pending
10	Communication via ngrok	1	High	C&C	Proxy Tools	Backdoor Communicatior	Pending
11	Infected with tdss (Rootkit)	1	High	C&C	Rootkit Virus	Normal Virus Intelligence	Pending
12	Infected with ramnit (worm)	1	High	C&C	Worm	Normal Virus Intelligence	Pending
13	Exploit Redis attacks.	1	High	Exploitation	Database Exploit	Database Attack Detectio	Pending
14	Infected with nitol (trojan)	1	High	C&C	Trojan	Normal Virus Intelligence	Pending
15	Infected with dnslog (Hacktool)	1	High	C&C	Others	Normal Virus Intelligence	Pending
16	Infected with oceanlotus(apt32) (trojan)	1	High	C&C	Trojan	Normal Virus Intelligence	Pending
17	Infected with dorkbot (botnet)	1	High	C&C	Bots	Normal Virus Intelligence	Pending
18	Infected with khalesi (trojan)	1	High	C&C	Trojan	Normal Virus Intelligence	Pending
19	Infected with kryptik (trojan)	1	High	C&C	Trojan	Normal Virus Intelligence	Pending
20	Infected with zeus (trojan)	1	High	C&C	Trojan	Normal Virus Intelligence	Pending
39	Fast brute-force attack on SMTP	1	Medium	Propagation	Brute-Force Attack on SM	Abnormal behavior analyt	Pending
40	Fast brute-force attack on Telnet	1	Medium	Propagation	Brute-Force Attack on Tel	Abnormal behavior analyt	Pending
41	Download files as forged images.	1	Medium	Propagation	Malicious File Download	File Analytics	Pending

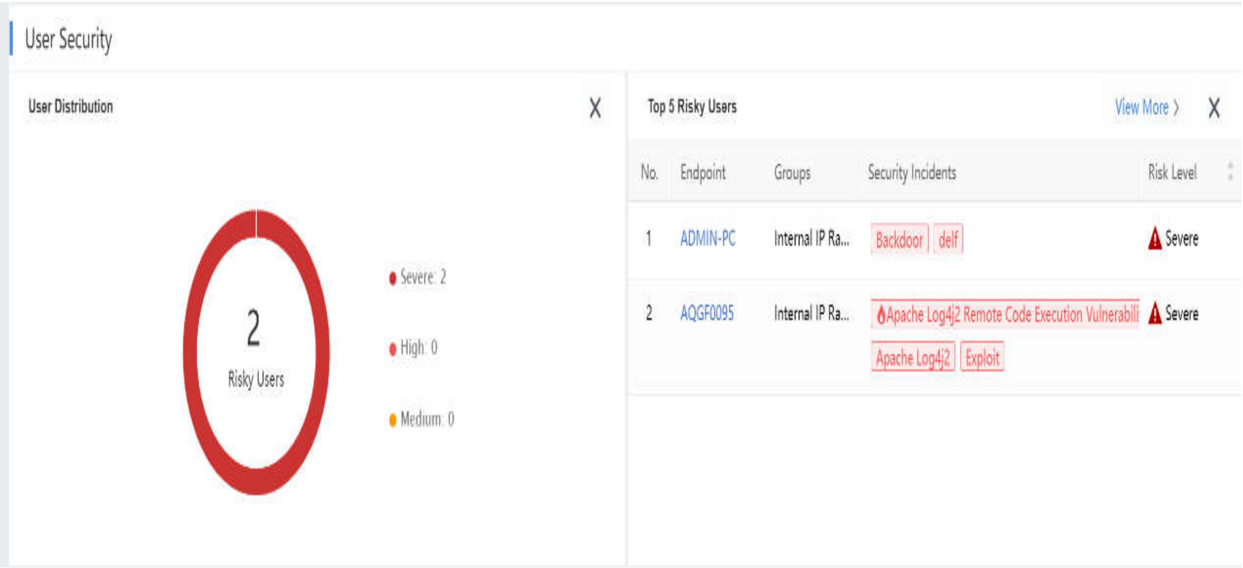
Fig. 6. The CSDRP security incidents by correlation chart

c.Evaluation

Through the above tests, CSDRP has detected relevant virus files, and through the linkage with the firewall, the threat has been dealt with in a timely manner. Through the CSDRP platform, the current risk of intranet risk assets can be displayed through topology visualization, and the analysis of intranet threats can be supported. View intranet threats from four dimensions: horizontal attack, illegal access, risky access, and suspicious behavior. Supports external network threat analysis, and checks the malicious situation of hosts to the Internet.

(1. Threat detection capability

Through full traffic analysis, multi-dimensional effective data collection, and intelligent analysis capabilities, real-time monitoring of the entire network security situation, internal horizontal threat situation, business external connection risks, and server risk vulnerabilities, etc., allows administrators to perceive the security of the entire network at a glance. , Where is it insecure, specific weaknesses, attack entry points, etc., around the attack chain (kill-chain) to form a set of security capabilities based on "pre-event detection, in-event analysis, and post-event detection" to see threats to the entire network, thereby assisting decision-making.



User Security

User Distribution

2 Risky Users

● Severe: 2
● High: 0
● Medium: 0

Top 5 Risky Users — View More 〉

No.	Endpoint	Groups	Security Incidents	Risk Level
1	ADMIN-PC	Internal IP Ra...	Backdoor delf	Severe
2	AQGF0095	Internal IP Ra...	Apache Log4j2 Remote Code Execution Vulnerabili Apache Log4j2 Exploit	Severe

Fig. 7. The CSDRP platform's risky user security part

(2. Traffic Visualization

CSDRP is designed based on Hadoop big data framework, combined with the Elastic Search engine, and can display real-time threat analysis and application traffic, asset management, and other capabilities through visualization.

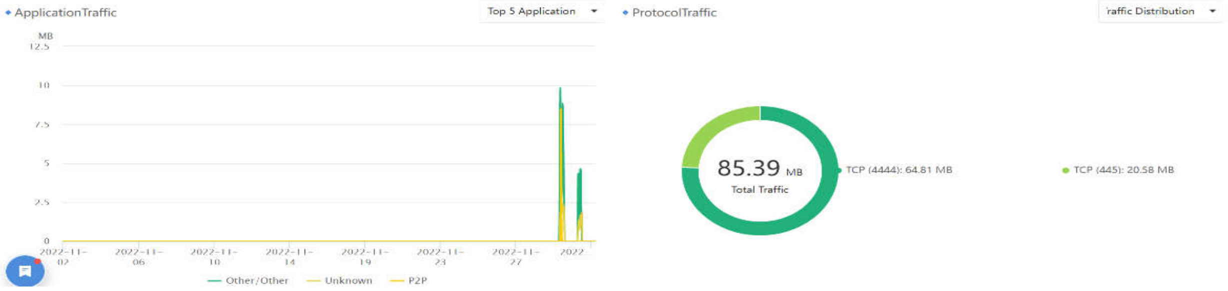


Fig. 8. The traffic monitoring part

(3. Efficient and collaborative response

CSDRP can link the existing security equipment system as a basic component, not only as a collection of security data but also to block and control through linkage when important security incidents or risks spread internally, to avoid the expansion of influence。

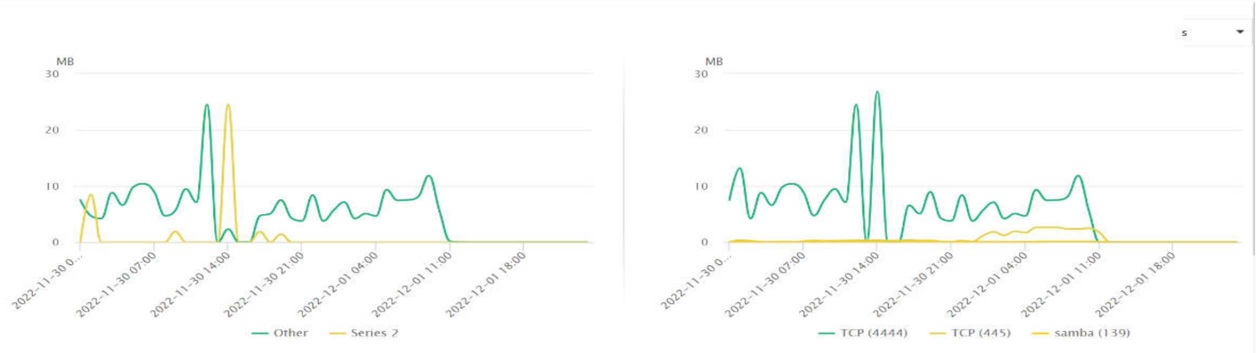


Fig. 9. The CSDRP platform efficient and response part

5. CONCLUSION

In this paper, we propose a security detection and response platform based on network security log analysis to assist large campus network security monitoring and management. The architecture we propose includes three layers: log acquisition layer, data processing layer, and visualization layer. We discuss a parallel log-based threat detection that integrates signature-based and anomaly-based detection. We also discuss common techniques used in threat detection models and visualization schemes to better identify attack behavior. Finally, we introduce the platform setup and implementation workflow to verify the effectiveness of our proposed system. Through the use of this platform, network administrators can use CSDRP to monitor the network status of the campus in real-time, and grasp the network operation status in time, According to the investigation and forecasting situation, timely rectification can be achieved, and the integrated management of effective early warning before the event, timely processing during the event, and interpolation of loopholes after the event can be achieved, to improve the management ability of campus network security and better maintain network security.

REFERENCES

[1] Logota, G. Mantas, J. Rodriguez, and H. Marques, “Analysis of the impact of denial of service attacks on centralized control in smart cities,” in International Wireless Internet Conference. Springer, 2014, pp. 91–96.

[2] J. Johnson, S. J. Lincke, R. Imhof and C. Lim, "A comparison of international information security, "Interdisciplinary Journal of Information, vol. 9, pp. 89-116, 2014.

[3] Goodwin and J. P. Nicholas, "A framework for cybersecurity information sharing and risk reduction, "Microsoft, 2015.

[4] J. Mtsweni, N. A. Shozi, K. Matenche, M. Mutemwa, N. Mkhonto and J. J. v. Vuuren, "Development of a Semantic-Enabled Cybersecurity Threat Intelligence Sharing Model," Boston, 2016.

[5] R. Richardson, "CSI computer crime and security survey," Computer Security Institute, pp. 1-30, 2008.

[6] K. Chatfield, K. Simonyan, A. Vedaldi, and A. Zisserman. Return of the devil in the details: Delving deep into convolutional nets. In British Machine Vision Conference, 2014.

[7] National Institute of Standards and Technology (NIST), “Overview: Nist cloud computing efforts, nist senior executive for cloud computing,”2010.

[8] W.-T. Tsai, X. Sun, and J. Balasooriya, “Service-oriented cloud computing architecture,” in Proceedings of 2010 Seventh International Conference on Information Technology: New Generations (ITNG), 2010.

[9] Y. Bengio, Learning deep architectures for AI, Foundations, and Trends in Machine Learning, vol. 2, iss. 1, pp. 1-127, 2009.

[10] S. K. Datta, C. Bonnet, and N. Nikaein, “An IoT gateway centric architecture to provide novel m2m services,” in 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 514–519, 2014.

[11] Rivera, E. Montes de Oca, W. Mallouli, A. Cavalli, B. Vermeulen, and M. Vucnik, Industrial IoT Security Monitoring and Test on Fed4Fire+ Platforms, 10 2019, pp. 270–278.

[12] J. Dean and S. Ghemawat, “Mapreduce: simplified data processing on large clusters,” Communications of the ACM, vol. 51, no. 1, pp. 107–113, 2008.

[13] Zhang, L. Ge, R. Hardy, W. Yu, H. Zhang, and R. Reschly, “On effective data aggregation techniques in host-based intrusion detection in manet,” in Proceedings of 2013 IEEE Consumer Communications and Networking Conference (CCNC), 2013.

[14] Ten, G. Manimaran, and C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4, pp. 853–865, 2010.

[15] P. D. Curtis and N. Mehravari, “Evaluating and improving cybersecurity capabilities of the energy critical infrastructure,” in 2015 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–6, 2015

[16] M. Cinque, D. Cotroneo, and A. Pecchia, “Challenges and directions in security information and event management (SIEM),” in 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pp. 95–99, 2018.

[17] S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a cybersecurity certification framework for the internet of things," IEEE Security Privacy, vol. 17, no. 3, pp. 66–76, 2019.