Research and Practice on Enterprise Network Security Management System Based on Security Operation Platform

Bin Lu[a*], Mingdong Chen[b], Chao Zhang[c], Hui Chen[d]

GUIZHOU QIANYUAN POWER CO., LTD., Nanming, Guiyang, Guizhou, China

[a*]qyscjsb@gzqydl.cn, [b]943512561@qq.com
[c]3180975250@qq.com, [d]1066497528@qq.com

Abstract. In the wave of digitalization, enterprise network security is facing severe challenges. This research and practice focuses on the application of the security operation platform in enterprise network security management. It analyzes in detail its system architecture, functions, characteristics and application practices, demonstrates its crucial roles in multiple aspects such as emergency command and security operation and maintenance, and explores how to help enterprises build an integrated and high-performance network security management system, thus providing strong support for enterprises to cope with network security threats.

Keywords: Security Operation Platform; Enterprise Network Security; Management System.

1 Introduction

With the rapid development of information technology and the acceleration of enterprise digital transformation, network security has decisively become a core element for stable operation of enterprises. The scope of network security is broad, covering many key aspects such as network attack prevention and data protection. In the process of actively participating in digital transformation, it has become an inevitable requirement for enterprises to deeply understand these concepts and construct effective network security management systems to achieve sustainable development[1][2].

Currently, the methods of cyber attacks are evolving at an astonishing speed, with increasing complexity and diversity, which undoubtedly poses a serious threat to the security of enterprise information assets. In such a severe context, carefully building a comprehensive and sound network security management system has become an urgent key task for enterprises to solve. As an emerging technological means, the security operation platform, with its powerful integration capabilities, organically integrates various cutting-edge security technologies with scientific management processes, providing a one-stop comprehensive solution for enterprise network security management. Its

S. M. Zabri et al. (eds.), *Proceedings of the 2025 4th International Conference on Big Data Economy and Digital Management (BDEDM 2025)*, Advances in Intelligent Systems Research 191,
https://doi.org/10.2991/978-94-6463-710-6_18

importance is increasingly evident in the practice of enterprises in responding to network security challenges, and it is gradually becoming a key supporting force for enterprises to build a network security defense line[3][4].

2 Overview of the Security Operation Platform System

2.1 System Architecture

The security operation platform adopts a layered architecture, which includes an application layer, a business processing layer, a data layer and an interface layer.

The application layer provides the user operation interface and function entrances, enabling management, analysis and collaborative operations. The business processing layer integrates multiple services, such as data analysis correlation engines, process engines and so on, to ensure that data processing is efficient and orderly. The data layer is responsible for data preprocessing and storage, providing data support for the business. The interface layer realizes data docking with external systems and the management and control of security devices, guaranteeing the extensibility and synergy of the platform. As Lu GH mentioned in “Fundamentals of Network Security Technology” about the basic knowledge of network security technology, it provides technical theoretical support for the data preprocessing, storage in the data layer, and data docking in the interface layer of the security operation platform[5].

2.2 Main Functions

1) Emergency Command Management

a) The overall security situation is presented:Starting from a global perspective of the enterprise, through intuitive and comprehensive visualization, the overall situation of enterprise network security is displayed in real time, presenting complex security situations in a concise and easy to understand form to managers, enabling them to quickly perceive the full picture of risk distribution and provide timely and accurate basis for decision-making. As emphasized by Hasan M K et al. in their in-depth study of information physics and network security systems in smart grids, the security operation platform fully references and draws on relevant standards and protocols in the field when designing system architecture and implementing functions, ensuring high standardization and effectiveness in addressing various security challenges[6].

b) Early Warning Notification and Closed-loop Management: When incidents occur, it activates warnings promptly, sending detailed info to relevant staff and manages the incident lifecycle comprehensively through an efficient loop. This enhances emergency response, ensuring quick and orderly command coordination and reducing losses.

c) Emergency command is coordinated and efficient: In emergencies, it assigns tasks precisely and tracks progress in real time. With integrated tools, it enables staff collaboration, breaks information barriers, improves response efficiency, and minimizes incident impacts.

d) Comprehensive management of security work: The platform covers key aspects such as planning, responsibility allocation, and level protection management, integrating them to make security work an organic whole and achieve standardized, systematic, and scientific management.

e) Task collaboration and assessment evaluation: It offers a flexible task collaboration mechanism, allocates tasks as needed, tracks execution, and has an assessment system to evaluate and improve work, promoting efficient safety work implementation and goal achievement[7].

2) Security Operation and Maintenance

a) The operation and maintenance of equipment is standardized and orderly:To ensure the standardized management of the operation and maintenance of security equipment, security operation and maintenance personnel are required to log in and operate the equipment through the bastion host. The bastion host management provides management for bastion host equipment and enables unified control over the operation and maintenance of security equipment through the bastion host.

b) Intelligent and precise vulnerability management:Automatically scan for vulnerabilities and associate them with assets to achieve effective management of vulnerabilities.

c) Visualized management of services:The online and offline service situations are clear at a glance, facilitating users' supervision and evaluation.

d) Work order management is flexible and convenient:Customize the work order process, track the progress of disposal, and improve work collaboration.

e) Knowledge base management and knowledge sharing:Provide abundant security knowledge, support knowledge update and query, and promote the dissemination of knowledge.

3) Monitoring and Analysis

a) Panoramic view of asset security:Integrate multi-source data to provide a comprehensive perspective for asset security management.

b) Unified handling of security alerts:Concentrate on displaying and processing alarm information to achieve the full life cycle management of threats.

c) Tracking and analysis of security incidents:Track the handling of incidents in real time, provide multi-dimensional analysis, and ensure that the information is comprehensive and accurate.

d) Real-time monitoring and early warning of equipment:Monitor the operating status of equipment in real time, and detect and handle abnormal situations in a timely manner.

4) Asset Management

a) Ledger management is meticulous and detailed:It supports the input and maintenance of multi-type asset information and can be flexibly interfaced with third-party data.

b) Asset discovery is comprehensive and efficient:Combine active and passive detection to comprehensively grasp the dynamics of assets.

c) Statistical reports are clear and intuitive:Conduct multi-dimensional statistics on asset information and display it in the form of charts, which is convenient for decision-making analysis.

5) Threat intelligence management

a) Real-time update with cloud synchronization:Obtain cloud intelligence in real time to ensure the timeliness of the intelligence[8].

b) Local management is flexible and autonomous:It supports the input of local intelligence and the setting of sharing, meeting personalized needs.

c) Intelligence query is precise and in-depth:Provide multiple types of intelligence queries and correlation analysis to provide a basis for security decisions.

6) Integrated large-screen display

a) Gain overall control of the whole situation and general trend:Display the overall security situation of the enterprise and assist senior management in decision-making (see Fig. 1).

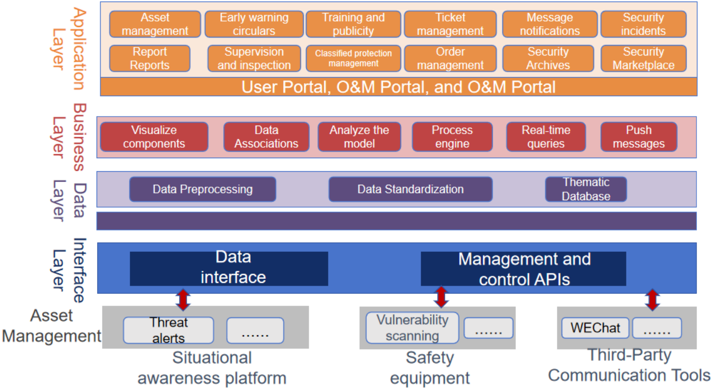

Fig. 1. Overall Situation

b) Manage and direct work in an orderly and effective manner:Present the progress of security work, facilitating command and dispatching.

c) The special work highlights key points:Provide detailed analysis for special work and evaluate the effectiveness of the work.

d) Present a panoramic view of the asset library:Comprehensively display asset information to facilitate the optimal allocation of assets.

f) Analysis and traceability of threat intrusions:Conduct in-depth analysis of threat intrusions and provide references for the adjustment of protection strategies.

2.3 Platform Features and key Technologies

1) Integrated operation support

Build a unified platform centered around the enterprise's business, achieve all-round management of business security, integrate security into the business process, reduce operational risks, and promote the effective implementation of security services.

2) Emergency command, coordination and linkage

The platform has developed an emergency command system focused on corporate assets, enabling real-time information synchronization and efficient collaboration. It ensures rapid information dissemination during network security incidents, allowing managers to make informed decisions. The system also supports interdepartmental collaboration, breaking down barriers and optimizing resource allocation. Departments like security, operations, and business work together to enhance the enterprise's emergency response and collaborative capabilities.

3) Data management, sharing and optimization

Integrate multi-source data to form comprehensive files. Achieve secure sharing through permission settings. Provide data support for security management and decision-making, and improve the efficiency of data utilization.

4) Flexible expansion and adaptation of the platform

The platform architecture is designed flexibly. It supports multiple deployment methods and functional expansions, can be integrated with external systems, and adapts to the needs of enterprises at different development stages and in different network environments.

3 Application Scenarios of the Security Operation Platform

3.1 Service scenarios of the Network Security Operations Center

The security operation platform offers a closed-loop management process based on vulnerabilities, incidents and threat intelligence, as well as functions like information-based tools for daily operation and maintenance work and work assessment reports. The preset operation and maintenance work groups and process engines can be flexibly configured according to actual needs.

3.2 Overall Security Operation and Maintenance Guarantee Scenario

When an enterprise outsources its security operation and maintenance, the platform helps professional teams to control the overall situation, make decisions, conduct command and supervision management. Meanwhile, it standardizes the work process of operation and maintenance to ensure the stable and secure operation of the enterprise's network.

3.3 The Scenario of Work Collaboration Between Superiors and Subordinates in Security Management

The security management department of an enterprise utilizes the platform to achieve efficient collaboration with subordinate units, complete tasks such as risk handling and information reporting, and enhance the collaboration and efficiency of the enterprise's overall security management.

4 Typical Deployments of the Security Operation Platform

4.1 Cascading Deployment

Build a tree-like structure of the main center and branch centers. The headquarters has control over all data, while the secondary centers manage the data of their own level and lower levels. This is applicable to large enterprises or complex network architectures, realizing hierarchical management and collaboration (see Fig. 2).

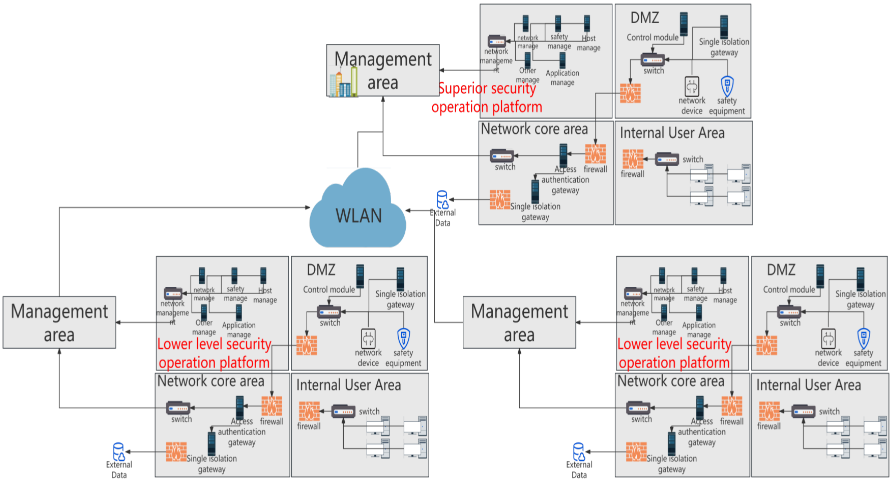

Fig. 2. Schematic diagram of hierarchical deployment across the whole network

4.2 Single-level Deployment

Single-level deployment is the simplest system deployment mode and also the most typical one, which is applicable to most network environments. In the single-level deployment scenario, users only need to deploy the security management system and connect the network directly between the security control module and the system.

4.3 Resources Required for Deployment

In terms of computing and storage resources, virtual machines of different specifications need to be configured for microservices, data storage, and so on. For network resources, a certain bandwidth, port mapping, and domain name configuration must be ensured to guarantee the normal operation of the platform.

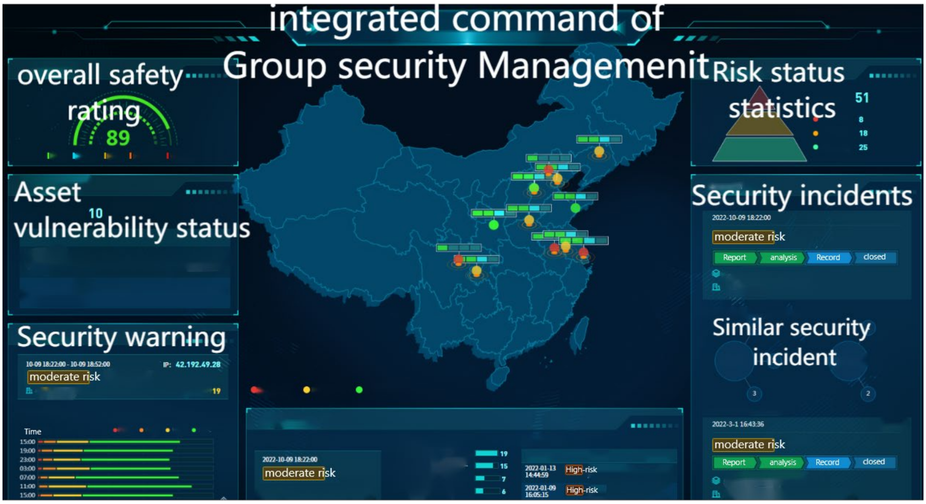

Fig. 3. Successful example

5 Analysis of Successful Cases of the Security Operation Platform

After implementing a security operation platform, a large enterprise reduced its emergency response time from an average of 4 hours to 1.5 hours, improved equipment maintenance efficiency by 35%, and increased the timely vulnerability repair rate from 60% to 90%. Compared with the industry average, the emergency response time is 2.5 hours lower than the industry average, the equipment maintenance efficiency is 20% higher than the industry average, and the timely vulnerability repair rate exceeds the industry average by 20 percentage points, fully demonstrating the platform's outstanding performance in improving the efficiency of enterprise network security management.(see Fig. 3).

6 Conclusion

This research and practice have deeply explored the enterprise network security management system based on the security operation platform. Through typical deployment models, it offers feasible plans for different-sized enterprises. Its application helps build a comprehensive security framework, effectively evaluate and improve security management performance via functions like data management and emergency command. Successful cases confirm its advantages in enhancing security levels, providing references for enterprises against cyber threats. However, it has limitations. In large-scale data processing, when daily data exceeds 1TB, processing latency may rise by 20%. Integrating with legacy systems based on private protocols may cause compatibility issues. For SMEs, the costs of high-performance equipment, advanced module licenses, and personnel training are high, restricting its application.

References

1. Shuang Qiu (2024) Construction and Practice of Enterprise Information Security Management System of Intrusion Detection Technology.The 4th International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy
2. Kirilchuk S, Reutov V, Nalivaychenko E, et al. Ensuring the security of an automated information system in a regional innovation cluster[J]. Transportation Research Procedia, 2022, 63(1): 607-617.
3. Charles Pfleeger (2023) Introduction to Cybersecurity.Addison-Wesley Professional Publishing,in the USA.
4. McLeod A, Dolezel D. Information security policy non-compliance: Can capitulation theory explain user behaviors?[J]. Computers &Security, 2022, 112(1): 102526.
5. Lu GH (2017) Fundamentals of Network Security Technology. Tsinghua University Press Publishing,in Beijing.
6. Hasan M K, Habib A K M A, Shukur Z, et al. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations [J]. Journal of Network and Computer Applications, 2023, 209(1): 103540-103541.
7. Herath T C, Herath H S B, Cullum D. An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks[J]. Information Systems Frontiers, 2023, 25(2): 681-721
8. Rostami E, Karlsson F, Gao S. Policy components–a conceptual model for modularizing and tailoring of information security policies[J]. Information & Computer Security, 2023, 31(3): 331-352.