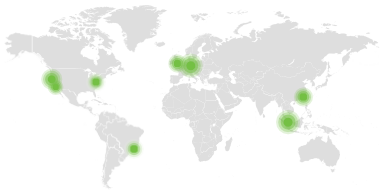
WHITEPAPER



2021

NSFOCUS Intelligence Security Operation Platform Whitepaper

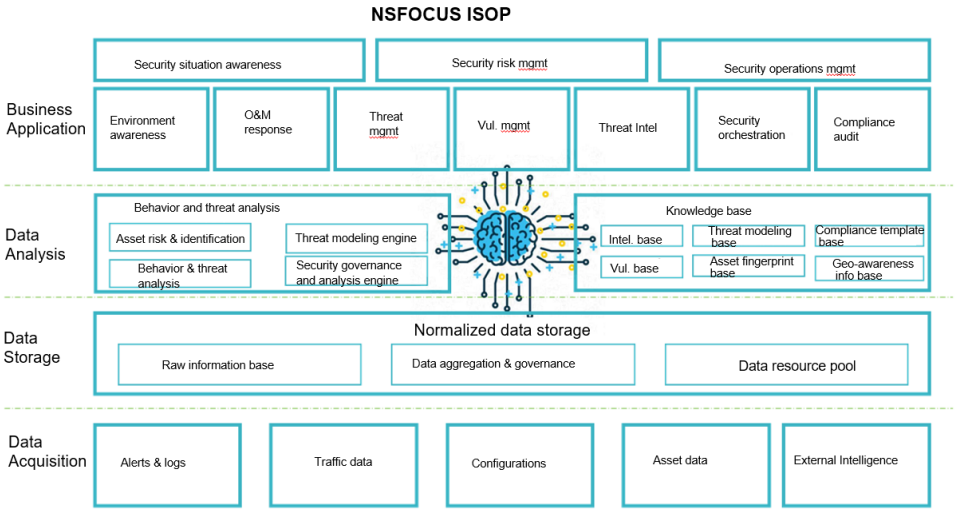
Content

1. About the Product

Built upon a big data architecture, NSFOCUS Intelligent Security Operation Platform (ISOP) is a trustworthy scenario-based security management platform for governments and enterprises. Following the concept of NSFOCUS's intelligent security 3.0, ISOP focuses on practical security operations for assets. By handling networkwide traffic data and heterogeneous log data in a centralized way, ISOP, by reference to threat intelligence, is capable of real-time analysis, intelligent decision-making, and asset and vulnerability lifecycle management, delivering a closed-loop security management process covering threat incident investigation, traceback, forensics, and response. Also, ISOP aids in security orchestration and abnormal behavior analysis. In this way, ISOP helps customers build a security center to provide strong support for security operations (management, analysis, and response) and implement security situation awareness and collaborative command across regions, in a bid to foster the building of a sound security protection ecosystem for enterprises.

2. Architecture

2.1 Overview



» Data acquisition

Through collaboration with traffic probes, log collectors, assessment probes, terminal probes, honeypot systems, and NSFOCUS Threat Intelligence (NTI), this system can acquire a wide variety of security data in a centralized manner, including security alerts, security logs, traffic data, environment configuration baselines, asset data, and intelligence (IP reputation, sample rules, MD5 values, and vulnerability intelligence), providing data support for security analysis personnel.

» Data storage and analysis

Depending on data source management, data handling, data analysis, and data services, NSFOCUS ISOP builds a comprehensive operations data set to enable data normalization and provide data invocations, data queries, data calculations, data modeling analysis, and security service applications in a unified way. With a threat modeling analysis engine and security governance and analysis engine, ISOP makes a correlative analysis of behaviors, threats, and their scenarios, including real-time alerts, attack sources, network threats, user behaviors, and special security business scenarios.

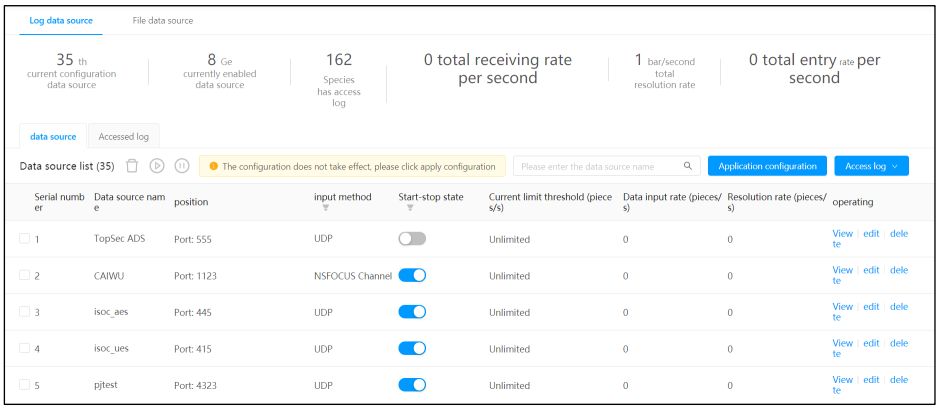
» Service application

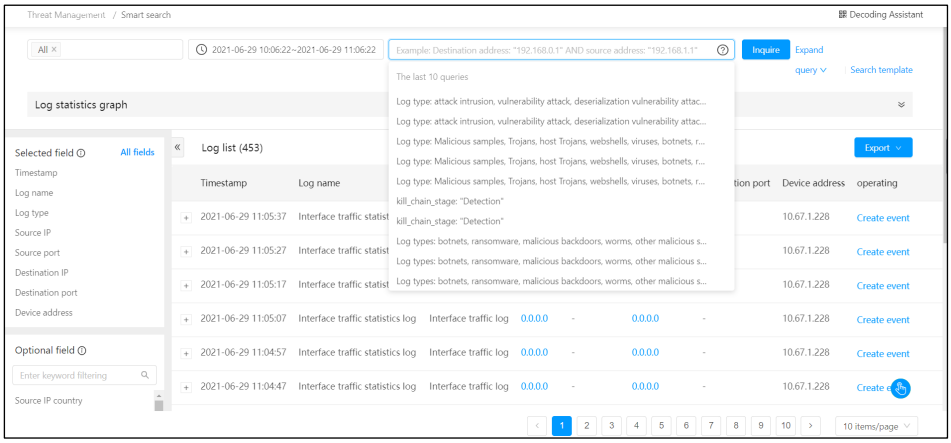
NSFOCUS ISOP provides multiple security management functions, including security situation awareness, security risk management, security operations managements, security orchestration, and threat management, to adapt to security management needs of governments, enterprises, and sectors like finance, carriers, transportation, education, and healthcare. With these strategic security capabilities, the system helps customers rapidly discover, analyze, and solve security issues to spur the output of strategic security capabilities, with the aim to be a scenario-based trustworthy and practical security operations management platform that provides security management and collaborative command to inform enterprises' decision-making.

2.2 Key Application Values

2.2.1 Flexible Access for Classified Protection Compliance

NSFOCUS ISOP receives logs concerning identity authentication, terminal security, security protection, security identification, and security audit in the live network through syslog, NSFOCUS's A interface, FTP/SFTP, and NetFlow. This system adopts the unified data structures and data exchange format to increase the data handling and transmission efficiency, as well as exercises unified data management for better data governance. To serve different data requirements, ISOP provides flexible data element expansion principles and methods to make data structures and data governance more scalable and retain the logs for 180 days to obey requirements of PB-level classified protection.





2.2.2 All-round Asset Monitoring and Management Across the Network in Different Areas

NSFOUS ISOP surveys assets in several ways (passive discovery of logs and traffic by scanning devices and active discovery by NTI and RSAS) to gain an insight into the exposure surface and discover assets that are difficult to locate, helping enterprises set up an asset security ledger to eliminate information silos for asset management, through a combination of asset baselines and asset audits. Using asset awareness and asset profiling for hierarchical asset monitoring and control, this system ensures the integrity and security of IT assets.

2.2.3 Dynamic Defense-in-Depth

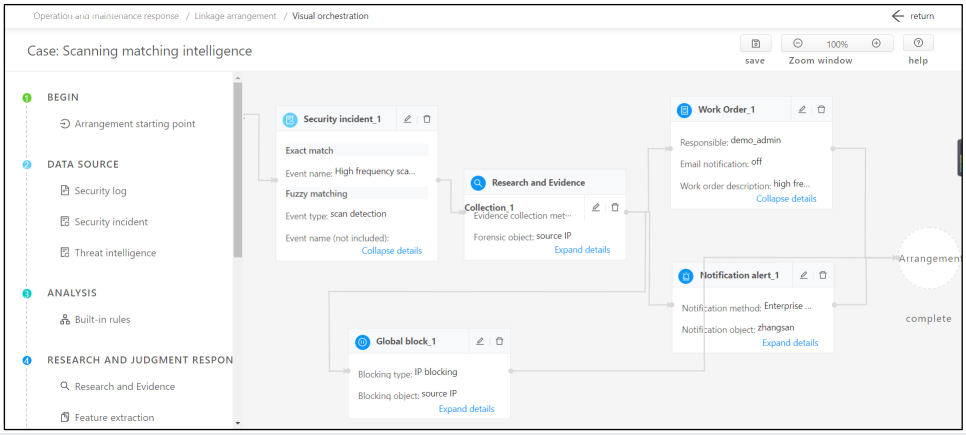
NSFOCUS ISOP leverages the big data technique to aggregate data in aspects of security detection, identification, audit, protection policies, identities, and authentication. Aided by endpoint detection and response (EDR) and threat hunting by honeypots, this system, by reference to threat intelligence, uses its built-in threat analysis modeling engine, abnormal behavior analysis engine, and security governance and analysis engine to make an in-depth correlation analysis to identify known, unknown, and suspicious behaviors, including accurate detection of compromised hosts, network viruses, illegitimate outreach, APT incidents, ransomware, and other threat events. Besides, using ATT&CK attack tactics, ISOP draws a graph to present the attack path, making security detection more accurate and intelligence.

2.2.4 Ongoing Security Risk Assessment for Security Compliance

NSFOCUS ISOP provides integrated vulnerability management covering system/website vulnerability check, configuration baseline check, weak password check, penetration testing, and check for classified protection configurations, helping security operations personnel automate classified protection compliance and ongoing risk assessment. Aided by NSFOCUS's proprietary "prioritization" model algorithm and the framework for closed-loop management of vulnerability-based threats, ISOP exercises vulnerability management and makes a quantitative analysis, letting security managers know classified protection compliance check results in such dimensions of enterprises' physical environment, communication networks, regulations, personnel, and network security system development.

2.2.5 Precise Command, Collaborative Protection

Using a trustworthy threat analysis algorithm and model based on plenty of protection practices, ISOP makes a correlation analysis of high-frequency attack scenarios and statistical elements on the platform to make inferences and predication about the attack path, thus improving the accuracy of attack results. Also, the system adopts the SOAR technique to investigate threats for forensics and collaborative responses in multiple security analysis scenarios, rapidly focusing on blocking threats on the network side and terminal side. Also, ISOP synchronizes block instructions to third-party devices for threat blocking and containment, helping users build a closed-loop mechanism for responding to threats within minutes. Based internal and external intelligence, ISOP reports security information in time via several alerting ways (DingTalk, WeCom, SMS, and email), implementing collaborative protection and command at the enterprise side.

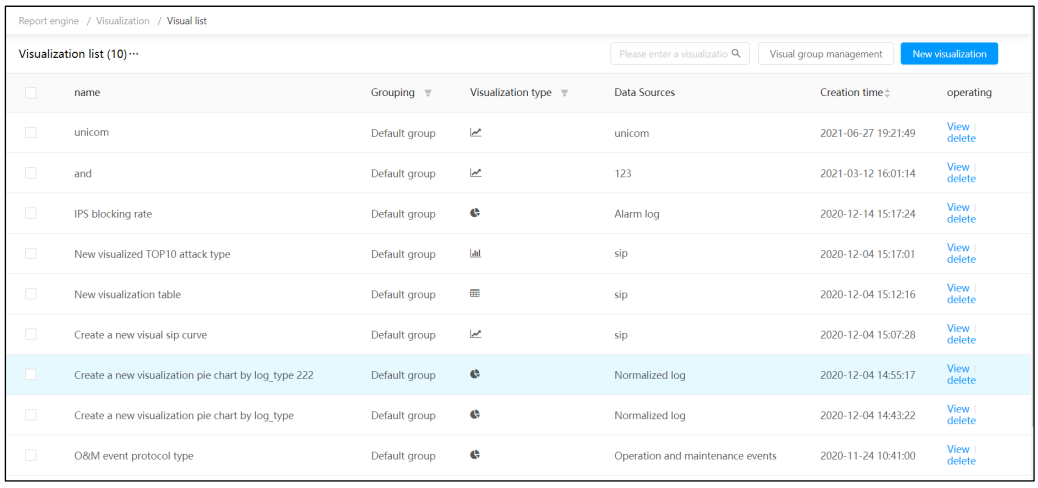


2.2.6 Threat Situation Awareness for Cloud Tenants via Collaboration with Third-Party Cloud Management Platforms

NSFOCUS ISOP can accommodate to tenant scenarios through collaboration with cloud management platforms and control platforms. Adopting a big data framework, ISOP can adaptively access, analyze, present, and search massive multilayer heterogeneous big data in multi-tenant scenarios, allowing users to view their own traffic data upon login with a tenant account. With the visualization technique, the system presents the security situation of public scenarios on a large screen to help customers build and improve the overall security status monitoring system. Built upon a proprietary adaptive architecture, ISOP provides reliable data support for security operations, assisting users with rapid issue discovery and analysis. Besides, this system implements closed-loop security management through O&M means, ensuring business continuity of systems of public cloud tenants.

2.2.7 Visualization of Multilayer Threat Status Data

NSFOCUS ISOP uses a visualization technique to present the network security situation from different security operation and analysis angles, like overall risk status, threat statistics, vulnerability statistics, security response, and log audit, helping executives stay up-to-date with the latest security trend and risks. By showing security governance indicators, this system gives executives an insight into the overall security situation of enterprises. By monitoring threats, vulnerabilities, and asset O&M, ISOP helps medium-level managers implement security management.



2.3 Key Technical Advantages

2.3.1 Open and Scalable Big Data Platform Architecture

Using a flexible and advanced design, NSFOCUS ISOP allows for rapid scalability to adapt to scenarios of various scales. This platform features a flow-based analysis engine based on the big data architecture, which addresses storage and management of data entries. Through big data cluster O&M management, ISOP updates users about the security status of cluster nodes and big data computing facilities and allows users to manage them. Besides, the platform allows users to monitor for service scalability requirements via SDKs or open APIs

and adapt platform functions to security service changes, making for more efficient platform development and increasing integrated security capabilities.

2.3.2 Asset Lifecycle Management

Collaborating with NSFOCUS Remote Security Assessment System (RSAS), NSFOCUS Threat Intelligence (NTI), NSFOCUS Unified Threat Sensor (UTS), and NSFOCUS Unified Endpoint Security (UES), NSFOCUS ISOP, aided by external data, enables ongoing monitoring and security management for internal and external assets. By detecting asset changes and abnormal asset baselines, the system further analyzes security risks incurred by asset changes and abnormal assets, generating alerts for asset change risks and making corrections to help customers maintain the security ledger for millions of assets and exercise fin-grained asset information management.

2.3.3 Risk Assessment and Prediction by the Intelligent Decision-Making Inference Engine

By reference to information about assets, threats, and vulnerabilities, and threat intelligence, NSFOCUS ISOP identifies threats and makes an in-depth correlation analysis from such perspectives as the asset importance, open ports/services/middleware, asset vulnerabilities, asset threat severity, and attack result and impact. Assume that the XXX exploit is discovered on the core asset A. ISOP determines that this exploit attack succeeds after a preliminary analysis of its traffic context, status code, device actions, and subsequent attack behaviors. If the vulnerable software is installed on the asset and the scan results indicate that this vulnerability exists on the asset, the ISOP concludes that this asset is compromised and has a high security risk.

2.3.4 Threat Determination Framework for End-to-End Threat Management

NSFOCUS ISOP makes a systemic analysis of all threat detection rules of probes and platforms from angles like the rule credibility, rule topicality, risk level, and ATT&CK tactic identities. Building up trustworthy security operations capabilities that focus on frequent and high-risk threats, NSFOCUS ISOP implements integrations security operations that involve routine operations and offensive/defensive exercises. Also, the system uses the threat analysis engine to provide in-depth correlative analysis scenarios, special attack detection process, and attack forensics scenario, assisting security analysis and management personnel to investigate and track attacks and make accurate judgments.

2.3.5 Threat Hunting and Trackback based on Clues

NSFOCUS ISOP associates signs (IP addresses, domain names, and MD5 values) of suspicious behaviors with the threat context, filters out false positives, adds missing information, and presents the attack process in chronological order. Also, by monitoring specific hints, NSFOCUS ISOP generates alerts for new threats and keeps tracking threats, implementing retrieval-like hunting and ongoing monitoring of unknown threats. Instrumentalizing the threat hunting assumptions, forensics, and revelations, as well as handling process improvements, the system streamlines the threat hunting process and delivers relatively mature threat hunting capabilities, increasing the efficiency of proactive hunting of unknown threats and providing more automated detection capabilities in threat hunting scenarios. In the case of sample exposure, the system allows users to define custom rules for topical events and query them for trackback. Alternatively, it can track samples for forensics based on PCAP packets acquired by probes in real time.

2.3.6 Vulnerability Risk Prioritization

Based on threat intelligence, NSFOCUS ISOP gives a priority score to vulnerabilities and locates key risk points by making a correlation analysis of threat elements such as vulnerability topicality, vulnerability PoC, local asset security ledger, network environment, and protective measures. It advises users to fix vulnerabilities and make corrections by vulnerability priority, minimizing security risks as soon as possible. For vulnerability risk prioritization, the key point lies in the vulnerability database accumulation and management. The ISOP platform has a built-in vulnerability database with more than 200,000 entries covering the IoT, industrial Internet, cloud computing, big data, and mobile security sectors.

2.3.7 Security Orchestration, Automation, and Response (SOAR)

NSFOCUS ISOP employs the visual orchestration technique for deep integration of personnel, security techniques, and processes. Also, it uses playbooks to build a security event handling workflow, automatically triggering responses delivered by security devices. Based on a

full understanding of security event context, threat intelligence, and fine-grained logs, NSFOCUS ISOP turns a complicated event response process and task into a consistent, repeatable, measurable, and effective workflow, thus implementing automated ongoing responses instead of passive emergency responses. NSFOCUS ISOP builds the security incident determination and alerting mechanism and process and translates them into attack identification rules and associations between security O&M events and automated responses and handlings. In this case, if an attack event matches a case enabled in the SOAR system, a closed-loop handling will be automatically implemented via playbooks, without manual interventions. Specifically, ISOP can automatically handle security events within minutes through direct responses, tickets, WeCom, DingTalk, and email notifications, lowering the labor cost of enterprises.

2.3.8 User and Entity Behavior Analytics (UEBA)

The ISOP platform extracts behavior data of users and entities (such as IP addresses, applications, devices, and networks) from massive data, analyzes, assesses, and correlates the behavior data, and sets up baselines to identify insider threats and outsider threats. Through abnormal behavior analysis of hundreds of scenarios concerning internal access, data disclosure, risky accounts, and risky devices, ISOP identifies potential abnormal associations between subjects and objects to nip security hazards in the bud.

2.3.9 A Rich Set of Threat Intelligence

NSFOCUS Threat Intelligence center (NTI), as a threat intelligence analysis and sharing platform launched by NSFOCUS after years' accumulation of security experience and intelligence data, can provide timely and accurate threat intelligence. With support from NTI, users can gain an immediate insight into security threats facing assets exposed on the Internet and generate accurate alerts. Being updated about the latest threat situation, users can implement active threat defense and fast response strategies. Based on NTI's in-depth analysis of security data, users can gain a big picture of the threat landscape and effectively track threats and attacks. Also, users can directly access NTI to upload, query, and confirm sample analysis results stay informed about the threats and risks.

2.4 Customer Value

In response to challenges like diverse security devices, massive logs, various emerging network threats, and the lack of analysis means, the security protection system gives priority to network security monitoring and response capabilities. With the improvement of China's security policies and laws, especially the official issuance of national standards of classified protection 2.0, security management platforms and security operations will become essential to security systems, with an aim to improve the monitoring and emergency response capabilities. NSFOCUS ISOP creates four values for customers:

2.4.1 Security Compliance and Role of Enterprise-Specific Security Center

ISOP is designed under the guidance of the ISO 27000 family of standards and regulations of national classified protection. It serves as a security center with multiple security management and protection capabilities such as security situation awareness, security risk management, and security operations management. With the end-to-end security capabilities, ISOP functions as a security operations center to help enterprises enable and improve techniques and process, allowing them to devote more resources and efforts to achieve better security management

2.4.2 Better Security Protection and Lower Labor Cost

Through incorporation of the kill chain model, ATT&CK model, and threat knowledge graph into platform threat modeling and correlative analysis, ISOP can discover threats and perform forensics and trackback to identify threats more accurately. By applying enterprises' security experience into SOAR, ISOP reduces the response time and helps security specialists improve technical competencies, bringing the effect of cost reduction and efficiency enhancement to the business.

2.4.3 Support for Security Management Evaluation and Assessment of Different Job Roles

ISOP helps an enterprise's CISO, security managers, and security O&M personnel with security management and security O&M. Visualizing the network-wide security situation, this system keeps executives updated about the latest security trend and risks, informing their decision-making on security development and investments. This system helps medium-level management implement security management and technique systems by means of threat alerting and attribution, vulnerability monitoring and closed-loop handling, and

monitoring of dynamic asset changes. Also, ISOP enables O&M personnel to discover attacks accurately and helps them with emergency response by means of prompt alerting, log audits, and incident attribution, thus reducing their workload and improving their efficiency.

2.4.4 Delivery of Shared Security Capabilities with Collaboration of Security Operations Services

Incorporating security operations services, the on-premises ISOP connects to NSFOCUS's cloud-side security operations platform so that NSFOCUS's security experts on the cloud side provide 24/7 security operations for customers and work with onsite operation personnel to optimize the threat alerting mechanism, streamline the asset security lifecycle, and make O&M and response plans. In this way, they can help customers rapidly discover, analyze, and solve security issues, as well as tailor-make a security operations and assurance mechanism, build security capabilities, and develop a security knowledge base to spur the output of strategic security capabilities, finally delivering a scenario-based trustworthy and practical security operations management platform for enterprises.

3. Conclusion

With the full implementation of the Internet Plus initiative, information technologies are increasingly widely used during the course of national socio-economic development. However, accompanied by IT development are emerging network security threats that are even more serious, posing a great challenge to the traditional security protection system with a focus on protection. The future network security protection system, placing more importance on network security monitoring and response capabilities, will take full advantage of all-around traffic monitoring, big data analysis, and predication technologies to greatly increase security event monitoring and alerting capabilities and make rapid responses to handle a lot of unknown security threats.

To better implement NSFOCUS's concept of intelligent security 3.0, NSFOCUS ISOP is designed to provide IPDR-centered defense-in-depth (DiD) capabilities and horizontal scenario-based security operations capabilities, with a focus on practical security operations. As an integrated adaptive security control platform powered by services, scenarios, and data, NSFOCUS ISOP merges all sorts of scattered security information and distills them, greatly increasing the O&M efficiency and enabling O&M personnel to make a more extensive and in-depth security analysis. Arguably, this system uses a platform-based security operations design to replace the people-led security operations method. With less interventions of O&M personnel, this new approach delivers security governance, classified protection, and security operations to maximize the protection effect through overall protection, intelligent analysis, and automated response, providing better support for enterprises' normal security operations governance ecosystem.