DATASHEET

NSFOCUS

NSFOCUS ISOP

Intelligent Security Operations Platform

OVERVIEW

Powered by Extended Detection and Response (XDR) technology, NSFOCUS ISOP is a consolidated security operations platform designed for modern security operations centers (SOC) to streamline security analyst experience, improve threat response efficiency and raise security operations productivity. NSFOCUS ISOP has comprehensive SOC capabilities and modular components that help:

- **Organizations that lack SOC capability** to build and go live their autonomous SOC quickly;
- **Organizations that have already had SIEM or SOC** to reduce Mean Time to Detect (MTTD) and Mean Time to Response (MTTR), improve security operations productivity by introducing NSFOCUS ISOP's modular components as required. NSFOCUS ISOP also enables large organizations to share their SOC resources with their branches.
- **Managed Security Service Providers (MSSPs) and Internet Service Providers (ISPs)** to boost their value-added security services and multi-tenant capabilities.

EXTENDED DETECTION AND RESPONSE (XDR)

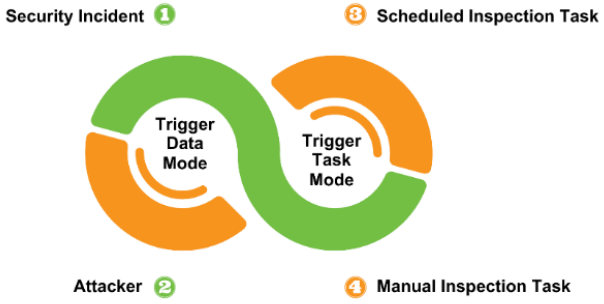
XDR aggregates and analyzes the telemetry data collected on the network and terminals, enabling a comprehensive understanding and visibility of security risks and attacks across an organization. With massive data, XDR enhances sustainable operations for advanced threat detection and response through multi-dimensional extended attributes. Telemetry and change perception help to deliver effective and closed-loop defense and operations.

Highlights enabled by XDR technology:

- Consolidated contextual information and telemetry data lead to quick detection of advanced threats and missed attacks;
- Visual root cause analysis effectively reduces MTTD and MTTR and improves threat detection and sustainable operational efficiency.

SECURITY ORCHESTRATION AND RESPONSE (SOAR)

NSFOCUS ISOP integrates people, technology, and processes in visual orchestration. It builds cases in series or parallels through a playbook, which automatically triggers different security devices to perform different response actions. Cases can be built based on security events, attackers, scheduled inspection tasks, and manual inspection tasks. The four types of cases transform complex response processes and tasks into a standardized and repeatable workflow, and passive emergency response into automated continuous response.



KEY BENEFITS

XDR
Provides correlation analysis of massive telemetry data for entity risk detection and investigation. Relies on SOAR technology to deliver automated, one-stop and closed-loop threat handling.

SOAR
Integrates people, technology and processes and delivers automated orchestration with constructed playbooks and cases. Continuously improve security efficiency and closed-loop operation ability.

Modular Architecture
Eight modular components available for on-demand requirements help SOC team and 3rd-party SIEM to expand security capabilities and improve operations proactivity.

AISecOps - 99% alert noise reduction
AI-powered triage engine; minimize missed detection and reduce false positives.

5G Security
Threat analysis of control plane and user plane such as malicious access detection, asset identification, signaling attack detection, event retrospection and forensics.

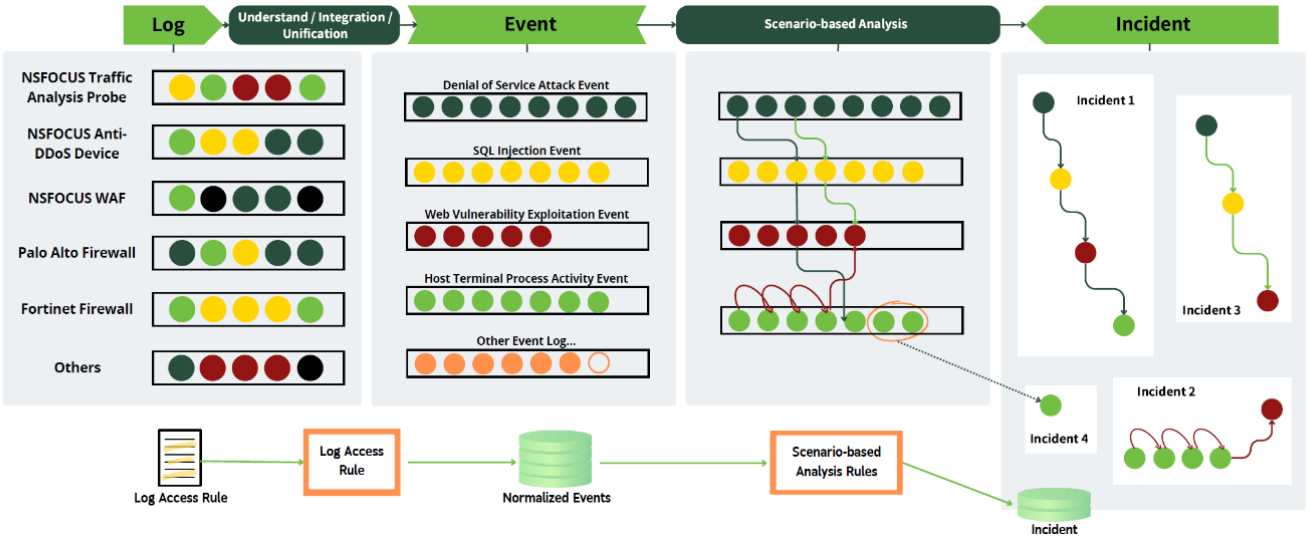
Full Traffic Analysis and Event Retrospection
Full traffic detection;
Over 150 encryption protocol parsing capabilities;
30 days event retrospection;
180 days or longer data storage.

Multi-Source Correlation Analysis
Collects and analyzes data from diverse sources, including network logs, endpoint data, and application information.

SIEM
Aggregates and correlates data from diverse sources for threat detection;
Realtime incident detection;
Actionable insights to enhance security posture and ensure compliance.

Collaboration with 3rd-party Devices
Including Palo Alto, Fortinet, Imperva, CheckPoint, TrendMicro, H3C, etc.

THREAT ANALYTICS AND INVESTIGATION



NSFOCUS ISOP can integrate all threat detection rules from sensors and platforms. It systematically sorts out rule credibility, rule popularity, risk level, and ATT&CK tactical labeling capability. It also combines daily operations and offensive and defensive drills to carry out continuous operation and optimization. The threat analysis engine provides deep correlation analysis, unique attack detection processes, and proof of attack to assist security management and security researchers in threat investigation and tracing attack sources.

5G SECURITY

NSFOCUS ISOP strengthens the capability of threat discovery in the user plane and security operations in the control plane in 5G core networks. It has built-in attack identification rules and behavioral analysis rules for 5G scenarios and provides a 5G security dashboard for real-time threat monitoring of 5G security events. NSFOCUS ISOP addresses threats resulting in the changes in 5G telecommunication businesses and infrastructure, including:

- Terminal-side security: malware, DDoS attacks, information defacement, man-in-the-middle attacks, etc.
- Access-side security: fake base station, air interface or transmission attacks, flooding attacks, session hijacking, etc.
- MEC security: impact after being compromised, edge node overload, abuse of border APIs, fake MEC gateway, etc.
- Core network and slice security: flood attacks targeting components of core networks, fraud of sharing slide resources, malicious register, border attacks and filtration, fraud related to roaming interconnection, etc.
- External threats: Signaling storms, DDoS attacks, attacks targeting APIs, etc.

THREAT HUNTING AND RETROSPECTIVE ANALYSIS

NSFOCUS ISOP streamlines the threat hunting process and exhibits robust threat hunting capabilities, with advanced detection techniques, retrospective analysis capabilities, and visualized hunting features.

- Supports full traffic analysis
- Recognizes more than 150 types of encryption traffic and over 300 fingerprints.
- Supports 180 days of data storage and allows users to define even longer storage periods.
- Allows batch retrospective analysis of endpoint network telemetry data for up to 30 days. With this data, NSFOCUS ISOP can discover unknown threats and 0-day vulnerabilities, enhancing proactive threat detection.
- Offers visualized threat hunting based on identified clues or indicators, and provides recommendations for suspicious clues, assisting security analysts in focusing on potential threats.
- Enables threat hunting experiences to be converted into custom rules, improving the overall detection capabilities.

VULNERABILITY PRIORITIZATION

NSFOCUS vulnerability scoring system uses threat intelligence and correlation analysis technologies to calculate and prioritize vulnerabilities based on vulnerability popularity, exploitation status, local asset security ledger, network environment, and protective measures. Vulnerability prioritization allows for the quick identification of key risk points and the timely repair of critical vulnerabilities in a closed-loop process. NSFOCUS ISOP has built in more than 300,000 high-quality vulnerabilities, covering various fields including the Internet of Things (IoT), industrial internet, cloud computing, big data, and mobile security. NSFOCUS ISOP also supports multi-source heterogeneous vulnerability import to help users expand the amount of vulnerability database data.

AUTOMATIC ASSET DISCOVERY AND MANAGEMENT

NSFOCUS ISOP supports full asset import, automatic and manual asset discovery and collection through scanning, agents, and traffic analysis. This makes all assets across an organization visible. In addition, NSFOCUS ISOP delivers the technology for identifying repeated IP addresses and domains, which can simplify asset management in organizations with multiple branches or tenants.

MDR SERVICE

NSFOCUS's MDR Service empowers ISOP users to better protect their clients and their own infrastructure with 24/7 monitoring and analysis of security events and incidents, ensuring potential threats are detected and responded to promptly. In addition, MDR Service provides access to a team of skilled security professionals who have experience in handling a wide range of security challenges and are capable of helping security analysts to fill skill gaps for in-depth and advanced threat analysis.

VISIBILITY

NSFOCUS ISOP delivers network-cross security visibility to meet decision-making and analysis requirements for different users. The executive dashboard helps chief officers to get insights from a higher level and quickly make decisions or adjust security strategies; Detailed events reports help security operations staff to improve efficiency; and critical events or correlated information helps security analysts to carry out threat hunting and discovery. Additionally, modular components are provided for users to create their own reports easily.

FLEXIBLE DEPLOYMENT

As a software-based platform, NSFOCUS can be deployed on a stand-alone server or the cloud. It provides customers a simple, flexible, efficient, and out-of-the-box management platform.

PLATFORM SPECIFICATIONS

Operation System	Hardware Requirement per node	Deployment Mode	Performance
			Access EPS (Events Per Second)
CentOS 7.3 or above	CPU： 20C(40T) Memory: 256G HDD: 12 * 4T Disk SSD: 2 * 500G	Single	2,000 – 5,000 EPS
	CPU： 20C(40T) Memory: 256G HDD: 12 * 4T Disk SSD: 2 * 500G	Cluster (3 nodes)	6,000 – 15,000 EPS
	CPU： 20C(40T) Memory: 256G HDD: 12 * 4T Disk SSD: 2 * 500G	Cluster (5 nodes)	10,000 – 25,000 EPS
Please Note: The capacity of EPS depends on the log type and log complexity			