NSFOCUS

2025 COMPETITIVE STRATEGY LEADER

Transforming Innovation Into High-Growth Performance and Competitiveness

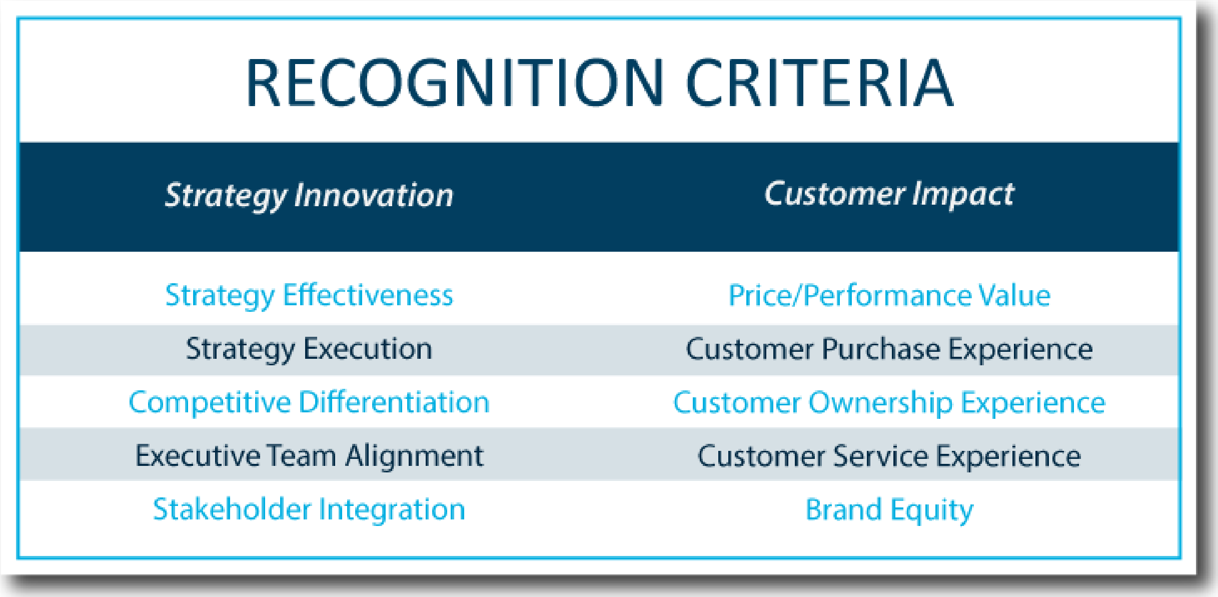
RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL AI DRIVEN SECURITY OPERATIONS INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. NSFCOUS excels in many of the criteria in the AI usage in security space.



RECOGNITION CRITERIA

Strategy Innovation	*Customer Impact*
Strategy Effectiveness	Price/Performance Value
Strategy Execution	Customer Purchase Experience
Competitive Differentiation	Customer Ownership Experience
Executive Team Alignment	Customer Service Experience
Stakeholder Integration	Brand Equity

The Transformation of AI Usage in Security Industry

The security operations industry—spanning the physical, identity, and cybersecurity domains—is undergoing a profound transformation driven by artificial intelligence (AI). Once considered a supplementary tool, AI has become a foundational element in modern security frameworks. Its integration is a direct response to the growing complexity, speed, and scale of threats that traditional security systems struggle to manage.

AI empowers security operations by processing vast datasets at unprecedented speeds, identifying patterns and anomalies that human operators might overlook. It enhances threat detection by recognizing subtle indicators of malicious activity, even within encrypted or obfuscated traffic. Predictive analytics powered by AI can forecast vulnerabilities and attack vectors before they are exploited, enabling proactive defense strategies.

In practical terms, AI automates routine tasks such as log analysis, alert triage, and incident prioritization. This automation reduces the burden on human analysts, allowing them to focus on strategic decision-making and complex threat investigations. In identity security, AI supports continuous authentication by monitoring user behavior and detecting unauthorized access attempts. In physical security, it enables facial recognition, object tracking, and perimeter monitoring, improving situational awareness and response times.

Despite its benefits, AI adoption in security operations presents a number of challenges. The sheer volume of data generated across domains can overwhelm legacy systems, leading to delays or false positives. Disparate platforms often lack interoperability, creating silos that hinder comprehensive threat visibility. Moreover, the threat landscape is evolving rapidly, with adversaries leveraging AI to craft sophisticated phishing schemes, deepfakes, and automated cyberattacks.

> *"NSFOCUS transforms cybersecurity operations through AI-driven automation and precision, achieving a 97% alert noise reduction and cutting incident response times to under 30 minutes—empowering organizations to do more with less"*
>
> ***- Pranav Sahai***
> ***Industry Analyst***

To overcome these obstacles, the industry is embracing AI-driven automation and collaborative platforms that unify data across domains. Innovations such as generative AI and edge computing are enhancing scenario planning and enabling real-time processing in resource-constrained environments. These technologies, combined with continuous learning algorithms, are building resilient, adaptive frameworks that position security operations to meet current and future challenges head-on.

As AI continues to redefine the boundaries of security operations, the industry's ability to adapt and innovate will determine its resilience against increasingly sophisticated threats. NSFOCUS exemplifies this transformation through its precision-driven platforms and strategic integration of AI, setting a new benchmark for intelligent, scalable, and proactive security frameworks.

Precision-Driven AI for Real-World Threats

With AI becoming central to modern security operations, NSFOCUS has developed precision-driven platforms that tackle one of the industry's most persistent challenges: alert fatigue. This issue—characterized by overwhelming volumes of low-value alerts—continues to strain security teams and dilute response effectiveness. To address this, NSFOCUS introduced NSFOCUS Generative Pre-trained Transformer, called NSFGPT. It is an AI security empowerment platform that integrates NSFOCUS' years of research experience in artificial intelligence and machine learning, offensive and defensive knowledge, as well as threat intelligence accumulation, and practical expert capabilities. NFSGPT incorporates NSFOCUS' security domain large model and DeepSeek dual-base model, along with various small models, knowledge bases, intelligence databases, etc. It supports the application of local security knowledge and the expansion of model capabilities based on AI Agent. It provides scenario-based AI empowerment support in an intelligent agent manner to meet customer needs. By leveraging multi-model collaborative modeling, NSFOCUS assigns confidence levels to alerts, enabling automated triage of routine events and escalation of complex threats to human experts. This human-machine synergy ensures both speed and accuracy in incident response.

A key differentiator of NSFGPT is its closed-loop optimization cycle, which continuously refines model performance using real-world operational data. This cycle captures metrics such as alert noise reduction, response latency, and expert intervention ratios, feeding them back into model training to improve accuracy, reduce false positives, and ensure sustained reliability. For example, NSFGPT delivers a 97% alert noise reduction rate, cutting response times to under 30 minutes, as demonstrated by an energy company that reduced its incident handling staff by 60%.

Complementing NSFGPT is NSFOCUS's ISOP platform—a next-generation security operations solution that integrates SIEM, XDR, and SOAR functionalities. The goal of the NSGPT application functions is to solve complex practical problems in security scenarios, covering basic functions such as security Copilot, AI voice assistant, threat assessment, response handling, incident investigation, noise reduction triage, report generation, and security knowledge Q&A.ISOP provides a comprehensive operational backbone for managing threat detection, investigation, and response. The goal of the NSGPT application functions is to solve complex practical problems in security scenarios, covering basic functions such as security Copilot, AI voice assistant, threat assessment, response handling, incident investigation, noise reduction triage, report generation, and security knowledge Q&A which automatically generates response strategies tailored to complex threat scenarios, reducing manual operator interventions by 70%.

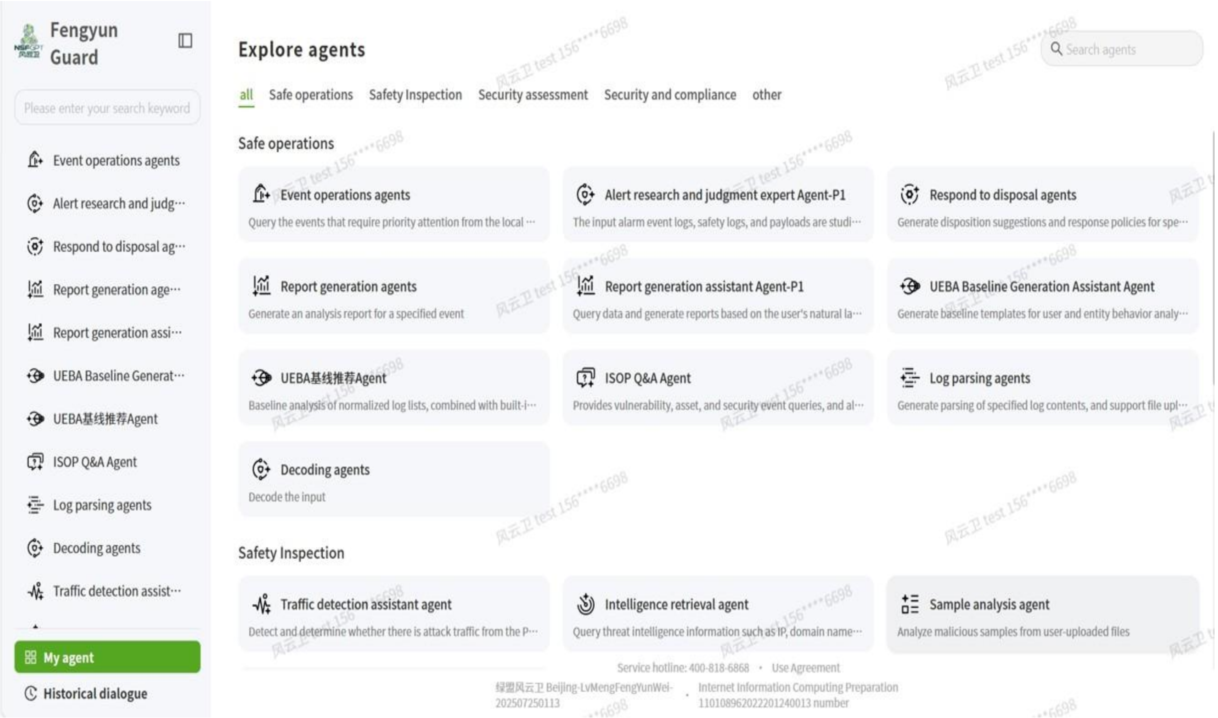
NSGPT is dedicated to completely transforming the traditional cybersecurity operation model by deeply integrating artificial intelligence with expertise in the field of security, in order to address the increasingly severe challenges of network threats. Its core objective is to enhance the intelligence level of security operations, enabling rapid identification, precise analysis, intelligent response, and effective defense of

complex network threats, thereby building a more stable, flexible, and efficient cybersecurity protection system for enterprises and organizations. This platform focuses on shortening the threat response time, improving detection accuracy, optimizing operational efficiency, and strengthening the protection of sensitive data, ensuring that the key assets of enterprises and organizations are comprehensively secured in the wave of digital transformation.

NSGPT is positioned as the intelligent hub in security operations, serving as a bridge connecting security data, analytical capabilities, and operational decisions. It is not merely a technical tool but also a comprehensive collection of security operation strategies and practical experience. By deeply integrating advanced large-model technology (SecLLM), big data processing, machine learning, and the wisdom of security experts, the platform provides one-stop security operation support, covering the entire chain of security operation processes from alarm noise reduction, threat analysis, response handling to traceability analysis. It is positioned as an intelligent assistant for security teams, aiming to enhance the quality of decision-making and response speed of the team, while reducing reliance on human experts and improving the overall security defense efficiency.

Based on the intelligent analysis capabilities of the large security model, the AI security capability platform can assist users in the auxiliary detection of messages, codes, attacks, and emails, effectively improving the speed and accuracy of malware detection, attack traffic detection, endpoint abnormal behavior detection, and phishing email detection in security monitoring and emergency scenarios. It can shorten the overall threat response time (MTTR) by approximately 75%, significantly reducing the cost of security monitoring for customers.

In a real-world deployment, a financial services organization using ISOP shortened its incident response time from 4 hours to 1.5 hours. This outcome was driven by the platform's ability to combine automated playbook generation with real-time data insights, ensuring rapid and accurate threat mitigation. Together, NSFGPT and ISOP exemplify NSFOCUS's commitment to technology-driven innovation and rapid implementation, delivering scalable, intelligent, and high-impact solutions that address both operational efficiency and the global shortage of skilled analysts.



Explore agents

Safe operations

Event operations agents
Query the events that require priority attention from the local ···

Alert research and judgment expert Agent-P1
The input alarm event logs, safety logs, and payloads are studi···

Respond to disposal agents
Generate disposition suggestions and response policies for spe···

Report generation agents
Generate an analysis report for a specified event

Report generation assistant Agent-P1
Query data and generate reports based on the user's natural la···

UEBA Baseline Generation Assistant Agent
Generate baseline templates for user and entity behavior analy···

UEBA基线推荐Agent
Baseline analysis of normalized log lists, combined with built-i···

ISOP Q&A Agent
Provides vulnerability, asset, and security event queries, and al···

Log parsing agents
Generate parsing of specified log contents, and support file upl···

Decoding agents
Decode the input

Safety Inspection

Traffic detection assistant agent
Detect and determine whether there is attack traffic from the P···

Intelligence retrieval agent
Query threat intelligence information such as IP, domain name···

Sample analysis agent
Analyze malicious samples from user-uploaded files

Service hotline: 400-818-6868 • Use Agreement
绿盟风云卫 Beijing-LvMengFengYunWei-202507250113 • Internet Information Computing Preparation 11010896202220124OO13 number

Figure 1: NSFOCUS AI Security Platform

Agility, Integration, and Global Reach

NSFOCUS demonstrates agility and integration through its ability to rapidly deploy tailored AI-driven security solutions across key verticals, including finance, telecommunications, and energy. In 2024, the company allocated 27% of its revenue into R&D, focusing on core areas such as AI security, data protection, and Zero Trust architecture. This strategic investment has led to the development of technological moats—a term referring to NSFOCUS's patented innovations like dynamic outbound control and single packet authorization. These capabilities create defensible barriers against competitors by offering unique functionality and cost advantages in high-security domains.

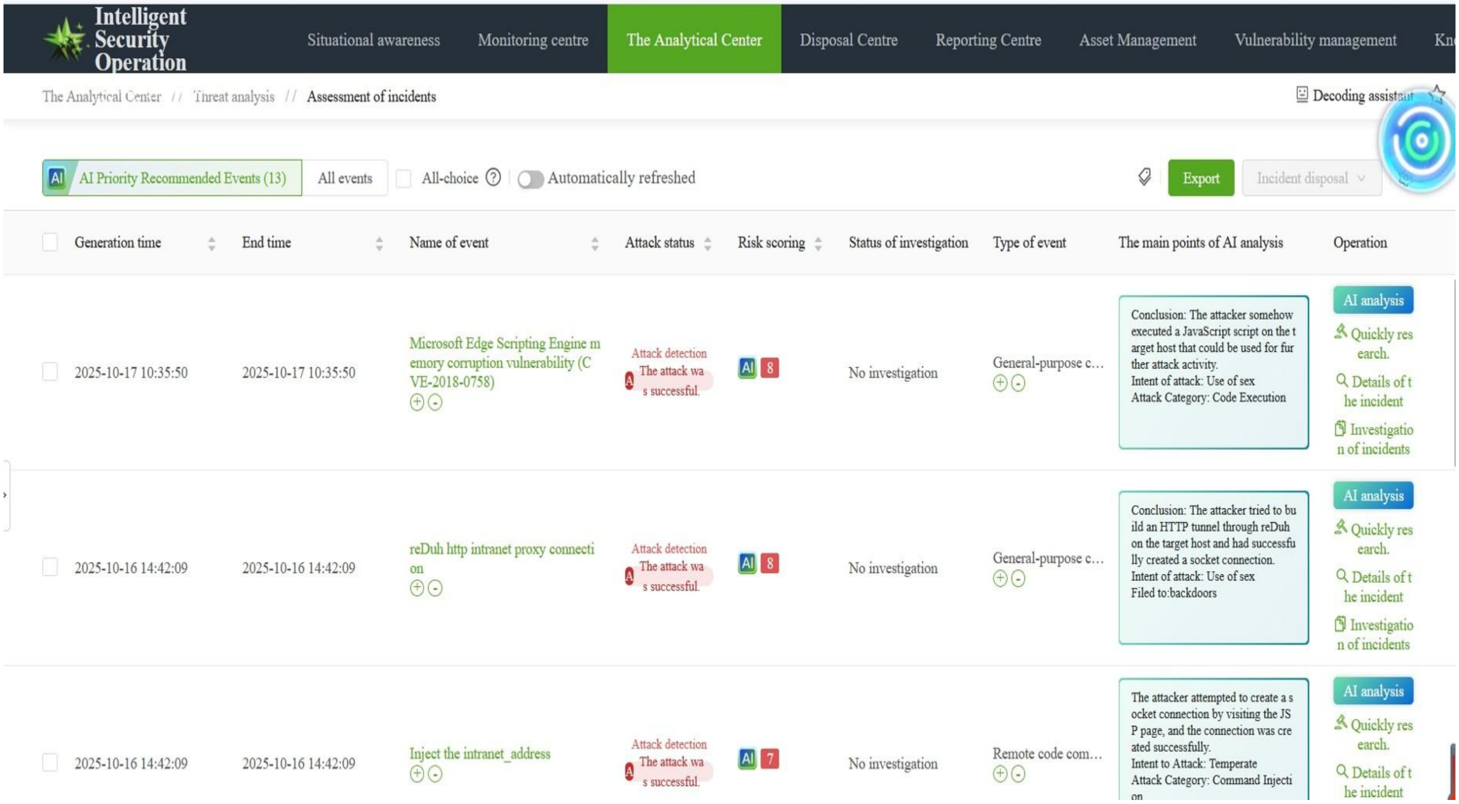
To scale its AI capabilities globally, NSFOCUS has formed deep partnerships with AWS, Alibaba Cloud, and Tencent Cloud, enabling SaaS offerings such as Cloud WAF, cloud-native container security, and cloud traffic scrubbing. These integrations are directly relevant to NSFOCUS's AI platforms—NSFGPT and ISOP—by enabling elastic resource scheduling, real-time threat mitigation, and cloud-edge coordinated protection. For example, the T-ONE CLOUD classified protection compliance platform, which incorporates AI-based compliance automation, helped a Singaporean financial institution reduce compliance costs by 40% and certification timelines by 70%, demonstrating the operational impact of NSFOCUS's AI strategy in regulated environments.

NSFOCUS's global footprint includes seven scrubbing centers across Asia-Pacific, Latin America, Europe and US, delivering 7T DDoS protection, 24/7 managed service and 10-minute response times, as demonstrated in its support for an Irish cloud service provider. These emerging markets are strategic targets for NSFOCUS's AI solutions due to their rapid digital transformation, growing infrastructure needs, and demand for scalable, cost-effective security operations.

Internally, NSFOCUS fosters agility through cross-functional task forces, daily stand-ups, and a unified operational data platform that synchronizes key metrics—such as alert noise reduction, response latency, and expert intervention ratios—across R&D, product, delivery, and operations teams. This structure enables rapid iteration and ensures that AI solutions remain aligned with real-world customer demands.

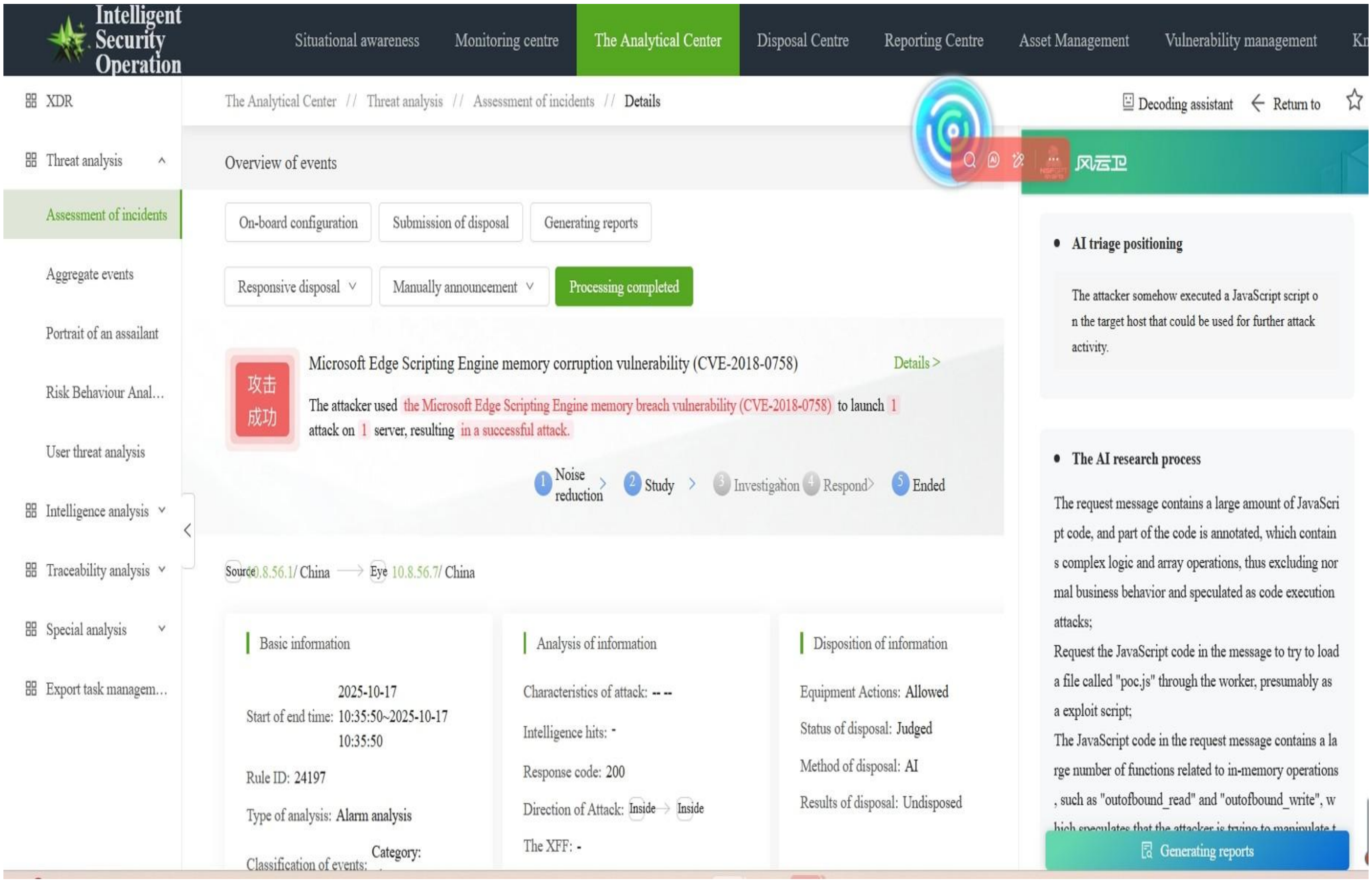
In terms of industry leadership, NSFOCUS actively contributes to technical standard development, including frameworks for Classified Protection 2.0, Zero Trust, and cloud-native security architectures. These efforts reduce interoperability gaps and promote consistent security practices across regions.

Additionally, quarterly investor briefings and university partnerships for technology transfer reinforce stakeholder alignment and accelerate innovation.



Generation time	End time	Name of event	Attack status	Risk scoring	Status of investigation	Type of event	The main points of AI analysis	Operation
2025-10-17 10:35:50	2025-10-17 10:35:50	Microsoft Edge Scripting Engine memory corruption vulnerability (CVE-2018-0758)	Attack detection The attack was successful.	AI 8	No investigation	General-purpose c…	Conclusion: The attacker somehow executed a JavaScript script on the target host that could be used for further attack activity. Intent of attack: Use of sex Attack Category: Code Execution	AI analysis Quickly research. Details of the incident Investigation of incidents
2025-10-16 14:42:09	2025-10-16 14:42:09	reDuh http intranet proxy connection	Attack detection The attack was successful.	AI 8	No investigation	General-purpose c…	Conclusion: The attacker tried to build an HTTP tunnel through reDuh on the target host and had successfully created a socket connection. Intent of attack: Use of sex Filed to:backdoors	AI analysis Quickly research. Details of the incident Investigation of incidents
2025-10-16 14:42:09	2025-10-16 14:42:09	Inject the intranet_address	Attack detection The attack was successful.	AI 7	No investigation	Remote code com…	The attacker attempted to create a socket connection by visiting the JSP page, and the connection was created successfully. Intent to Attack: Temperate Attack Category: Command Injection	AI analysis Quickly research. Details of the incident

Figure 2: NSFOCUS, Intelligent Security Operation



Microsoft Edge Scripting Engine memory corruption vulnerability (CVE-2018-0758)

The attacker used the Microsoft Edge Scripting Engine memory breach vulnerability (CVE-2018-0758) to launch 1 attack on 1 server, resulting in a successful attack.

Source 10.8.56.1/ China → Eye 10.8.56.7/ China

Basic information

Start of end time: 2025-10-17 10:35:50~2025-10-17 10:35:50

Rule ID: 24197

Type of analysis: Alarm analysis

Classification of events: Category:

Analysis of information

Characteristics of attack: -- --

Intelligence hits: -

Response code: 200

Direction of Attack: Inside → Inside

The XFF: -

Disposition of information

Equipment Actions: Allowed

Status of disposal: Judged

Method of disposal: AI

Results of disposal: Undisposed

- **AI triage positioning**

The attacker somehow executed a JavaScript script on the target host that could be used for further attack activity.

- **The AI research process**

The request message contains a large amount of JavaScript code, and part of the code is annotated, which contains complex logic and array operations, thus excluding normal business behavior and speculated as code execution attacks;
Request the JavaScript code in the message to try to load a file called "poc.js" through the worker, presumably as a exploit script;
The JavaScript code in the request message contains a large number of functions related to in-memory operations, such as "outofbound_read" and "outofbound_write", which speculates that the attacker is trying to manipulate t

Figure 3: NSFOCUS, Intelligent Security Operation

Delivering Scalable Value Through Innovation

NSFOCUS's value proposition blends cost efficiency with high-performance, AI-enhanced security operations. Its SaaS model, which includes offerings like lightweight penetration testing services, leverages AI-driven automation to reduce capital costs by 80% and vulnerability resolution time by 75%. These services are integrated with NSFOCUS's broader AI platforms—NSFGPT and ISOP—to streamline detection, triage, and remediation workflows.

The Cloud DDoS Protection Service, which provides 7T bandwidth, incorporates AI-based traffic analysis and dynamic protection algorithms to reduce maintenance costs by 60% compared to self-built solutions. Similarly, compatibility with domestic platforms like Kylin ensures zero-cost compliance, while enabling AI models to operate seamlessly in localized environments—doubling operational efficiency for government clients. NSFOCUS's patented technologies, such as dynamic outbound control (Patent No.: CN105226832B), are embedded within its AI platforms to enhance data loss prevention and access control.

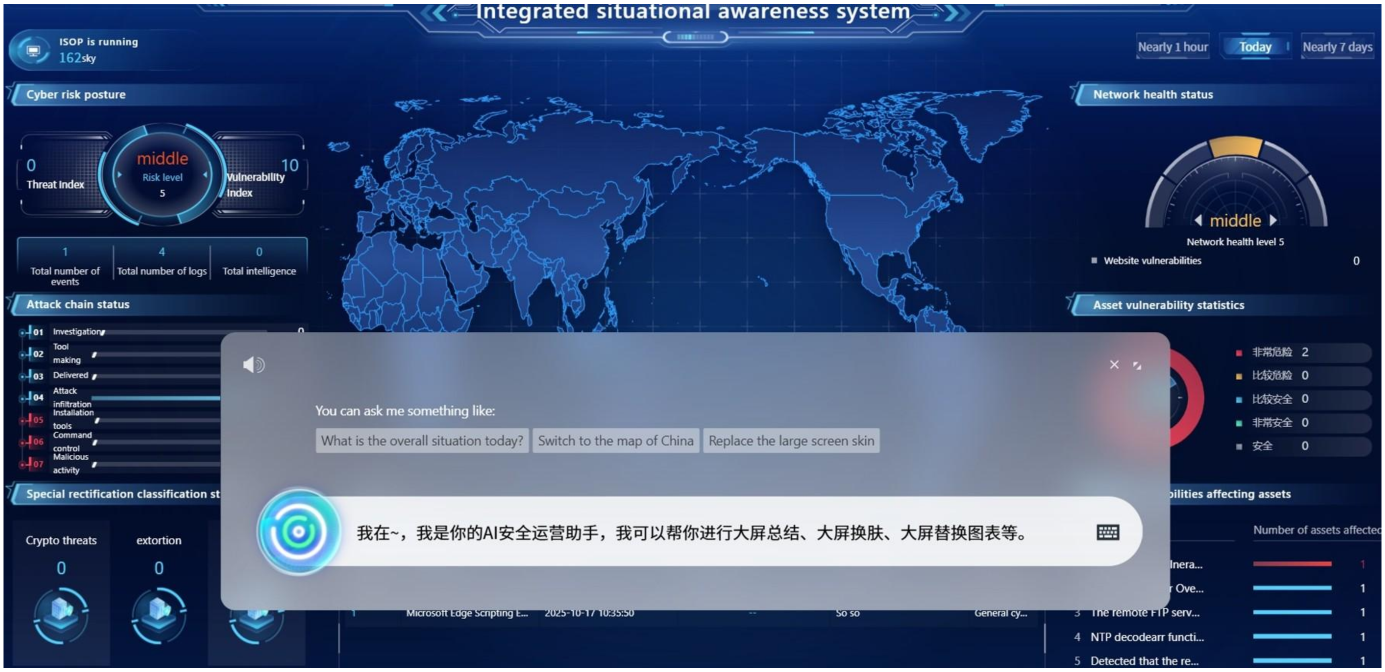
The customer purchase experience is designed to support AI adoption through interactive showcases, free trials, and technical conferences, fostering informed decisions. Pre-purchase testing and third-party validations confirm the cost-effectiveness of NSFOCUS's AI solutions, enabling clients to achieve equivalent protection at 30% of traditional budgets, as noted by a financial institution.

Post-purchase, NSFOCUS's tiered service model supports AI solution deployment across diverse customer segments. SMEs benefit from localized support via 5,000 channel partners, while large clients engage directly with expert teams. A multi-level feedback system, including Customer Success Managers and joint innovation labs (e.g., with the National Microbial Data Center), ensures continuous optimization of AI models based on real-world usage data.

NSFOCUS's global service network, comprising 50 branches and backed by ISO20000/ISO9001 certifications, achieves a 98% satisfaction rate, based on survey results from a government cloud deployment. Its Managed Security Services (MSS) integrate NSFGPT and ISOP capabilities to reduce costs by 50% for manufacturing clients, while innovations in low-altitude economy and blockchain security extend AI applicability into emerging domains.

Strategic talent development, including training 5,000 professionals, and robust compliance management ensure long-term reliability and sustained performance of NSFOCUS's AI platforms. These efforts reinforce the company's commitment to scalable, intelligent, and cost-effective security innovation.

Pre-purchase testing and third-party validations confirm the cost-effectiveness of NSFOCUS's AI solutions, enabling clients to achieve equivalent protection at just 30% of traditional budgets, as noted by a financial institution. Post-purchase, the company's tiered service model, offers localized support for SMEs via 5,000 channel partners and expert engagement for large clients, backed by a multi-level feedback system. Customer Success Managers and joint innovation labs, like one with the National Microbial Data Center, ensure tailored solutions.



You can ask me something like:

What is the overall situation today? | Switch to the map of China | Replace the large screen skin

我在~，我是你的AI安全运营助手，我可以帮你进行大屏总结、大屏换肤、大屏替换图表等。

Figure 4: NSFOCUS, Integrated Situational Awareness System

Credibility at Scale: NSFOCUS's Global Brand Impact

> *"NSFOCUS delivers enterprise-grade security at a fraction of traditional costs—cutting capital expenses by up to 80% and vulnerability resolution by 75%, while achieving 98% customer satisfaction through patented innovation, global support, and tailored services."*
>
> ***- Pranav Sahai***
> ***Industry Analyst***

NSFOCUS strengthens its brand through technology-driven leadership, validated by consistent wins in cybersecurity competitions and its founding team's deep expertise—many of whom are Tsinghua University alumni with backgrounds in computer science and security engineering. The company's reputation is further reinforced through its active participation in global forums such as the TechWorld conference, RSA, and Black Hat, where it showcases innovations like NSFGPT and other AI-driven platforms.

NSFOCUS publishes the quarterly "Security+" magazine and regular APT reports, positioning itself as a thought leader in the cybersecurity space. Its commitment to vulnerability discovery and responsible reporting enhances customer trust and contributes to the broader security ecosystem.

According to NSFOCUS, its approach emphasizes technical credibility over marketing-led positioning, setting it apart from many competitors. NSFOCUS's brand is built on technical credibility. The company operates four expert teams specializing in cybersecurity operations, threat intelligence, vulnerability research, and AI model development. These teams leverage real-world experience to continuously refine NSFOCUS's platforms and maintain a competitive edge in a rapidly evolving, low-barrier industry.

Conclusion

NSFOCUS showcases its AI expertise through its precision-driven, agile, and customer-centric approach. Its NSFGPT platform and patented technologies achieve 97% alert noise reduction and 70% faster responses, setting industry benchmarks. Strategic cloud partnerships and global reach deliver 50% cost savings, while co-creation and continuous innovation ensure tailored solutions for high-security sectors. Validated by rigorous testing and industry contributions, NSFOCUS's leadership transforms security operations, driving unparalleled value and resilience. With its strong overall performance, NSFOCUS earns Frost & Sullivan's 2025 Global Competitive Strategy Leadership for the AI driven security operations.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Competitive Strategy Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes best practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

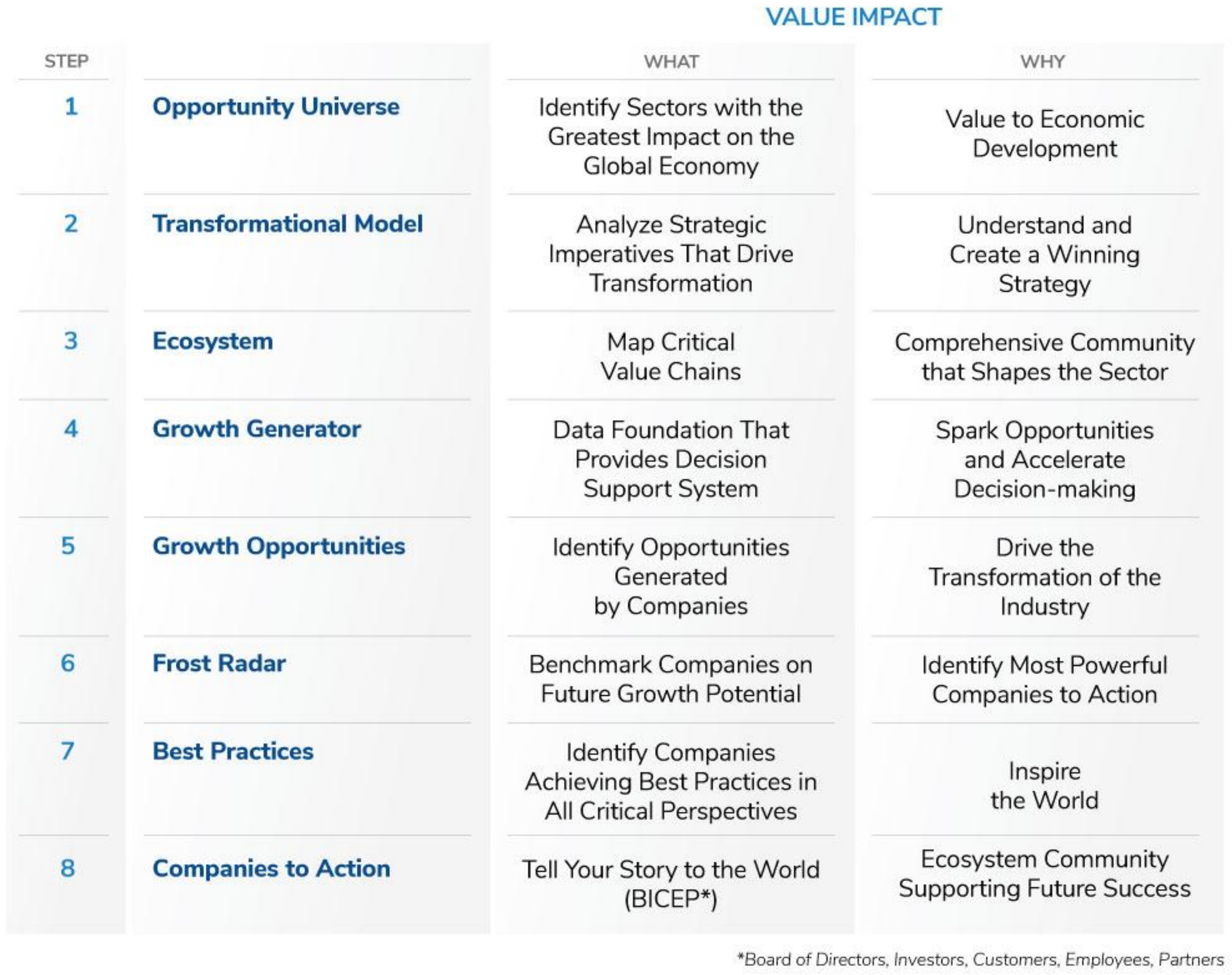
Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.



		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

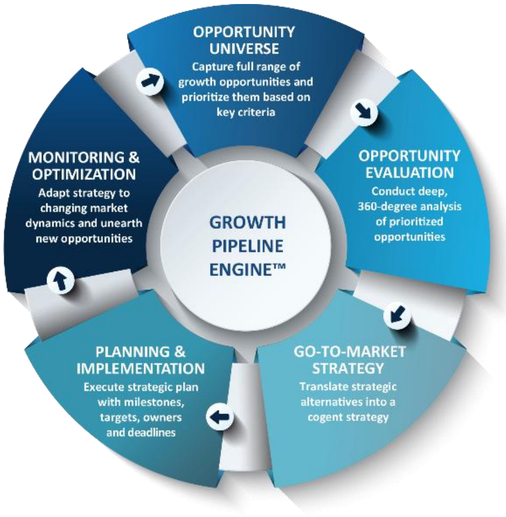
The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

Learn more.

Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** Industry Leadership

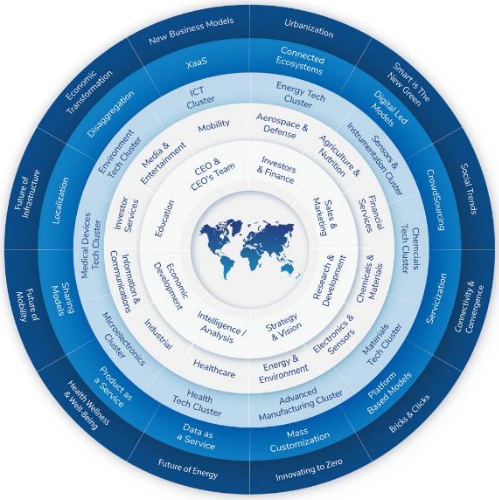

OPPORTUNITY UNIVERSE
Capture full range of growth opportunities and prioritize them based on key criteria
OPPORTUNITY EVALUATION
Conduct deep, 360-degree analysis of prioritized opportunities
GO-TO-MARKET STRATEGY
Translate strategic alternatives into a cogent strategy
PLANNING & IMPLEMENTATION
Execute strategic plan with milestones, targets, owners and deadlines
MONITORING & OPTIMIZATION
Adapt strategy to changing market dynamics and unearth new opportunities
GROWTH PIPELINE ENGINE™

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)


New Business Models
Urbanization
Smart is The New Green
Social Trends
Connectivity & Convergence
Bricks & Clicks
Innovating to Zero
Future of Energy
Health Wellness & Well-Being
Future of Mobility
Future of Infrastructure
Economic Transformation
XaaS
Connected Ecosystems
Digital Led Models
CrowdSourcing
Servicization
Platform Based Models
Mass Customization
Data as a Service
Product as a Service
Sharing Models
Localization
Disaggregation
ICT Cluster
Energy Tech Cluster
Sensors & Instrumentation Cluster
Chemcials Tech Cluster
Materials Tech Cluster
Advanced Manufacturing Cluster
Health Tech Cluster
Microelectronics Cluster
Medical Devices Tech Cluster
Environment Tech Cluster
Mobility
Aerospace & Defense
Agriculture & Nutrition
Financial Services
Chemicals & Materials
Electronics & Sensors
Energy & Environment
Healthcare
Industrial
Information & Communications
Investor Services
Media & Entertainment
CEO & CEO's Team
Investors & Finance
Sales & Marketing
Research & Development
Strategy & Vision
Intelligence / Analysis
Economic Development
Education