NRI SECURE

Empowering Your Security

How NRI Secure Protects You Against The Top Six Security Threats of 2024

Corporate Overview

Executive Summary

NRI Secure identifies six major security threats for 2024. These include supply chain risks targeting weak points, advanced phishing and ransomware threats requiring rapid detection, AI security threats from prompt injections and data leaks, internal threats from IoT devices, zero-day attacks exploiting vulnerabilities, and a severe shortage of cybersecurity personnel.

Each threat emphasizes the need for robust security measures, timely detection, and proactive management to safeguard organizations. NRI Secure's comprehensive services address these threats, enhancing security and operational efficiency.

Corporate Overview:

NRI Secure Technologies, Ltd. stands at the forefront of managed security solutions, offering a comprehensive array of cybersecurity services tailored to safeguard organizations and optimize their security operations. Headquartered in Tokyo with a regional base in Irvine, California, NRI Secure serves over 400 clients across Japan, Asia, the Americas, and the EU. With a robust team of over 400 IT security specialists, including more than 80 CISA, 40 CISM, 40 CISSP, and 150 GIAC certified professionals, NRI Secure is committed to delivering security solutions with precision, speed, and efficiency.

Key Services and Customer Insights

Neo SOC: Tailored 24/7 Security Monitoring

Neo SOC offers round-the-clock cloud-based security services, including monitoring, alerting, and managed detection and response, tailored to each organization. It ensures constant monitoring, swift threat detection, and prompt response execution.

Managed EDR (MDR) Service

Enhance your cyber defense with NRI Secure's endpoint monitoring and managed response service. This service provides 24/7 protection and proactive defense, ensuring continuous monitoring and swift threat response.

Co-Managed SIEM with Security Specialist Team

NRI Secure's Co-Managed SIEM service integrates expert SIEM management with tailored monitoring. It offers 24/7 oversight, rapid alert analysis, and efficient incident response, ensuring robust security operations.

Hybrid Penetration Testing Services

NRI Secure's hybrid penetration testing services combine manual and automated methods for comprehensive security. This approach ensures cost-effective, thorough assessments, and identifies vulnerabilities that automated tools might miss.

Comprehensive Security Consulting Services

NRI Secure's consultants offer thorough gap analysis and policy development to strengthen security. They craft robust security plans tailored to your needs, providing strategic guidance and practical solutions.

AI Red Team Security Assessment Service

NRI Secure's AI Red Team Service proactively identifies and mitigates AI system vulnerabilities. It addresses risks like prompt injections and data leaks, ensuring comprehensive protection for AI-enabled environments.

Company Overview

NRI Secure Technologies, Ltd. is a leading provider of managed security solutions, with a comprehensive portfolio of cybersecurity services designed to protect organizations and enhance the efficiency of their security operations.

With its main office in Tokyo and a regional base in Irvine, California, the company caters to over 400 clients across Japan, Asia, the Americas, and the EU.

NRI Secure boasts a team of over 400 IT security specialists, including more than 80 CISA, 40 CISM, 40 CISSP, and 150 GIAC certified professionals, underscoring its commitment to delivering security solutions with precision, speed, and efficiency.

Voices of Our Customers

Marubeni-Itochu Steel America Inc.

NRI Secure caters to our group companies' distinct security needs with their managed security offerings and adaptable solutions that's unlike other security firms. We appreciate their professionalism and rely on their years of experience to help ensure our operations continue to run smoothly and securely.

Safer Foundation

We were recommended NRIS by our engineer, and they have proven to be an excellent choice. We have regular meetings with them, receive quarterly reports, and they helped us during a ransomware incident. Their services are fully customized to our needs, monitoring everything in our network, and providing useful features and tools.

CDF Capital

• Is there anything, in particular, that NRIS should improve?
No, nothing I can think of.

• How do you feel about the report documents by NRIS?
I love them. They go over any anomalies each quarter, following up on anything abnormal. The reporting is very detailed, but I can also get a high-level view. It's presented very well.

2024's Security Landscape

1

Supply Chain risk

Attackers target weak points in the supply chain. Small sites and factories are especially vulnerable due to inadequate security. Quick detection and prevention of secondary damage are crucial.

2

Advanced Phishing and Ransomware Threats

Ransomware infections through phishing emails and websites are on the rise and unavoidable. It's crucial to quickly detect and isolate these threats, and to preserve evidence such as operation logs, as malware often targets endpoint devices.

3

Severe Security Personnel Shortage

Companies face a constant shortage of cybersecurity professionals. High turnover makes retaining expertise difficult. Outsourcing to specialized vendors can be a solution.

4

Zero-Day Attacks and Advanced Threats

Secure cloud services reduce risk, but attackers are getting more skilled. Zero-day attacks are increasing, making critical information more accessible. Companies need tailored attack simulations to visualize and mitigate risks.

5

Internal Threats Using New Technologies like IoT Devices

WFH evolution and IoT device adoption increase internal threats. Defining security rules, identifying gaps with external standards, and effective risk visualization are essential.

6

AI Security: A New Frontier

The advent of LLM AI introduces novel threats such as prompt injections and data leaks, spotlighting the urgent need for meticulous AI security assessments.

Your Security Allies: NRI Secure's Suite of Services

NeoSOC: Tailored 24/7 Security Monitoring

NeoSOC provides 24/7 cloud-based security services, including monitoring, alerting, and managed detection and response, customized for each organization via a SOC-as-a-Service model.

Managed EDR (MDR) Service

Upgrade your cyber protection with NRI Secure's advanced endpoint monitoring and managed response. Our proactive defense provides 24/7 protection, tailored to your needs.

Co-Managed SIEM with Security Specialist Team

Elevate your defense with NRI Secure's SOC Analyst as a Service, integrating expert SIEM co-management. Our pros offer 24/7 tailored monitoring, swift alert analysis, and response, fortifying your security with precision and expertise.

Hybrid Penetration Testing Services

Get comprehensive security from all angles with our blend of manual and automated tests. Our experts ensure cost-effective and thorough assessments for complete coverage.

Comprehensive Security Consulting Services

Our seasoned consultants provide gap analysis and policy development to fortify your security. Leveraging extensive expertise, we craft robust plan tailored to your unique needs.

## AI Red Team Security Assessment Service

Stay ahead of threats with NRI Secure's AI Red Team Service. Proactively identifying and mitigating vulnerabilities in AI systems, we safeguard your business against sophisticated risks like prompt injections and data leaks.

NeoSOC: Tailored 24/7 Security Monitoring

Do you have the visibility of your environment?
Are you confident that you can detect any suspicious activities?
Do you have knowledge on how to investigate and handle an incident?

**Our Monitoring Service Detects Incidents and
Quickly Alerts You with Actionable Information**
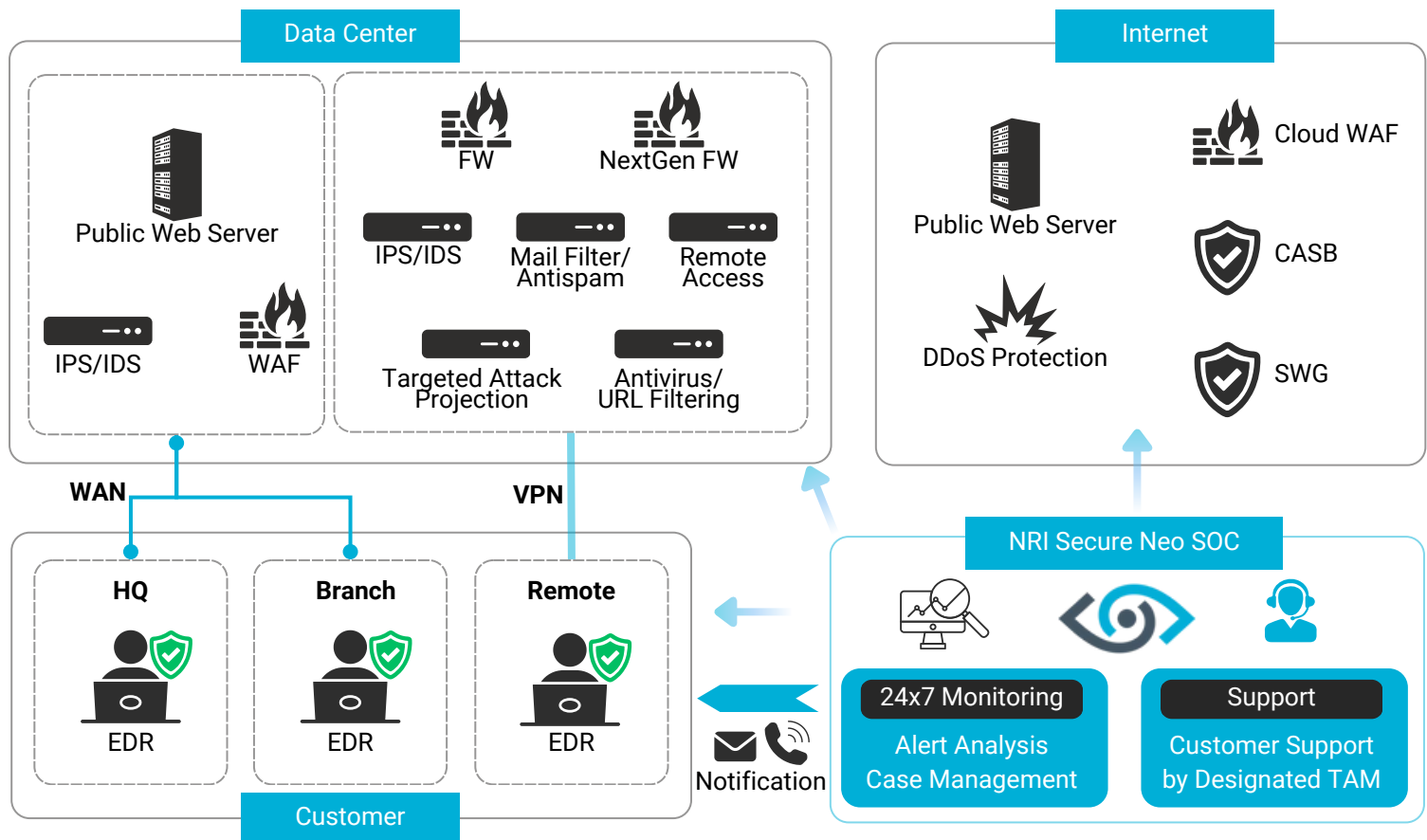
What makes "Neo"

✓ Support for 400+ security devices, solutions, and services

✓ 24/7 stable, sustainable service from our skilled team

✓ Filtering of false positives to focus on critical cases

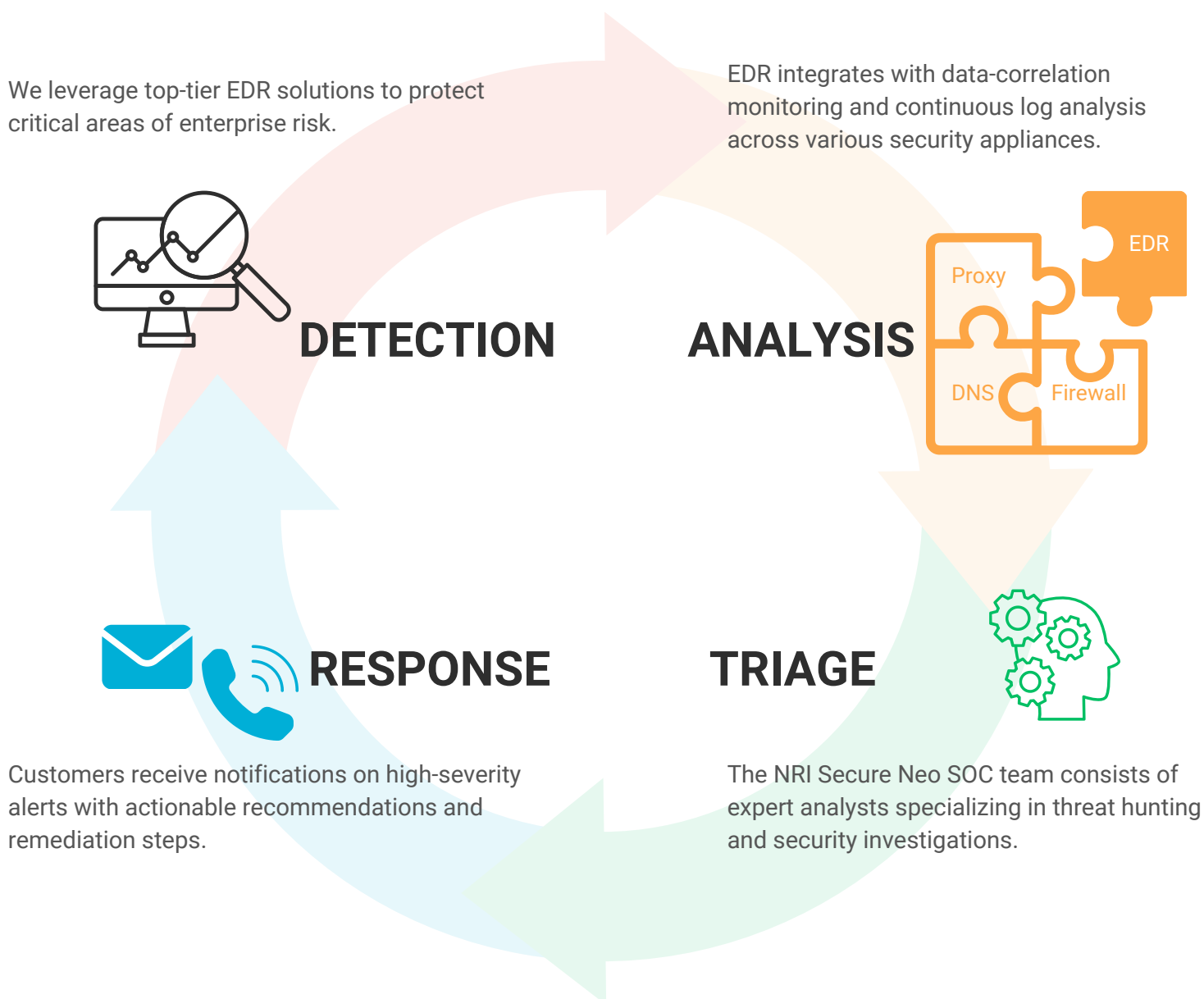✓ Keeping your organization updated on latest threat trends

Managed EDR (MDR) Service

Can you quickly detect security incidents like malware infections or attacks?
Can you prioritize and respond to security incidents effectively?
Can you identify the root cause to prevent future incidents?

**24 x 7 Security Monitoring Solution with Active Containment,
Tailor-made for the Zero-Trust Era**

We leverage top-tier EDR solutions to protect critical areas of enterprise risk.

EDR integrates with data-correlation monitoring and continuous log analysis across various security appliances.

DETECTION

ANALYSIS

Proxy
EDR
DNS
Firewall

RESPONSE

TRIAGE

Customers receive notifications on high-severity alerts with actionable recommendations and remediation steps.

The NRI Secure Neo SOC team consists of expert analysts specializing in threat hunting and security investigations.
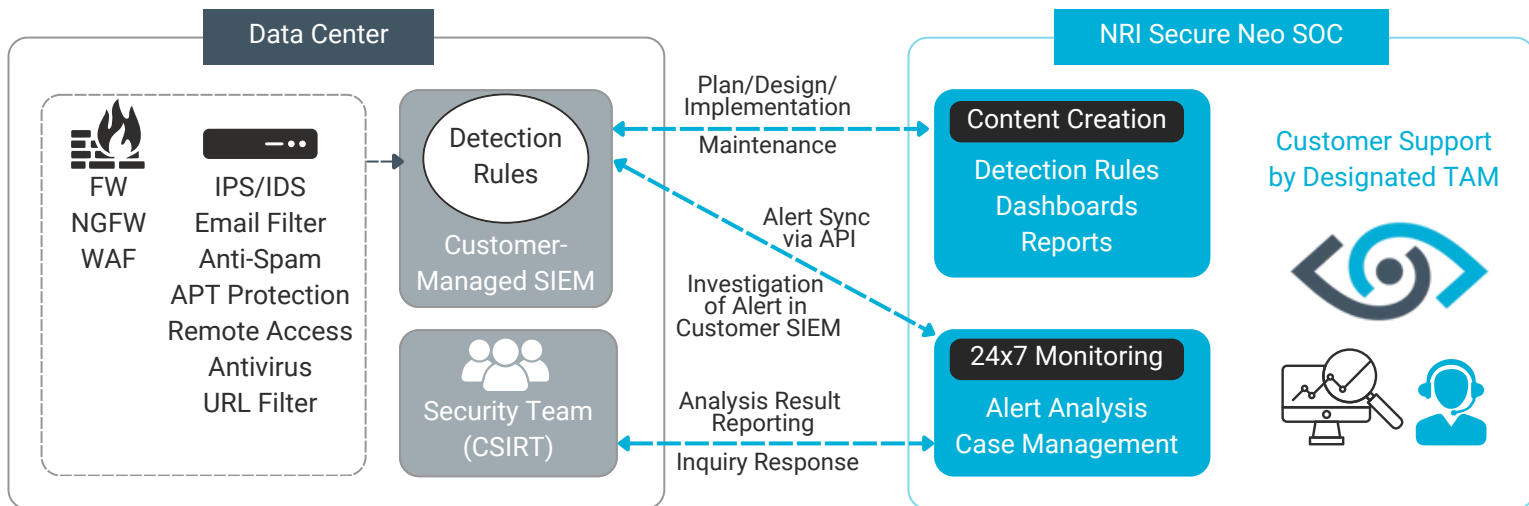
Co-Managed SIEM with Security Specialist Team

Can you understand the true cause of the alert your SIEM detected?
Are you confident that your SIEM operation is appropriate and efficient?
Do you have the human resources for around-the-clock, 24x7 monitoring?

**Our Monitoring Service Detects Incidents and
Quickly Alerts You with Actionable Information**

Category	Item	Customer	Neo SOC
Security Management	New Device Log Ingestion		✓
Security Monitoring	Rule Creation		✓
	Threat Hunting		✓
	Rule Addition for New Attacks and Vulnerabilities		✓
	24x7 Security Monitoring		✓
	Alert Reporting		✓
Incident Response	Traffic Restriction/Host Isolation	✓	✓
	Communication with Users on Incidents	✓	

What makes "Neo"

✓ SIEM operation implementation from the ground up

✓ Tailored SIEM optimization for your organization

✓ 24/7 stable, sustainable service from our skilled team

✓ Keeping your organization updated on latest threat trends

Hybrid Penetration Testing Services

Why Your Business Needs Penetration Testing

- Uncover hidden system vulnerabilities before criminals do
- Strengthen security processes and strategies
- Lower remediation costs and reduce dwell time
- Adhere to regulatory compliance around security and privacy
- Preserve brand reputation and customer loyalty

Cloud Services, Web Application Servers

Web Application Penetration Testing
Penetration testing to dig deeper and uncover vulnerabilities which automated tools cannot detect
» Manual testing that accounts for application logic and practical business context

Cloud Security Posture Assessment
Security assessment against third-party IaaS/PaaS to uncover security risks in configuration and management.
» Assessment Items: Network Security / Account Security, Management Configuration, Compliance (CIS, PCI-DSS, GDPR, etc.)

Internal Assets, Servers, Network Devices

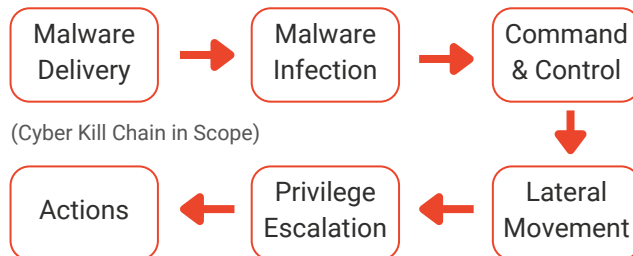**Internal Penetration Testing (Scan-based)**
Penetration testing provides visibility of assets in the network, such as open ports and running services, and identifies existing vulnerabilities in these findings.
» Testing performed against internal IP addresses acting as an internal attacker.
» Testing can be performed on-site or remotely from NRI Secure's offices using VPN access.

Internal Penetration Testing (Threat-based)
Manual penetration testing simulates the real-world attacks to evaluate the resilience of the target environment. NRI Secure offers customizable test scenarios, methods, and perspectives according to the client's requirements and the goals.

Malware Delivery → Malware Infection → Command & Control

(Cyber Kill Chain in Scope)

Actions ← Privilege Escalation ← Lateral Movement

Internet-facing Assets/IP Addresses

External Penetration Testing
Penetration Testing performed via the Internet without any prior information about the target networks/assets, emulating highly skilled external adversaries (black-box testing).

Why NRI Secure?	
Cost-effective combined test methods (tools/manual)	Testing is performed by skilled and experienced security experts utilizing the latest threat intelligence
Thorough testing from multiple perspectives	Utilizes thorough and deep inspection from various perspectives by combining multipletools and methods
Threat-based testing to emulate real-world attacks	Threat-based testing follows the cyber kill chain to evaluate the target environment's resilience to real-world cyberattacks
Web Application Testing manually performed by experienced experts	Manual testing considers application logic and business context to detect vulnerabilities which automated tools cannot
Quality and technical capability accredited by CREST	NRI Secure is CREST certified as an Accredited Company Providing Penetration Testing

Comprehensive Security Consulting Services based on Extensive Knowledge and Experience

We provide services that cover entire security life cycle.

SECURITY ASSESSMENT

🔍 Gap Analysis (NRI Secure Framework based)

Security assessments are conducted using our proprietary framework to create improvement roadmaps for your company.

Two versions are available: Brief (approx. 90 checked items) and Premium (approx. 270 items per system/area) in accordance with budget and requirements.

🔍 Gap Analysis (Customer Policy based)

Security assessments based on your IT/Security/HQ policy and create roadmaps to meet your security needs.

POLICY DEVELOPMENT

🔍 Policy Development (Template-based)

Create your policy document(s) using our templates. It will be tailored to your requirements.

🔍 Gap Analysis

Analyze gaps between your current policy and major global standards, such as NIST, SP800, and ISO27000. The resulting report(s) can assist in highlighting items to be addressed and evaluated.

🔍 Advisory

Provide information from our knowledgebase, such as best practices, cases from other companies related to specific issues, and suggest revisions to your policy.

PROJECT SUPPORT

🔍 Project Management Office (PMO)

Manage progress, issues, and tasks for security projects, such as security solution implementation.

🔍 Planning/Product Selection Support

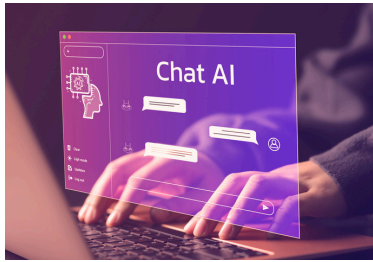Create a plan for security improvements and/or make suggestions about ideal products/solutions for your environment.

CHECK
Assessment

PLAN
Policy Development

DO
Solution
Implementation

AI Red Team

Specialized Security Assessment Service for AI-Enabled Systems

In recent years, AI usage has surged across industries, introducing novel vulnerabilities.

Prompt to LLM System Assessment: Comprehensive evaluation spanning prompt injection to overall system security.

Threats in LLM EX RAG Systems and NRI AI Red Team Assessment Scope

(Numbers 1 to 6 indicate the flow of responses when asking questions to the generative AI)
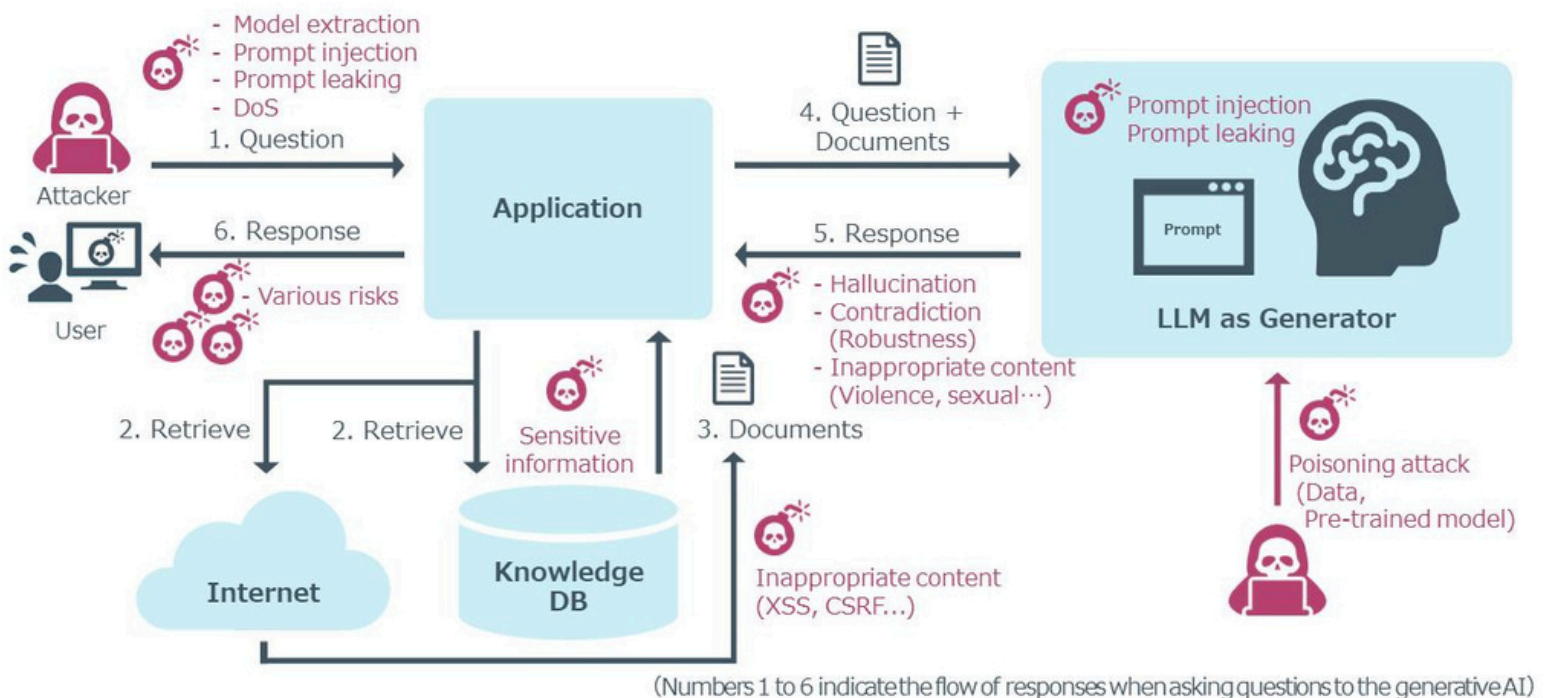
What You Get

✓ Efficient, Comprehensive, and High-Quality Assessments

Our automated assessment effectively detects vulnerabilities, complemented by manual checks by LLM security experts for deeper analysis.

✓ Assessments with Complete Coverage of a System and its Components

We use our traditional security assessment expertise to uncover AI-related vulnerabilities throughout the platform, including OWASP LLM Top 10. Our holistic approach evaluates every component for a comprehensive understanding of potential vulnerabilities.

✓ AI Blue Team Service Collaboration

AI Blue Team will leverage insights from AI Red Team's attack simulations to enhance its monitoring capabilities, based on observed successful attack strategies. This synergy bolsters the security of AI services, leveraging the strengths of both services for comprehensive protection.

Why NRI Secure?

Our value lies in the principle that "Security Starts with Visibility." We pride ourselves on our unique ability to visualize raw data and take the necessary measures based on our technical expertise.

1 End-to-End Security Management

Trust us with every aspect of your security strategy, from inception to execution.

2 Tailored Monitoring Solutions

Customize your 24x7 monitoring services to align with your specific security requirements.

3 Consulting Excellence

Our qualified consultants, driven by log monitoring, provide frequent reporting and consulting, ensuring your security stays on the right track.

4 Customize & Scalability

Customized security solutions and strategies developed based on the specific needs and risk profile of the enterprise.

NeoSOC

Neo Soc: Your Customized 24/7 Cloud Security Solution. Tailored protection for your unique business needs, ensuring peace of mind and growth.

Why Neo? It's where flexibility meets the forefront of security technology, ensuring your defenses are always ahead of the curve. Our Neo Soc platform embodies the future of SOC-as-a-Service, offering a comprehensive suite tailored to elevate your security posture and drive business success.

Our Quality Standard

SOC 2 Type II Certification

Independent Audit Verifies NRI Secure's Internal Controls and Processes. This report contains information on the development and operation status of internal controls, including security, based on international standards. This allows third parties and customers to easily understand the status of internal controls and security measures, which gives greater peace of mind for customers using our services.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

Empowering Your Security

In our mission to protect your organization and optimize your security resources with accuracy, speed, and efficiency, we are committed to safeguarding you from all threats. To achieve this, we utilize industry-leading security technologies.

Our Team

Peter Vu

Principal IT Security & Business Development Executive

Yusaku Sato

Senior Manager of Pentest & Security Assessment Team OSCP, GCIH, GWAPT

Professional Certifications

Partner Vendors & Security Tools

Unlocking Cyber Resilience with NRI Secure: A Proven Approach

Elevate Your Security Posture with NRI Secure's PoC

In today's digital-first world, your organization's cybersecurity framework is not just a defense mechanism; it's a strategic asset. NRI Secure leverages unparalleled expertise and innovative technologies to transform your security landscape. Our Proof of Concept (PoC) isn't just a demonstration; it's your first step towards impenetrable cyber resilience.

Bespoke Security Solutions:

At NRI Secure, we understand that one size doesn't fit all. Our PoC offers tailor-made solutions that align with your unique business needs, ensuring comprehensive protection where it matters most.

Advanced Threat Intelligence:

Our proactive approach harnesses advanced threat intelligence, providing your organization with predictive insights and the agility to preempt potential threats, keeping you one step ahead of cyber adversaries.

Innovative Technology Integration:

Leveraging the latest in cybersecurity technology, our PoC showcases seamless integration capabilities, enhancing your existing systems without disrupting operations, ensuring smooth and secure transitions.

Robust Compliance Assurance:

Navigate the complex web of regulatory requirements with ease. Our solutions not only ensure your security but also guarantee compliance with industry standards, safeguarding your reputation and customer trust.

Take the Next Step: Engage with NRI Secure

Ready to experience a transformation in your cybersecurity approach? Contact us to schedule your customized PoC. Discover the NRI Secure difference and embark on a journey to unparalleled cyber resilience.

/NRI SECURE/

Empowering Your Security

NRI SecureTechnologies, Ltd.
26 Executive Park Suite 150, Irvine, CA 92614, USA
nri-secure.com

info@nri-secure.com

TEL: +1-949-537-2957
FAX: +1-949-284-4355
Headquarters: Tokyo Sankei Building, 1-7-2 Otemachi, Chiyoda-ku, Tokyo 100-0004