securonix NEC

INDUSTRY: **MANAGED SECURITY SERVICES PROVIDER (MSSP)**

LOCATION: **ASIA PACIFIC**

CASE STUDY

NEC Asia Pacific Transforms Security Operations with Securonix Unified Platform

Challenge: NEC Asia Pacific PTE Ltd faced mounting complexity managing infrastructure and cybersecurity for diverse clients across industries. Their traditional SIEM lacked AI and automation, leading to time-consuming manual detection efforts, slow response times, and difficulties meeting SLA requirements. Security operations were hampered by high false positive rates, tool fragmentation, and a lack of advanced analytics to identify insider and emerging threats effectively.

Solution: NEC deployed the Securonix Unified Defense SIEM platform, integrating SIEM, UEBA, and SOAR capabilities to consolidate operations and automate threat detection. With machine learning-driven analytics, insider threat detection, and automated response playbooks, the solution significantly improved the efficiency and accuracy of NEC's security team. Cloud-native scalability and expert partner support ensured rapid onboarding and alignment with NEC's service expansion across geographies.

Benefits

- **60%+ Reduction in False Positives** through AI-driven alert tuning
- **70%+ True Positive Detection Accuracy** with behavioral analytics
- **40% Faster Mean Time to Respond (MTTR)** via automated playbooks
- **50%+ Detections Identified as Insider Threats,** improving internal security posture

Results

NEC achieved a 40% faster mean time to respond, over 70% detection accuracy, and more than 60% reduction in false positives with Securonix.

- **40% Faster** MTTR
- **70%+ Detection** accuracy
- **60%+ Reduction** in false positives

> “Securonix’s unified SIEM, UEBA, and SOAR platform has transformed our ability to detect, respond, and automate responses to threats. With their native integration and AI capabilities, we’ve significantly improved our MTTD and MTTR while enhancing our SOC’s efficiency. It’s one solution that does it all—and does it well. Together with Securonix, we offer advanced, AI-driven security services that empower our customers with faster response times and more intelligent, autonomous operations.”
>
> – Job Chan, Head of RHQ Managed Services, Vice President, NEC Asia Pacific Pte Ltd

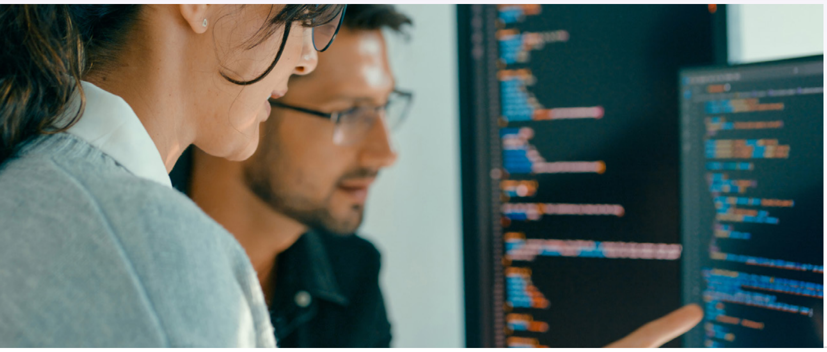
The Challenge

NEC Asia Pacific Pte Ltd delivers comprehensive infrastructure and cybersecurity solutions to various clients across multiple industry verticals. Their services span security monitoring, threat intelligence, infrastructure support, workplace solutions, and service desk operations, forming a fully integrated offering for their customers. Supporting these operations is a security operations team of 30 professionals, including analysts, engineers, threat hunters, and monitoring specialists, who work collaboratively to safeguard organizations’ digital assets and operational integrity.

As the threat landscape evolved rapidly, the team encountered significant challenges maintaining an effective security posture. Initially, NEC utilized a basic log management system, which later evolved into a full-scale deployment of McAfee’s SIEM platform. While this transition represented a step forward, it fell short of meeting the growing demands of modern threat detection and response. The absence of advanced analytics and machine learning capabilities meant the team was burdened with manual processes for developing detection use cases and responding to threats. This manual effort made it difficult to react quickly to emerging threats within their required service level agreements. Additionally, the complexity of managing and integrating multiple disparate tools strained both the technical infrastructure and the team’s resources.

Recognizing these limitations, NEC sought a solution that went beyond the scope of traditional SIEM platforms. They needed an intelligent, automated, and scalable system—one that could seamlessly integrate machine learning, advanced analytics, and orchestration to not only reduce operational overhead but also elevate the value delivered to their customers.

> “We are proud to partner with NEC Asia Pacific in securing their customers across the region. Our unified platform enables them to provide best-in-class security monitoring and incident response, while driving operational efficiency and delivering measurable business outcomes.”
>
> – Ajay Biyani, Vice President, Sales - APMEA, Securonix



Key Challenges

- **Inability to Detect Emerging Threats Rapidly:** Prior tools lacked advanced analytics and automation, making it difficult to keep up with evolving threat vectors and ensure timely detection.
- **High Reliance on Manual Processes and Policy-Based Detections:** Threat detection workflows were heavily dependent on manually developed use cases, increasing response time and analyst fatigue.
- **Lack of AI and Machine Learning Capabilities in Prior SIEM Tools:** The absence of intelligent detection technologies reduced the effectiveness of security monitoring and threat hunting efforts.
- **Difficulty Meeting SLA Commitments for Incident Response:** Manual investigation and limited automation made it challenging to respond to security incidents within customer SLA windows.
- **Inefficient Use of SOC Analyst Resources and High False Positive Rates:** Analysts spent excessive time managing false positives and conducting repetitive tasks instead of focusing on higher-value initiatives.
- **Complex Toolsets Requiring Steep Learning Curves and More Training:** Legacy solutions required extensive training and resource allocation to maintain, reducing team agility and operational efficiency.

Key Features Utilized

- **Unified SIEM with Native UEBA and SOAR Capabilities:** Delivered end-to-end threat detection, behavioral analytics, and automated response within a single, seamlessly integrated platform.
- **Integrated Machine Learning and AI-Driven Threat Detection:** Enabled advanced threat identification and adaptive detection mechanisms across dynamic attack vectors.
- **Behavioral Analytics for Insider Threat Detection:** Provided visibility into anomalous user activities, identifying over 50% of detection events as insider threats.
- **Automated Incident Response Playbooks:** Improved speed and reduced manual effort, contributing to a 40% reduction in MTTR through threat chaining and correlation.
- **Custom Use Case Development and Fast Data Correlation:** Led to more than 70% True Positive detection accuracy in a 6-month period.
- **Scalability and Cloud-Native Architecture:** Supported efficient expansion across multiple geographies with high availability and operational flexibility.
- **Strong Partner Enablement and Training Support:** Ensured effective onboarding and sustained operational maturity through continuous enablement and knowledge transfer.

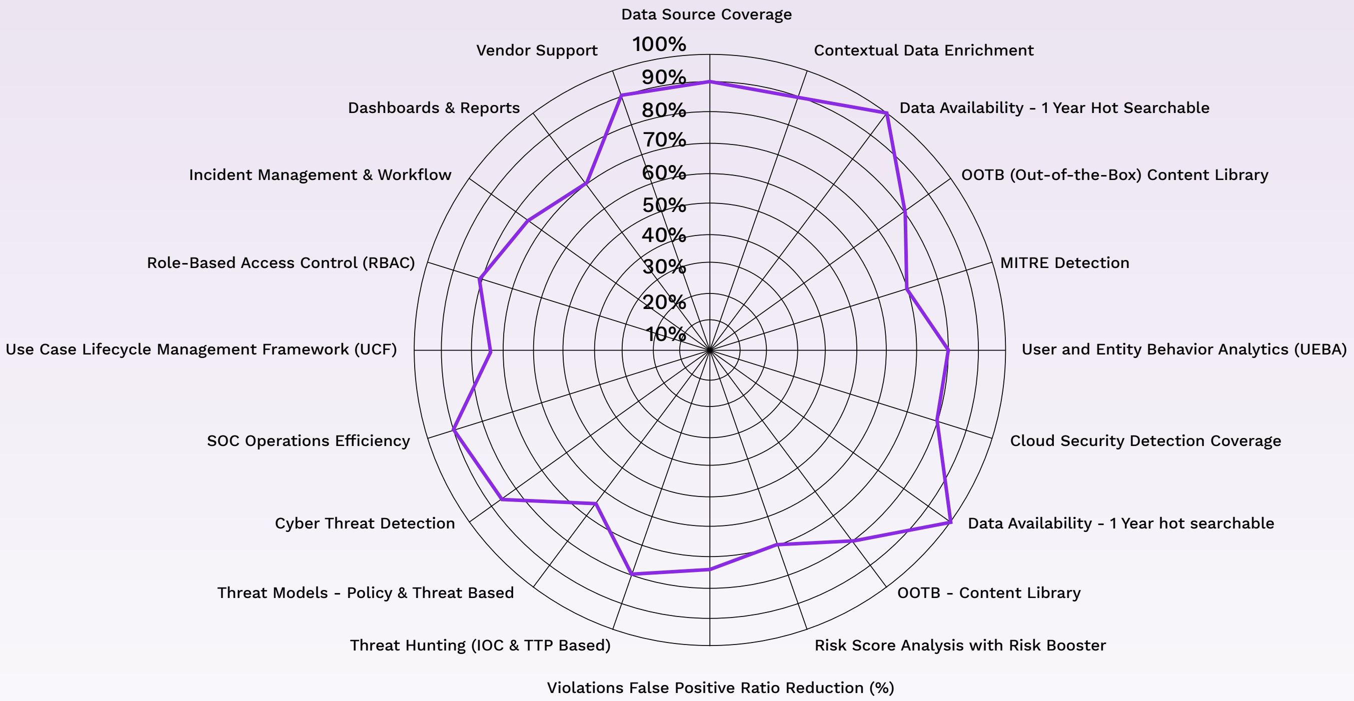
Benefits

- **Over 60% Reduction in False Positives:** Driven by well-tuned policies and AI-led detection mechanisms, enabling analysts to prioritize high-fidelity alerts.
- **70%+ True Positive Detection Accuracy:** Over six months, reinforcing confidence in automated decision-making and threat validation.
- **40% Faster MTTR:** Achieved through intelligent threat chaining and automated correlation, accelerating containment and recovery timelines.
- **More than 50% of Detection Events Identified as Insider Threats:** Empowering NEC to address internal risks with greater precision.

Benefits

- **Achieved and Treated 35% of Detections Related to Credential Dumping and Logon Behaviors:** Informing internal policy enhancements around password sharing and credential misuse.
- **Enhanced SOC Analyst Efficiency, with Less Time Spent on Manual Processes:** Freed up analyst resources through automation, allowing greater focus on strategic security tasks and process improvement.
- **Streamlined Incident Investigations:** Provided fast and detailed visibility during high-pressure scenarios, improving the speed and effectiveness of root cause analysis.
- **Faster Deployment of New Use Cases, Accelerating Time-to-Value:** Enabled rapid customization and implementation of new detection logic to address emerging threats more quickly.
- **Greater Scalability:** Supported NEC's regional growth plans with a flexible, cloud-native solution that could scale across geographies.
- **High Partner Responsiveness and Innovation:** Fast access to commercial and technical support ensured prompt assistance and ongoing innovation through close collaboration with Securonix teams.

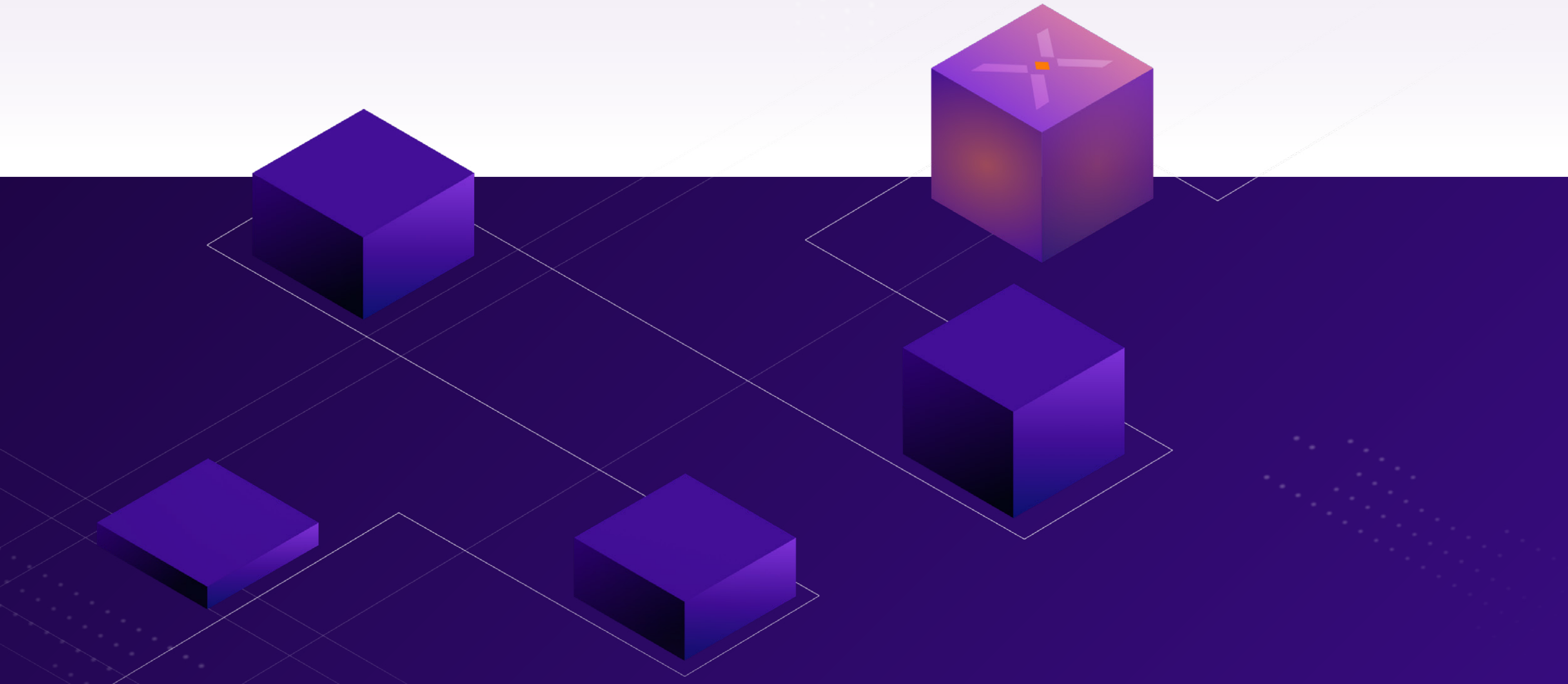
Securonix Unified Defense SIEM



Conclusion:

By implementing Securonix's unified defense SIEM and security analytics platform, NEC Asia Pacific has modernized its SOC, improved detection accuracy, reduced response times, and scaled its managed services with greater efficiency. Key improvements, including a 60% drop in false positives, 40% faster MTTR, and over 70% true positive detections, have enabled NEC to meet SLA commitments and proactively mitigate risk at scale.

For NEC, success goes beyond adopting a powerful tool—it lies in effectively leveraging it through enablement, automation, and strategic alignment. With Securonix, , NEC has not only met its SLAs, but consistently exceeded customer expectations through proactive and intelligent security operations.



About the Customer

At NEC Asia Pacific, we lead in propelling Singapore's Smart Nation initiatives, integrating trusted technology with social responsibility. As a leading information and communications technology provider, we provide innovative solutions through AI, analytics, data, digital services, enterprise infrastructure and managed services to promote safety, security and enhance the quality of life for individuals and the community. Our technological advancements, dedicated to privacy and ethical usage, solidify trust among businesses and citizens.

Together with our research laboratories, NEC Asia Pacific provides cutting-edge public safety, cybersecurity technologies and enterprise solutions to enable smart and sustainable cities, with a vision to create a brighter future.

About Securonix

Securonix is pushing forward its mission to secure the world by staying ahead of cyber threats, reinforcing all layers of its platform with AI capabilities. Securonix Unified Defense SIEM provides organizations with the first and only AI-reinforced solution built with a cybersecurity mesh architecture on a highly scalable data cloud. The innovative cloud-native solution is enhanced by Securonix EON to deliver a frictionless CyberOps experience and enables organizations to scale up their security operations and keep up with evolving threats. For more information, visit securonix.com, or follow us on LinkedIn and X.

securonix