

A man with glasses is shown in profile, focused on his work. He is sitting at a desk in a dimly lit room, illuminated by the blue and purple light of his computer monitors. He is wearing a dark sweater and has his hands on a laptop keyboard. In the background, several other monitors are visible, displaying various data and charts. The overall atmosphere is one of intense concentration and technological sophistication.

Lenovo Powers Lenovo - AI-powered Security Operations Center

Lenovo built its own AI-powered Security Operations Center, improving threat detection accuracy by 20x

Lenovo's AI-powered Security Operations Center protects 140,000 devices and has reduced mean time to detect attacks by 87.5%.

As cyberthreats grow more frequent and complex, Lenovo developed an AI-powered Security Operations Center to assess and enrich incoming alerts, helping its cybersecurity experts focus on and resolve the most significant issues faster. The knowledge and experience gained through this internal deployment now inform the AI cybersecurity solutions and services Lenovo offers its customers.

Smarter
technology
for all

Lenovo

Challenge: Protecting a Global Enterprise Against a Faster-Moving Threat Landscape

“



One of our key responsibilities is protecting Windows license keys worth tens of millions of dollars. If they were compromised, it would be more than a security issue—it would present significant financial risk. AI helps us extend the reach of our team so we can address that risk at scale.”

Greg Hansen

Director of Cyber Security Operations at Lenovo

For Lenovo, an effective Security Operations Center (SOC) is essential to protecting proprietary information and helping prevent security incidents from disrupting employee productivity. This is an especially demanding responsibility at Lenovo’s scale, where the SOC helps protect 140,000 devices used by 80,000 users across 150 countries. The challenge has become even more complex as Lenovo’s threat landscape has doubled over the past five years.

Across the industry, AI-powered attacks are becoming faster and more sophisticated, forcing security teams to identify and contain threats before they can spread across increasingly complex environments. The pressure is significant: many traditional security operations are largely reactive, still relying heavily on manual review, and 66% of SOC teams cannot keep pace with alerts.

Challenge: Managing Billions of Daily Security Events

Every day, over 15 billion computing events are analyzed across Lenovo's network, 4,000 of which require deep investigation. To protect internal networks, the team also blocks an average of 300 unauthorized devices daily.

In the past, when a security alert arrived, SOC employees had to manually review device status, file hashes, and evaluate network information to determine whether it required attention and what action to take. Highly skilled security professionals were spending valuable time filtering benign alerts, making it harder to separate noise from genuine threats. Complex, fragmented workflows across different security tools also lengthened resolution times and increased the risk of human error.

Lenovo needed to reduce manual triage and move toward a more proactive security operation—one that could filter low-value incidents, give human experts the context they needed to act quickly, and identify patterns that could help strengthen policies and prevent future attacks

15B

computing events
analyzed daily

4,000

events requiring
deep investigation

300

unauthorized
devices blocked daily

Solution: **Lenovo Powers Lenovo**

To address the growing security challenge within its own enterprise, Lenovo used its global SOC as a real-world proving ground for a new AI-powered model. Working with cybersecurity partners, the team set out to build an always-on security operation that could reduce the burden of manual alert reviews while giving analysts better context to identify and respond to genuine threats.

At the foundation of this approach was an intelligent data-ingestion platform, designed to bring together relevant security signals and reduce noise before alerts reached analysts. Lenovo then began developing the AI-enabled workflows that would help prioritize incidents and prepare the right context for human review.

“



If AI is essential to keeping pace with the threat landscape, then customers rightly expect us to use our own AI capabilities to protect Lenovo before we ask them to trust us with their own enterprise. That is why we set out to build and refine an AI-powered SOC.”

Thirumalai Seshadri Krishnakumar

Director of Advanced Service Delivery at Lenovo



“

AI is most valuable when it puts the right information in front of people at the right time. We kept refining the model with the SOC team so it could learn from their expertise and support better, more consistent and proactive decisions.”

Thirumalai Seshadri Krishnakumar

Director of Advanced Service Delivery at Lenovo



Solution: Refining the Model for Real-World Security Operations

Lenovo did not deploy the new model all at once. Over several months, the team worked iteratively with cybersecurity partners and SOC analysts to test and refine AI outputs for different alert types. The team developed playbooks that could guide AI-supported workflows, creating the foundation for additional security processes to be transformed over time.

As accuracy improved and analyst confidence grew, Lenovo put the new workflows into operation. Some AI agents began triaging incoming alerts, while others enriched alerts requiring human attention with relevant context from across Lenovo’s systems and suggested potential next steps. This enabled the highly skilled human SOC team to focus on the 25 most-critical issues each day rather than spending time on lower-level manual tasks.

Solution: Four Pillars of AI Readiness

An AI-powered SOC depends on more than the technology itself. To make the model effective across a global enterprise, Lenovo also had to prepare its people, adapt its processes, integrate the right technologies, and create strong cyber security controls.



People

Successful AI deployment depends on preparing people for new ways of working while preserving human judgment for the decisions that require it. Lenovo upskilled and cross-skilled employees and partnered with HR to support the workforce through the change, while also working with universities to introduce AI electives that help new graduates arrive with foundational AI knowledge.



Processes

Enterprise AI adoption requires teams to review and adapt the processes behind the technology. The SOC team created AI-enabled workflows and alert-specific playbooks, moving beyond traditional SOP-based processes.



Technology

AI must be integrated and refined around the organization's real operating environment. Lenovo worked with market-leading cybersecurity alliances to align AI capabilities with internal SOC processes, improving signal quality and helping reduce false positives.



Security

AI-powered cybersecurity operations must be subject to the strictest guardrails. Lenovo segregated, masked, and logged data in a controlled way to ensure sensitive information is protected.

Result: Detecting Threats Faster and More Accurately

Today, Lenovo's AI-powered Security Operations Center helps protect its global enterprise by taking over repetitive, lower-level work and bringing its highly skilled analysts the context they need to quickly and effectively respond to cyber threats. What previously could take a human analyst 45-60 minutes to investigate can now be assembled in seconds, allowing the team to focus on higher-priority incidents.

As a result, Lenovo reduced its mean time to detect an attack by 87.5%, from four hours to 30 minutes. The AI-powered model is also 20x more accurate than legacy tools at identifying malware and attacks, while reducing the false-positive rate to below 10%. Together, these improvements have reduced cybersecurity total cost of ownership by 60%.

87.5%

reduction in mean time to detect

20x

more accurate identification of malware and attacks

>80%

of low-level incidents resolved without analyst intervention

60%

total cost of ownership savings

“



By leveraging AI to shift SOC processes from reactive to proactive, our mean time to resolution has been reduced from 96 hours to just 24 minutes. This supports high uptime for endpoints, reduces cybersecurity costs, and helps ensure an attack does not spread far into the network. It also gives Lenovo a more resilient, scalable security model for a threat landscape that will continue to evolve.”

Rakshit Ghura

VP & GM, Digital Workplace Solutions at Lenovo

Result: Building a More Proactive Security Operation

With more than 80% of low-level incidents handled automatically, SOC analysts can focus on more complex, higher-priority events instead of routine manual tasks. This helps Lenovo maintain broad security coverage across the enterprise and respond more proactively to threats.

Beyond individual incidents, the team can use insights from alerts, reports, and detailed metrics to identify patterns, refine policies, and improve operations over time. Lenovo is now extending AI-powered workflows to new types of attacks, including phishing and brute-force login attempts.

“



AI allows us to apply our expertise where it matters most. By automating routine work and continuously learning from new patterns, the SOC can deliver more consistent protection today and strengthen our defenses as new threats emerge.”

Pradip Dabir

Sr. Manager, Services Delivery Engineering at Lenovo

Result: From Internal Deployment to Customer-Ready AI-Powered Security Services

By building, deploying, and operating its AI-powered Security Operations Center across its own global enterprise, Lenovo gained firsthand experience in what it takes to make AI-supported security operations work at scale. Those lessons now help Lenovo deliver AI-enhanced cybersecurity services to customers—bringing together technology, processes, and expert oversight to reduce manual workload, improve decision-making, and respond more effectively to threats.

Available in more than 180 markets, Lenovo's cybersecurity services can be purchased as a standalone offering or combined with software and endpoint services. Lenovo's end-to-end cyber resilience framework helps customers build a stronger security posture from "pocket to cloud." Geographically distributed SOC's support a range of technology environments, while services align with leading standards including ISO 27001, NIST CSF, ISO 20000, and ITIL practices.

The AI-powered SOC is one example of how Lenovo is applying AI inside its own business to solve real operational challenges. Experiences like this help inform the Lenovo AI Library—a growing collection of validated AI agents and enterprise use cases that customers can adapt to accelerate their own AI journeys. Built on the Lenovo Hybrid AI Advantage, these solutions combine proven technologies, reusable architectures, and AI services to help organizations move from experimentation to measurable business outcomes.



“

Operating an AI-powered SOC in our own global enterprise has shown us what it takes to make this model work in practice. We can bring that firsthand experience to help customers strengthen security end to end, whatever their scale, environment, or industry.”

Tiago Da Costa Silva

Security Services Director, Digital Workplace Solutions at Lenovo

Lenovo Powers Lenovo - Security Operations Center

Talk to Lenovo

Contact your Lenovo representative to discuss how these capabilities could apply to your organization.

**Smarter
technology
for all**

Lenovo

Explore Lenovo Hybrid AI Advantage

See how Lenovo helps organizations build, scale and operate enterprise AI.

Discover AI-powered cybersecurity services from Lenovo

See how Lenovo helps protect your organization.

All offers subject to availability. Lenovo reserves the right to alter product offerings, prices, specifications or availability at any time without notice. Lenovo is not responsible for typographic or photographic errors. Information advertised has no contractual effect. All trademarks are the property of their respective owners. For full Lenovo product, service, and warranty specifications, visit www.lenovo.com. ©2026 Lenovo Group Limited.