Sekuro launches Sovereign Next-Gen SIEM and Log Management Adaptive Security Platform

Pioneering, Generative AI-based solution combats adversary stealth and emerging threat tactics


Brodie Downes, Director of MSS, Sekuro

SYDNEY, NSW, AUSTRALIA, May 28, 2024 /EINPresswire.com/ -- Sekuro has today announced the launch of its Sovereign LogScale Adaptive Security Platform to revolutionise the landscape of threat detection and response and usher in a new era of cyber resilience to help businesses protect themselves against rising cyber threats.

As the world faces increasing cyber threats, Sekuro's adaptive security platform, powered by CrowdStrike® Falcon LogScale™, CrowdStrike's Next-Gen SIEM and log management offering, empowers organisations of all sizes, especially those who traditionally may not have access to enterprise-grade defences, with the technology required to increase their cybersecurity effectiveness to stop breaches.

Despite progress and maturation in cyber defences and detection technology, cyber adversaries are adapting and becoming faster and more sophisticated. CrowdStrike's 2024 Global Threat Report revealed a 75% increase in cloud intrusions, a 76% spike in data theft victims named on the dark web, and that 75% of attacks over the past year were malware-free.

Sekuro's pioneering managed security solution transcends the boundaries of conventional threat detection and response solutions by giving organisations:

1. Sovereign Architecture: Unlike traditional security frameworks, Sekuro's adaptive security

platform is designed to work seamlessly as an open and extendable platform to protect an organisation's entire extended enterprise. This platform is delivered in a totally isolated, customer specific tenancy – leaving data ownership securely in the customers' hands.


Michael Sentonas, President, CrowdStrike

2. Extended Detection & Response (XDR): XDR has emerged as the benchmark in threat detection, investigation and response. Unlike traditional siloed solutions, XDR consolidates security capabilities from enterprise data sources and control points. Leveraging analytics and AI, it automates detection, investigation, and correlation of alerts, reducing response time and enhancing security.

3. Adaptive Intelligence: The innovative Generative AI technology in Sekuro's adaptive security platform dynamically evolves its custom detection content and adapts to the ever-changing threat environment. As a result, Sekuro's cybersecurity practitioners can deliver highly efficient and effective responses to even the most sophisticated cyber-attacks, significantly bolstering the overall security resilience of organisations.

"Our team has experienced the frustrating realities of slow, costly, and painfully integrated security solutions throughout our careers. That's why we developed our Managed XDR platform, powered by CrowdStrike and AWS—to defy those limitations," said Brodie Downes, Director of Managed Services, Sekuro. "This platform is exactly what we always needed but could never get in the past. By taking a novel approach to traditional SecOps problems, incorporating human-driven threat intelligence, and using AI to reduce tech debt and the subsequent TOIL tax, we've created a solution that not only detects and blocks attacks across the enterprise, but does so faster and more efficiently than ever before."

The Power of Sovereignty
What truly makes Sekuro's security offering unique is its sovereignty. What does this mean?

 Data Independence: With data ownership entirely in the customer's hands, organisations are liberated from data dependency on foreign entities and can avoid international borders and foreign jurisdiction concerns.

 Global Reach, Local Control: The platform is designed to be entirely deployed and contained within any in-country instance of AWS whilst still benefiting from real-time telemetry delivered by

the CrowdStrike Falcon platform.

 Reduced Latency: Leveraging local AWS instances ensures swift threat detection, incident response, and data analysis, bolstering overall security posture.

“Our core mission at CrowdStrike is stopping breaches, which aligns with Sekuro’s dedication to assist organisations of all sizes to improve cybersecurity,” said Michael Sentonas, President at CrowdStrike. “With Falcon LogScale powering Sekuro’s adaptive security platform, we’re providing industry leading technology to advance our shared objectives while allowing customers to gain greater control over their data.”

“As leaders and architects of cyber resilience,” commented Noel Allnutt, CEO of Sekuro, “we take immense pride in crafting a solution accessible to all organisations, regardless of their inhouse capabilities. Our holistic approach to Managed XDR closes visibility gaps for security teams managing operations across hybrid environments, detecting, investigating and responding to threats across all attack vectors.”

“We've woven People, Process, and Technology into a single turn-key system that delivers immediate, measurable organisational outcomes that even a CFO can get behind. We've reduced Mean Time to Acknowledge, Notify, and Respond by up to 95%, whilst increasing threat detection coverage by 10x over the same period. Lowering TCO whilst boosting security capabilities? Technology sufficiently advanced is indistinguishable from magic,” stated Downes.

###

About Sekuro
Sekuro is a cyber security and digital resiliency solutions provider that helps CIOs and CISOs take a strategic approach to cyber security risk mitigation and digital transformation. Operating at the intersection of the digital technologies and cyber security industries, Sekuro reduces cyber risk while new technologies are adopted - ultimately building business resiliency and enabling fearless innovation.

Our six practice areas (Strategy and Architecture, Governance, Risk and Compliance, Technology and Platforms, Offensive Security, Managed Security Services and People and Program Enablement) are full of the brightest minds in the industry. They work together to look beyond the threat landscape of today and into an opportunity landscape of tomorrow.

Learn more at sekuro.io.
About CrowdStrike
CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.
Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform

leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.
CrowdStrike: We stop breaches.
Learn more: https://www.crowdstrike.com/

Katherine Chong
Sekuro
+61 1800 735 876
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
YouTube
