



Case Study

Provintell

**PROVINTELL Partners with an Open and Unifying SecOps Platform to Deliver External Attack Surface Monitoring, Continuous Threat Hunting, and Intrusion Monitoring Services**



We choose the open and unifying SecOps platform as our main data collection and processing platform for many practical reasons to support our mission in combating dynamic and sophisticated cyber threats 24x7.



— Nicholas Ng, PROVINTELL CEO

## Before



### Licensing

Since cyber defense is getting harder and more expensive for many start-up organizations and SMBs, the unified platform allows PROVINTELL to scale its business more efficiently to cater to various customer requirements while ensuring cost-effectiveness regardless of customer size.



### Fast Customer Onboarding

The open and unifying SecOps platform enables easy integration of other security, IT, and productivity tools, simplifying and reducing the processes and time needed for customer onboarding.



### Unified

A single license enables the platform's NG-SIEM, NDR, IDS, UEBA, and SOAR capabilities, eliminating complexity.

## With the Open and Unifying SecOps Platform



### Training and eLearning

The platform provider invested time and effort to ensure PROVINTELL's technical operations teams mastered the unified platform via various product training and certification tracks. In addition, the provider also offers an eLearning platform for PROVINTELL and their customers, saving time and money for continuous improvement of skill sets.



### Incident Triaging

Multi-Layer AI™ evaluates and groups related alerts automatically and helps operation teams reduce their mean time to respond (MTTR) based on threat fidelity and severity scores, minimizing the risk of human error in threat analysis.



### Visibility and Telemetry

The unified operational view of threats impacting customers eliminated blind spots that previously existed, enabling faster detection across environments.

## What Changed

PROVINTELL is an emerging Managed Security Service Provider (MSSP) and Cybersecurity-as-a-Service (CSaaS) provider in the region specializing in Next-Gen Cyber Defense and Response. It now leverages the open and unifying SecOps platform to hunt, detect, and respond to threats in the most complex environments

PROVINTELL's 24x7 Next-Gen CyberSOC is fully managed by in-house certified cybersecurity specialists highly skilled in threat hunting, incident response, red teaming, and penetration testing. They employ 'Threat Intelligence as First Line of Defense' by continuously assessing the attack surface, data breaches, and exposure risk for customers to enhance their CyberSOC capabilities in orchestrating the most effective cyber defense and response strategies against sophisticated threats.

To maintain a competitive advantage, MSSPs must adopt innovative ways to deliver better security services to customers. PROVINTELL requires a solution that can:

- Break down current silos between security products.
- Automate previously manual tasks associated with threat detection and response to improve mean time to respond.
- Utilize **Multi-Layer AI™** to complement human limitations in threat hunting for external and internal threats, requiring mass and complex data processing.
- Allow the company to support customers of different sizes in multifaceted environments in a scalable manner.



**Being a prominent MSSP in delivering Next Generation Cyber Defense and Response services, we emphasize our data collection and processing capabilities from anywhere and everything. With our technical R&D expertise in threat intelligence and attack surface management technology, we are collaborating to enhance the platform's data collection continuously and its Multi-Layer AI™ capabilities for mass and complex data processing.**

— Nicholas Ng, PROVINTELL CEO



## How the Platform Works

The open and **unifying SecOps platform** automatically normalizes and enriches data from every sensor and security tool upon ingestion. Then, **Multi-Layer AI™** engines automatically evaluate and group related alerts and identify new threats based on abnormal user and asset behaviors, producing a **prioritized list of contextual incidents on the platform's intuitive dashboard**.

With the unified platform, PROVINTELL delivers better customer experiences, improves its ability to support customers of different sizes, and simultaneously enhances business profitability.

## About Stellar Cyber

**Stellar Cyber's open and unifying SecOps platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments.**

With Stellar Cyber, organizations move from manual, alert-driven operations to a human-augmented autonomous SOC that identifies, validates, and responds to risk with speed and precision. Customers reduce false positives by more than 80%, improve analyst productivity, and lower operational costs—while retaining existing security investments and gaining measurable improvements in risk reduction and response consistency. The company is based in Silicon Valley.

---

stellarcyber.ai  
sales@stellarcyber.ai

