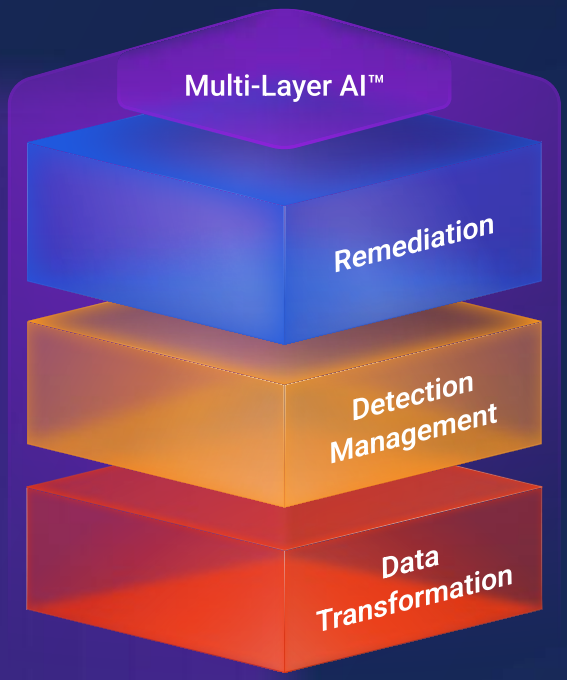
STELLAR CYBER®



Case Study

BLACKSWAN CYBERSECURITY

Blackswan Cybersecurity Adds an Open and Unifying SecOps Platform as a Strategic Partner in Its Fight Against Cyber Threats

Overview

After extensive research, product testing, and critical evaluation by their technical teams, Blackswan chose an open and unifying SecOps platform to expand its MDR capabilities and spearhead its critical breach response protocol due to its quick deployment, multi-environment usability, and adaptability.

Before

Time-Consuming Deployment

The legacy platform could not be used for incident response. Blackswan relied on partners to deploy their technologies to obtain visibility and actionable response capabilities.

Limited Availability of Integrations

Blackswan's legacy platform offered limited integrations to third-party products and slow response times, making it costly, unreliable, and restrictive when trying to onboard specific clients.

Lack of MSSP Focus

The legacy tool was not explicitly designed for MSSPs, meaning the flexibility/adaptability Blackswan needed was missing or only partially available.

With the Open and Unifying SecOps Platform

Fast Deployment

With close client coordination, Blackswan can deploy the platform within the critical first day of an incident.

Hundreds of Integrations Available Out-of-the-Box

Blackswan's IR team can now quickly connect to almost any data source to build effective visibility into the client's environment.

MSSP Expertise In-House

The extensive catalog of integrations and responsiveness to platform engineering and integration requests allows Blackswan to deploy new customers faster than ever before.

Blackswan Cybersecurity is a leader in fit-for-purpose cybersecurity solutions delivering risk identification, mitigation, and remediation services. Blackswan's Cyber Fusion Center (CFC) provides:

- Multiple full-scale cybersecurity disciplines under one roof.
- Access to real-time dashboards, reporting, and cybersecurity experts around the clock (24/7/365).
- Continuous, US-based, eyes-on-glass monitoring, detection, and response.

Blackswan helps companies identify proper safeguards to protect their data assets and outperform cybersecurity compliance requirements by offering a customizable, comprehensive suite of services.

These services range from comprehensive 24/7/365 managed security services (SOC-as-a-service), gap analysis, vulnerability identification and remediation, incident and breach response, user awareness training, GRC assessments and analysis, and virtual CISO services.

As part of ongoing continuous improvement initiatives, Blackswan evaluated multiple alternative security monitoring solutions that might improve its ability to service clients.

Over several months, the Cyber Fusion Center team identified this platform as part of a shortlist of solution providers that might meet their needs. Blackswan engaged in a proof of concept. To begin, the platform provider gave Blackswan an environment to evaluate, where engineers and analysts ran several threat scenarios testing alerting capabilities, console and user interface, and integration capability evaluations.

After completing the proof of concept, Blackswan valued that the provider is wholly US-based and US-supported, and that the leadership team proved responsive, collaborative, and innovative.

> **We needed a partner that could provide quick deployment, integration with multiple devices, be MSSP focused, and deliver top-tier support. That partner is the open and unifying SecOps platform.**
>
> — Dr. Mike Saylor, CEO, Blackswan Cybersecurity

How the Platform Works

The unified 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. Using pre-defined or ad-hoc playbooks, security analysts can complete investigations and take remediation actions that eliminate the threats.

> **After integration with the client's major data sources, we narrowed down the infected servers and endpoints to have them remediated and identify the root cause of the infection. The open and unifying SecOps platform made this swift response possible.**
>
> — Dr. Mike Saylor, CEO, Blackswan Cybersecurity

The Results

The platform's practicality and adaptability enabled Blackswan to react quickly during crises. For example, when a government agency notified a Blackswan client that file signatures related to ransomware were detected in their environment, Blackswan took decisive action. Blackswan rapidly stood up platform sensors in the client's environment to begin data ingestion and signature review. This response allowed the client and Blackswan's Cyber Fusion Center to view the environment within a matter of hours.

Blackswan plans to continue to grow its security service offerings, taking advantage of the hundreds of pre-built integrations available. This approach empowers the Cyber Fusion Center to be effective and timely in providing its 24×7 monitored detection and response services.

The platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill level to successfully secure their environments. With the platform, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity — delivering an 8× improvement in mean time to detect (MTTD) and a 20× improvement in mean time to remediate (MTTR).

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

STELLAR CYBER®