BATTLECARD

Blackswan's OpenXDR vs. LogRhythm

Blackswan's OpenXDR platform (Stellar Cyber) delivers critical advantages over the suite of LogRhythm products, such as physical and virtual sensors to collect telemetry across the entire IT and OT environments, embedded UEBA capabilities, and automated correlations. The platform's single license for everything makes it a proven choice for enterprises of all sizes.

One Partner » One Phone Call » One Solution

855.BLK.SWAN (855-255-7926)

BLACKSWAN CYBERSECURITY

Overview

"Blackswan's Stellar Cyber platform helped close our visibility gap as no other solutions could. As a result, it has become indispensable to our organization, allowing us to act on potential threats immediately."

Amanda Stowell, Information Security & Privacy Analyst A-Dec

How Blackswan Beats LogRhythm

- **Physical and Virtual Sensors –** Stellar Cyber enables organizations to push their security capabilities to the edge of their networks, decreasing MTTD and MTTR via physical and virtual sensors to collect and process data wherever it resides.
- **Embedded UEBA Capabilities:** Organizations get critical user and entity behavior visibility across their environment at no extra charge.
- **Automated Correlations –** Using purpose-built deep learning (ML) models and curated correlation rules, Stellar Cyber automatically correlates related alerts and logs to generate investigation-ready incidents driving a significant increase in security analyst productivity.
- **Single Licensing –** The platform includes all features and functionality under a single license with no hidden fees or surprise upgrade-charges making budgeting easy for security decision-makers.
- **Modern Detections –**Stellar Cyber is committed to solving the alert fatigue problem by delivering automated correlations, purpose-built machine learning, and curated threat detection rules all in one platform.
- **All-In Partnership –** Blackswan is committed to working with every customer to get the security outcomes they need from day one.

What Our Customers Say

"I've worked with several MSSPs over my career and Blackswan Cybersecurity stands out as one of the best and most collaborative service providers I've ever worked with. Soon after deploying the Stellar Cyber OpenXDR platform, we saw threats that the previous security providers missed. Together with Blackswan, we were able to investigate and remediate the threats quickly and effectively."

- Financial Services SOC Manager

"...our cybersecurity posture was significantly improved with the addition of Blackswan's services and the Stellar platform. Additionally, we were also impressed with the cost savings, scalability, and flexibility we've seen from Blackswan."

- Manufacturing Security Leader

Comparison

Customers switching from LogRhythm to Stellar Cyber found easier implementation, superior support, and efficacy gains from automated correlation. Additionally, Stellar Cyber's single license for all features is preferred over the the add-on LogRhythm licensing approach.

Positioning Point	Stellar Cyber	LogRhythm
Architecture		
Multi-Level, Multi-Tenancy with RBAC	✓	X No multi-tenancy
Tenant Onboarding	✓ Immediate, self-service	X Months before full deployment achieved
Sensors & NDR	✓ NDR, IDS, Sandbox, DPI	✓ NDR capabilities via acquisition
Automated Response	✓ Bi-directional integrations with SOAR functionality	✓ Included
Integration Suite	✓ Hundreds of integrations	✓ Hundreds of integrations
API	✓ Fully featured public API	✓
Detections & Security		
Modern Slate of Detection Capabilities	✓ ML and Rule based detections	✓ Some ML but heavily reliant on human created correlation rules
Automated Correlation	✓	✓
Analyst Experience	✓ Case Management, Reporting, Threat Hunting	✓
Partnership		
Single License	✓ NDR, Open XDR, NG-SIEM, TIP, UEBA, SOAR under single license	X Some capabilities, such as UEBA, requires add-in licenses
Feature Development	✓ Highly responsive, included in license	X Slower moving development
Technical Enablement	✓ 4 week enablement at NO cost to expedite deployment	X Deployment and training not included
Customer Support	✓ Global, in house team, strict SLAs	✓
Sales Enablement	✓ Dedicated program for MSSPs	✓

Deep Dive

LogRhythm

LogRhythm benefited from multiple years in the leaders quadrant of the Gartner SIEM MQ, however as they are now in the challengers quadrant due to lack of innovation they are attempting to reshape their offering, with mixed results.

LogRhythm is a 20-year-old SIEM security vendor. Fundamentally, LogRhythm is a rule-focused SIEM requiring constant maintenance to ensure detections are relevant. For the last 4 years since 2019, they continuously moved in the wrong direction in Gartner's Magic Quadrant for SIEMs and finally in 2022, they moved from the leader's to the challenger's quadrant. Not coincidentally, LogRhythm had significant challenges to migrate their on-prem solution to a SaaS solution in the last several years, which was also mentioned by Gartner in the last two years. It eventually launched Axon in 2022, the company's first foray into delivering a cloud-based SIEM solution. As its initial release, it had lots of deficiency as a cloud native SaaS platform. As a result, most of their customers have yet to transition from their on-premises solution to Axon, presenting an opportunity for organizations to consider replacing their LogRhythm deployment altogether.

The security industry has observed a lack of innovation from LogRhythm and the lost market share over the past several years. Additionally, their SIEM, NDR, and UEBA (cloud only) are all separate products with separate licenses, and/or different consoles.

Challenges

- No multi-tenancy
- No modern detection techniques, customers complain of manual analysis and painful maintenance of rules
- Cloud is new and lacking capabilities, in some cases, with different consoles
- Lack of partnership and good support
- Slow innovation

The Blackswan and Stellar Advantage

- **Native NDR & Sensors –** Stellar Cyber enables organizations to push their security capabilities to the edge of their networks, decreasing MTTD and MTTR via physical and virtual sensors and its native NDR capabilities.
- **Multi-Tier Architecture –** For Enterprises with segmented environments, the Stellar Cyber architecture ensures individual customers/entity data integrity.
- **Automated Correlation –** Using purpose-built deep learning(ML)models and curated correlation rules, Stellar Cyber automatically correlates related alerts and logs to generate investigation-ready incidents driving a significant increase in security analyst productivity.
- **Simple No Surprises Licensing –** Stellar Cyber sells all features and functionality under a single license with no hidden fees or surprise upgrade charges making budgeting easy for security decision-makers.
- **All-In Partnership –** Blackswan is committed to working with every customer to get the security outcomes they need throughout the relationship.
- **Rapid Deployment Capabilities –** Blackswan can deploy the Stellar Cyber platform in as quickly as one day. If your technology teams are available to support the deployment of on-premise virtual machines, firewall changes, and API authentications – Blackswan could be monitoring and protecting your environment before the end of day one.