Avertium & LogRhythm

EXTENDED DETECTION & RESPONSE

AVERTIUM

www.avertium.com

877-707-7997

Company Overview

We are the cybersecurity services provider that companies turn to when they want more than standard security services. Everyday, Avertium security experts rise to meet clients' not-so-standard business requirements, technology environments, processes and policies with a show-no-weakness approach to cybersecurity.

Unique Value Proposition

Comprehensive end-to-end coverage through advanced certified LogRhythm expertise and the rigorous Avertium Engagement Methodology.

By the Numbers

- ☑ 120+ Certifications
- ☑ Fully-redundant 24/7/365 dual security operations centers
- ☑ 400,000:1 Event to Alert Ratio
- ☑ 540,000+ devices under management

The Avertium show-no-weakness approach to implementing, managing and customizing LogRhythm's NextGen SIEM Platform ensures faster time to deployment and ROI. As a **Service Authorized Partner**, Avertium experts partner with you to develop custom correlation and LogRhythm SmartResponse™ rules tailored to your environment.

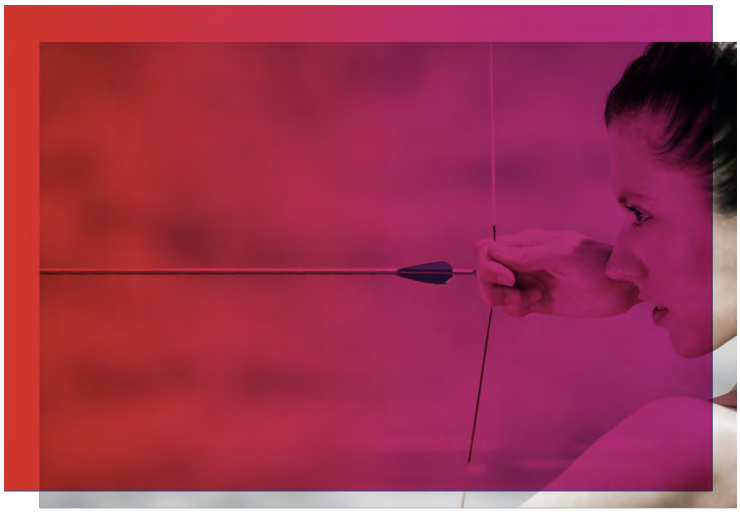
AVERTIUM BENEFITS

- XDR capabilities to **rapidly detect** threats across attack vectors with our proprietary use cases and escalation techniques, all mapped to the industry standard MITRE ATT&CK framework
- **Achieve visibility** into your environment with our expertise integrating data across data sources including on-premise, cloud, SaaS, IaaS, PaaS, network, endpoints, etc.
- **Power up** advanced threat correlation capabilities by adding Avertium's Threat Intelligence feeds to your LogRhythm implementation
- Dedicated **Technical Account Manager**
- **More relevant alerts** at a 400,000 to 1 event to alert ratio with our proprietary security operations orchestration and workflow platform, OmniQueue.

AVERTIUM ADVANTAGE

The rigorous **Avertium Engagement Methodology** combines a strategic approach using industry-leading NIST CSF with a tactical approach using the MITRE ATT&CK framework to assess your security program's maturity, assign a score and develop corresponding action steps prioritized to your objectives, risk threshold and resources.

> "With the information [from Avertium], we were able to go through our vulnerability data and located several machines with one of the vulnerabilities, but more importantly we identified a single laptop with both vulnerabilities...Finding the perfect storm on a single device out of thousands proactively is an excellent success story."



Information Security Analyst, **Avertium/LogRhythm Joint Customer**

USE CASE	AVERTIUM
Company outgrows their existing SIEM and selects LogRhythm for its modern capabilities. The high demand for LogRhythm certified experts, a tight implementation timeframe along with the need for 24/7/365 monitoring, detection and response leads the company to seek external resources.	With experience migrating a variety of SIEM technologies to LogRhythm, we offer customers shorter deployment times. Our expertise integrating data across critical data sources including on-premise and cloud environments, SaaS, IaaS, PaaS, network, endpoints, etc., ensures better visibility into the customer's environment.
Company seeks an MSSP with expertise in optimizing and tuning the LogRhythm platform to fully leverage its advanced capabilities while also possessing the experience in incident response.	Avertium is a LogRhythm Service Authorized Partner with expertise developing custom SmartResponse rules. We leverage this along with our proprietary playbooks and escalation techniques to ensure clients maximize their investment while improving threat detection and response.
Company seeks an MSSP with LogRhythm expertise and that also provides additional cybersecurity consulting and compliance assessment services.	Avertium not only offers certified LogRhythm expertise leveraging our turnkey managed security environment, our professional services team has domain expertise in the full continuum of cybersecurity consulting, from assessments to compliance, and incident response planning and digital forensics to virtual CISO services.

THE AVERTIUM MANAGED SECURITY SOLUTION

The award-winning **Avertium** managed security solution combines best-in-class technologies managed by Avertium's certified CyberOps team for 24/7/365 monitoring, detection and response. The turnkey service encapsulates XDR capabilities and provides coverage across your networks, servers, email, endpoints, and cloud environments to provide visibility and context in the identification and handling of cyber threats wherever your data may flow.

Our proprietary security operations orchestration and workflow platform, OmniQueue, ensures more responsiveness and more relevance in our CyberOps Centers of Excellence consistently delivering a **400,000 to 1** event to alert ratio.

avertium.com | 877-707-7997