AVERTIUM

AVERTIUM SOLUTIONS FOR MICROSOFT SECURITY

MANAGED SIEM FOR MICROSOFT SENTINEL

CUT THROUGH THE NOISE

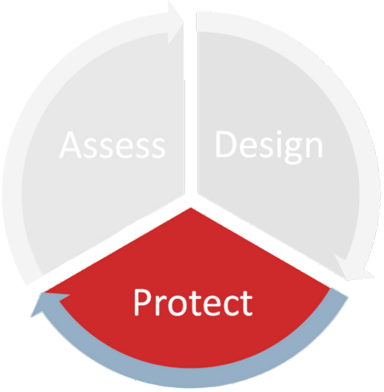
Avertium can help you maximize your Microsoft Security investment. We are an extension of your team, helping you both design your Microsoft Security strategy and put it into action. Our **Assess - Design - Protect** approach makes you more secure, compliant, and efficient.

- ✓ **5 STARS, 100% RECOMMENDED:** Gartner Peer Insights Rating.
- ✓ **FUSION ENGINE:** Threat Intelligence integrated with Microsoft Sentinel and response playbooks.
- ✓ **COMPREHENSIVE MICROSOFT XDR PROTECTION:** Identity, O365, Cloud Apps, and Endpoint

Avertium combines a fusion-first approach with Microsoft Sentinel to **PROTECT** your security operations.

Designed for companies in the Healthcare, Manufacturing, Retail, and Financial industries with less than 3,500 employees and limited security resources. Our proprietary threat detection rulesets and data correlation result in actionable and meaningful alerts.

A well-tuned Microsoft Sentinel cuts through the noise of other SIEM platforms by enabling rapid identification of threats, enabling sound monitoring, analysis, and prioritization of response to suspected security issues.



PROTECT

v /prəˈtekt/
24/7/365 fused defense operations with Microsoft Sentinel that are continually improved by technology integrations, proactive threat identification, tuning, and testing.

When you combine Microsoft Sentinel and the strength of Avertium's highly trained Cyber Fusion Center (CFC) teams, you can attack the chaos of SIEM alerts with context. Our team of expert analysts continuously tune Microsoft Sentinel to eliminate false alarms, enable rapid identification of emergent threats, and align with your organization's unique threat landscape.

APPROACH

FUSION ENGINE INTEGRATION

- Cyber fusion telemetry between Microsoft Sentinel and your other defense operations
- Advanced threat detection and reoccurring detection-as-code-releases
- Threats flow from Sentinel to Fusion Engine, correlating threats with our Threat Intelligence Platform

RESPONSE

- Fully managed Microsoft Sentinel
- 24/7/365 monitoring, alerting, human response
- Platform health checks, updates, patches
- Ongoing tuning

ACCOUNT TEAM

- Dedicated Project Manager
- Service Delivery Manager
- Threat Response Team

REPORTING

- Weekly, month, quarterly, and annual reporting
- Leverage Fusion Engine to aggregate + relevant threats into a single feed
- Zero-Day vulnerability Flash Notices
- Threat Intelligence Reports

THREAT EXPOSURE

- Map rules to Microsoft Sentinel MITRE ATT&CK® framework analytics
- Tailored threat intelligence
- Security incident reports
- SME support for remediation efforts & actions

CAPABILITIES

- Compliant and threat-informed SIEM configured with collectors for log correlation
- Detection, severity triage, and human response to Indicators of Compromise (IoCs)
- Reduced Total Cost of Ownership (TOC)
- Greater incident fidelity: reducing noise to isolate true positive alerts
- Fully configured rules, log sources, workflows, and baselines
- Ongoing threat advisories and IoCs
- Threat-informed automated and tailored response

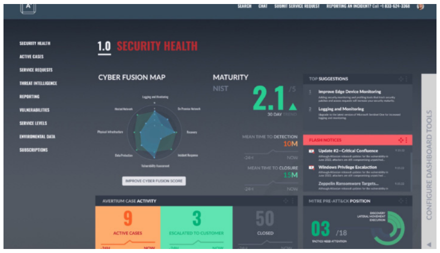
Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Threat Protection

Member of
Microsoft Intelligent Security Association
Microsoft

AVERTIUM CONNECTOR FOR MICROSOFT SENTINEL

Avertium Connector for Microsoft Sentinel correlates our proprietary threat intelligence with your Microsoft Sentinel platform to improve detection and hunting capabilities. This advanced layer of threat intel telemetry enables Avertium's CFCs to review all alerts, remove false positives & noise, and respond to real threats.



OUTCOMES

Avertium's Cyber Fusion teams act as an extension of your internal teams, enabling you to get more from Microsoft Sentinel.

MORE SECURE

Drive greater incident fidelity while reducing false alarms through continuous tuning. Avertium's team takes a cyber fusion-first approach, offering advanced threat detection 24/7/365.

MORE COMPLIANT

Avertium's threat-informed, compliance-first approach to Microsoft Sentinel management helps you lay the groundwork for meeting compliance mandates.

MORE RETURN ON INVESTMENT

Get a team that configures, optimizes, deploys, manages, and maintains Microsoft Sentinel in a way that aligns with your business, drives efficiency within your teams, and reduces the total cost of ownership.

ABOUT AVERTIUM

Avertium is a cyber fusion company with a programmatic approach to measurable cyber maturity outcomes. Organizations turn to Avertium for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive approach to cybersecurity. That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**