Trustwave® | Microsoft Azure

Trustwave Co-Managed SOC Services for Microsoft Azure Sentinel

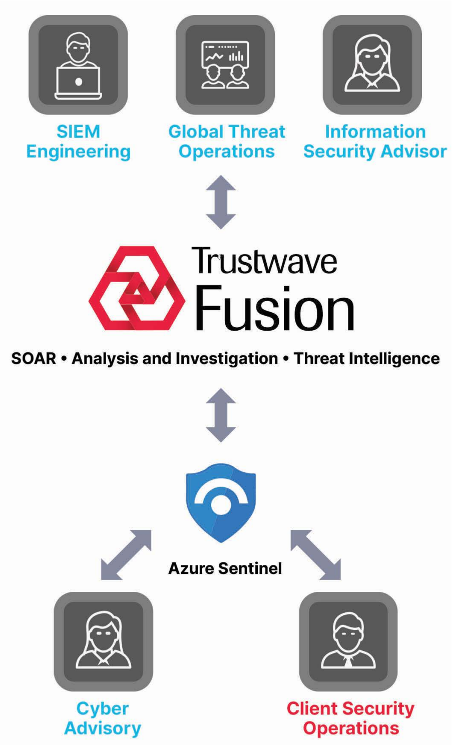
OPTIMIZE YOUR SOC WITH TRUSTWAVE THREAT INTELLIGENCE AND EXPERTISE

Benefits

- Extend your team with elite cybersecurity expertise
- Strengthen your security posture
- Recognize value on your existing Microsoft Azure Sentinel investment
- Flexible management options
- Industry-leading cyberthreat intelligence from Trustwave SpiderLabs
- Get more insight and context from Azure Sentinel alerts

Analyzing and correlating log and event information coming from devices and solutions in your Security Operations Center (SOC) can be complicated and time-consuming for any organization. As a leader in managed detection and response and one of Microsoft's first Managed Security Services Provider (MSSP) partners for Microsoft Azure Sentinel, Trustwave can help you co-manage your Azure Sentinel SIEM and security operations.

We can help you expedite Sentinel deployment and provide expert resources to accelerate detection, respond quicker and adapt sooner to security threats.


SIEM Engineering
Global Threat Operations
Information Security Advisor
Trustwave Fusion
SOAR • Analysis and Investigation • Threat Intelligence
Azure Sentinel
Cyber Advisory
Client Security Operations

World Class People and Processes

Expertise matters when it comes to evaluating threats and findings, making decisions, performing investigations, and performing consistently for a predictable service outcome. Armed with hundreds of annual training hours and seasoned by hundreds of thousands of monthly investigations, our skilled security practitioners understand the threats and help you make fast, accurate decisions on actions to mitigate or remediate threats.

Our investigators and analysts have immediate access to the renowned global Trustwave SpiderLabs team for further context and research on potential threats, indicators of compromise, malware and up-to-the-minute threat intelligence to improve your security outcomes.

What We Offer

Trustwave offers **Co-Managed Security Operations Center (SOC) Services** which integrate with Microsoft Azure Sentinel to extend your team's capacity. Services include:

- **SIEM Jumpstart:** Transitional project consulting and provisioning to plan, build and/or optimize threat detection and response solutions to steady state.
- **Threat Detection & Response:** 24×7 threat monitoring, human-led investigation and notification by analysts in the nine global Trustwave SOCs.
- **SIEM Management:** Maintenance, tuning and use case implementation.
- **Information Security Advisor (ISA):** Ongoing management and maintenance of the Co-Managed SOC environment, guidance in maturing system and process capabilities.
- **Threat Detection & Response (TDR) Agility Program (Optional):** Program whereby you have full access to the entire SOC consulting and engineering skills and experience.

How We Do It

- Plan, build and/or optimize threat detection and response use cases
- Microsoft Azure Sentinel is used to collect, normalize, store and analyze logs and events, producing alerts based on your pre-defined use cases. Trustwave Fusion, our extended detection and response (XDR) platform, leverages cloud-based integrations to Azure Sentinel and other infrastructure including clouds and networks. The Trustwave Fusion platform monitors and escalates incidents to security analysts, who triage and investigate threats, enrich using threat intelligence feeds and investigate on your Azure Sentinel instance. This rich telemetry enables you to receive more value from your existing security tools and empowers Trustwave Security Analysts who leverage unique SpiderLabs threat intelligence to enrich data during investigations on your behalf.

About Trustwave SpiderLabs:

Trustwave SpiderLabs is a world-renowned team of security researchers, ethical hackers, forensics investigators and responders specialized in research, threat hunting, response, forensics, and reverse engineering. The team includes cyber threat analysts from law enforcement and military backgrounds with expertise tracking nation-state and professional criminal threat actor’s offensive campaigns. Trustwave SpiderLabs conducts hundreds of deep investigations and thousands of penetration tests for companies and organizations each year.

About Trustwave:

Trustwave is recognized as a global security leader in managed security services (MSS) and managed detection and response (MDR). With more than 2,000 world-class security professionals operating on behalf of clients across 96 countries, Trustwave helps organizations across the globe detect and respond to threats in the hybrid multi-cloud world. The elite Trustwave SpiderLabs team provides award-winning threat research and intelligence, which is infused into Trustwave services and products to fortify cyber resilience in the age of advanced threats. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS.

Member of
Microsoft Intelligent
Security Association

Microsoft

Trustwave®

www.trustwave.com