protiviti®

Face the Future with Confidence

Microsoft Azure Sentinel: Managed Security Operations

End-to-End Security Monitoring with Microsoft Azure Sentinel

Monitoring and alerting for attackers requires a clear understanding of an organization's most important assets. But without a clear understanding of what data needs to be logged and monitored, companies quickly discover too much data within a security operations center creates broken processes and unsustainable operations.

Protiviti's Managed Security Operations services deliver security monitoring on a global scale with Microsoft Azure Sentinel, Microsoft cloud-native SIEM and SOAR . Our services give organizations scalable, secure Microsoft cloud management, advanced threat detection, and real-time security monitoring services. Our team builds and operates secure and high-performing Microsoft cloud infrastructures combining all flavors of on-prem, SaaS, PaaS, IaaS and FaaS while connected to customers and workers alike across dedicated mobile and personal devices.

17-Time

Microsoft Gold Partner

Client Problems We Solve

- Inefficient operation processes, staff or technology to centralize the monitoring and remediation of security issues across the organization
- Unsustainable monitoring practices with increasing costs
- Keeping security operations centers current as systems and assets are commissioned or decommissioned
- Maintaining adequately trained operations staff
- Lack of unified monitoring and governance framework
- Limited attack surface monitoring for threats and data leakage
- Too many security technologies to manage with limited options

Business Outcomes

- Next generation Security Operations with Cloud and Artificial Intelligence
- Clients move immediately from no monitoring to real-time visibility
- A cost-effective, cloud-native solution with predictable billing and flexible commitments
- Scalable teams and solutions to protect the most valuable data assets while eliminating noise
- Improved security incident detection, monitoring and remediation through continuous analysis

INNOVATE. TRANSFORM. SUCCEED.

Microsoft Security Operations Center Services

Cloud Integration

- Cloud maturity and readiness assessment: Azure Sentinel implementation roadmap
- Cloud governance: governance structure to guide application services deployed onto the cloud in a risk-sensitive, secure, economical, and compliant manner
- Security gap assessment
- Integration of legacy systems to enable a hybrid environment

Cybersecurity Intelligence Response Center (CIRC)

- Enhanced "white glove" Cybersecurity AAS solution
- Incident triage and containment via Azure Sentinel hunting queries
- Collect and analyze digital evidence
- Ongoing probabilistic cyber risk quantification

Active Security Assessment

- Infrastructure/Application/Network Assessment: Leveraging Azure Sentinel to test IT infrastructure vulnerabilities
- Executed by probing systems with bespoke simulations designed to refine understanding of vulnerabilities and deploy mitigating measures
- Monitoring of intelligence sources (i.e., Security forums, dark web channels) for new and novel cyber threat methods

Incident Response & Forensics Services

- Pre-incident activities: Incident Response Plan (IRP) Development and Tabletop Exercise (TTX); Cyber Threat Hunting/ Breach Assessment
- Customization of threat rule template.
- AAS enhanced forensic and incident response capability via rapid alert and automated playbook updates
- Forensic E-discovery support

Client Success Story

Client Challenge: A client was implementing an on-premise security operations center (SOC) and was challenged with selecting the right tools to monitor security activity, while also designing the security center structure and determining its monitoring and escalation procedures.

Solution Delivered: Protiviti scoped the critical data, assets and requirements for building a security operations center; performed solution selection and implementation including building out space for the SOC; reviewed existing staff and capabilities within the environment, and qualified and trained them to run the SOC.

Value & Results: Understanding of SOC implementation requirements. Centralized security monitoring capabilities. Established continuous monitoring program with regular health checks and improvement.

Gold
Microsoft Partner
Microsoft

Protiviti.com/Microsoft

MicrosoftSolutions@Protiviti.com

TCblog.Protiviti.com

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85 locations in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Face the Future with Confidence