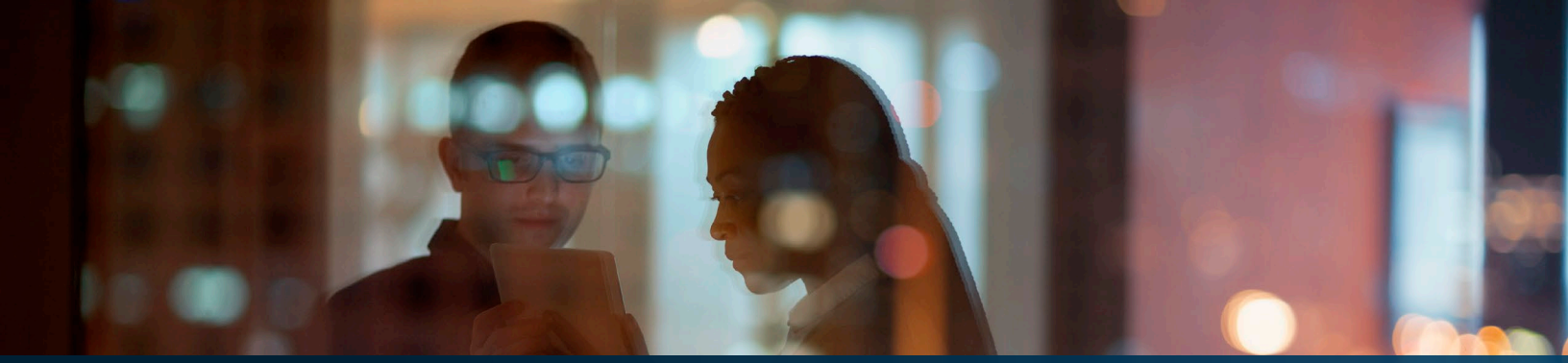

Managed Security Services and Security Operations

Cyber Defense Hub

protiviti®
Global Business Consulting

Organizations today face a hostile cyber landscape, necessitating around-the-clock monitoring and immediate response to potential security incidents. However, managing this is resource-intensive, costly and beyond the capabilities that many organizations can accommodate. Compliance with evolving regulatory requirements for data protection and privacy present additional complexities. Cybersecurity leaders are challenged to identify an operating model that provides adequate expertise, continuous surveillance, and compliance management.

Enabling complete visibility for reduced risk

Monitoring and alerting for attackers requires a clear understanding of an organization's most important assets. Without a clear understanding of the data that needs to be logged and monitored, companies quickly discover too much data within a Security Operation Center (SOC) leads to broken processes and unsustainable operations. Protiviti enables companies to see and reduce risk, by partnering with them to answer the following questions:

- How can the organization identifying threats proactively and respond swiftly and with minimal disruption?
- Which security and privacy standards must the organization meet?
- Malicious actors are constantly refining their tactics, techniques and procedures to evade organizational defenses… what can be done to ensure my organization is adapting quickly?
- With bad actors operating around the clock, but a growing talent shortage, is continuous monitoring possible?

Business outcomes of our solutions

- Enhanced protection from our SaaS, PaaS, and IaaS, and FaaS services
- Better monitoring of security anomalies and use of unauthorized services
- Data security through data-centric policies
- Enhanced threat protection through content and context-based policies
- Improved operations through technology integration

Protiviti's experts deliver security monitoring on a global scale with Microsoft Sentinel. Our services offer scalable, secure cloud management, advanced threat detection, and real-time security monitoring services. Protiviti builds and operates secure cloud infrastructures combining all flavors of on-prem, SaaS, PaaS, IaaS, and FaaS .

Core components of Protiviti's Cyber Defense Hub:

Threat Monitoring and Response

Constant review of activity across the organization's network is needed to manage threats and identify risks, playing a pivotal role in preventing threats. While not every situation can be predicted or prevented, the Cyber Defense Hub responds quickly when incidents occur to mitigate the threat with minimal disruption to the organization's operations.

Compliance Management

Which regulatory standards must your organization meet? Organizations align to and protect themselves through external security standards such as ISO 27001x, the General Data Protection Regulations (GDPR), and the NIST Cybersecurity Framework (CSF). Protiviti assists in ensuring that our clients meet requirements of key best practices and security standards.

Security Process Improvement

Malicious actors are constantly refining their tactics, techniques and procedures to evade organizational defenses. Improvements must be made on an ongoing basis that benefit the organizational clients. Our approach involves performing after action reporting/post-mortem investigations of incidents to identify areas of improvement for organizational security processes.

Continuous Monitoring

Organizations require the ability to observe anomalous behaviors at all layers of their network, and an operations center that monitor 24/7 can enable this support. The SOC serves as a dedicated space that can be staffed in shifts round-the-clock to provide consistent monitoring and crisis response, ensuring swift action if, and when critical events occur.

How Protiviti can help:

Protiviti's managed security solutions team delivers the following offerings:

- 24x7x365 Security Monitoring from onshore and offshore
- Threat detection and containment
- Automated system health monitoring
- Threat response and incident containment
- Tuning of the environment to ensure the highest fidelity coverages are deployed within Microsoft Sentinel
- Enhanced visibility into threat activity utilizing threat intelligence and customized hunt campaigns
- Investigations across disparate technologies
- Detailed containment automation
- Customized runbooks
- Dedicated response that reduces mean times to detect and resolve

Leveraging Microsoft Sentinel to elevate your security posture

Protiviti's Cyber Defense Hub delivers security monitoring on a global scale with Microsoft Sentinel, a cloud-native platform. Our experts provide organizations with scalable, secure real-time security monitoring and advanced threat detection.

Microsoft Solutions Partner
Microsoft Cloud

Ready to transform your business?

Let's create a tailored strategy for your success.

LEARN MORE
Protiviti.com

Protiviti is a global business consulting firm and a wholly owned subsidiary of Robert Half, that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Together, Robert Half and Protiviti provide an unmatched range of professional services from consulting and project implementation to managed services and staff augmentation.

protiviti®
Global Business Consulting