protiviti®
Global Business Consulting

Cyber Defense Hub

Prepare, Prevent, Protect

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's Cyber Defense Hub experts deliver security monitoring on a global scale with Microsoft Sentinel. Our services give organizations scalable, secure Microsoft cloud management, advanced threat detection, and real-time security monitoring services. Protiviti 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.

Enabling complete visibility for reduced risk

Microsoft Solutions Partner
Security

Key Themes of the Cyber Defense Hub

Proactive Threat Monitoring and Response

SOC analysts consistently review activity across the organization's network to manage threats and identify possible risks, playing a pivotal role in preventing threats. While not every situation can be predicted or prevented, the SOC enables an organization to respond quickly when incidents occur to mitigate the threat with minimal disruption to the organization's operations.

Compliance Management

Which security and privacy standards must your organization meet? Organizations align to and protect themselves through external security standards such as ISO 27001x, the General Data Protection Regulation (GDPR), and the NIST Cybersecurity Framework (CSF). Working with Protiviti to can assist in ensuring that the organization meets 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. The managed SOC must carry out improvements on an ongoing basis that benefit the organizational clients. Part of these improvements to organizational security processes involves performing after action reporting/post-mortem investigations of incidents to identify how the organization could be more well protected.

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.

Cyber Defense Hub

Proactive Monitoring for Security Threats

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.

Threat Monitoring

- 24x7x365 Security Monitoring from onshore and offshore
- Threat detection and containment
- Automated system health monitoring

Protection against Risk

- Threat response and incident containment
- Ongoing consistent tuning of the environment to ensure the highest fidelity coverages are deployed within Microsoft Sentinel

Visibility

- Enhanced visibility into threat activity utilizing threat intelligence and customized hunt campaigns
- Faster, consistent investigations across disparate technologies

Streamlined Incident Response

- Detailed containment automation and plays
- Customized runbooks
- Focused, dedicated response that reduces mean times to detect, respond, and resolve

Business Outcomes

- Protection of 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
- Microsoft Sentinel Monitoring

Schedule a Technology Assessment today by contacting us at TechnologyConsulting@Protiviti.com.

Protiviti.com/Technology Consulting

TechnologyConsulting@Protiviti.com

TCblog.Protiviti.com

protiviti®
Global Business Consulting