snp technologies inc.

SNP's Managed XDR Adaptive SOC Services Powered By Microsoft Sentinel and Copilot

SNP's Managed Extended Detection and Response (MXDR) for Microsoft Sentinel service, brings integrations with Microsoft services like Microsoft Defenders, Threat intelligence and customer Hybrid/Multi-cloud infrastructure to monitor, detect and respond threats quickly. With our managed security operations team, SNP's threat detection experts help identify, investigate and provide high fidelity detection through ML-based threat modelling.

SERVICES

Security Posture
Comprehensive stance towards protecting against security threats and risks. Encompasses a combination of policies, procedures, technologies, and practices designed to safeguard assets, data, and systems from unauthorized access and breaches.

SecOps
Maintaining security measures, processes, and tools is essential to uphold stringent security standards and effectively defend against potential threats.

MDR
Continuous loop of detection and response, which provides comprehensive protection, customized to specific environment and business needs.

SOAR
Security Orchestration, Automation and Response will streamline security operations and improve incident response times

Copilot Fuelled Security
Elevating security operations through intelligent automation and collaboration.

Service Delivery Management
Access to 24*7 Security Analysts, Security Technical Lead, Dedicated Service Delivery Manager

1 Security Architectural Analysis

- Assess the client environment and the requirements for Zero Trust
- Evaluate the organization's technology stack, intrusion detection systems, and any other security tools in use.

2 Security Maturity Model

- Enhancing the cybersecurity maturity, where we ensure that the state we are building is safe and secure.
- Conduct testing to verify that security controls and procedures are effective and aligned with the security framework.

3 Manage Extended Detect & Response (MXDR)

- Maintaining the state of maturity with MXDR services.
- Prioritize identified risks/incident based on their severity and potential impact.
- Incident response procedures for containing and mitigating security incidents.

Tools

- Defender for Cloud
- Defender for M365
- Defender for Identity
- Azure Sentinel
- Azure Playbooks
- SNP's CMP Portal
- Azure Sentinel
- Copilot for Security

SNP's Managed Extended Detect & Response (MXDR) Services

MANAGED SECURITY

- **What** – Ensure security organization(s) has visibility into all subscriptions connected to your enterprise environment
- **Why –** Visibility is required to assess risk and to identify whether the policies of the organization and any regulatory requirements are being followed.
- **How** – Ensure all Azure environments that connect to production environment/network apply Governance /Security controls

MONITORING & MANAGING

Continuous monitoring and identify the most critical events leading to intrusion attempts, at risk IPs, critical vulnerabilities and threats in the real time using the security tools

MANAGED SIEM & M365

Fully managed rule and correlation optimization evolves based not only on your threats, but threats to our customers worldwide.

MANAGED DETECTION & RESPONSE (24X7)

Detect and have complete control over any malware trying to make its way into your organization. Keep a close on subsequent payloads and employ contextual remedial tactics.

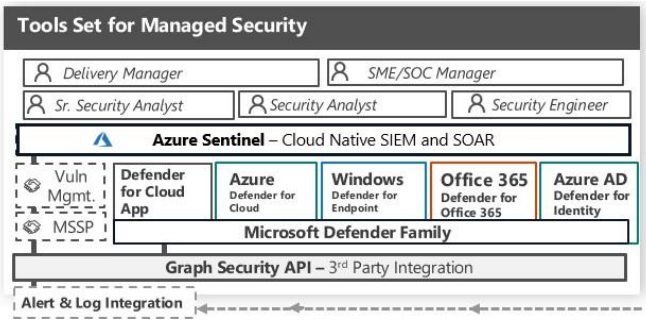
SNP's Manage, Extended Detect Response (MXDR) Tools & Responsibilities

Red Team Key Responsibilities:

- **Cyber Security Manager** – Responsible for security team delivery.
- **SME/Technical Lead** – Focus on Security design, identifying the tools and solutions, GRC and strategies
- **Security Engineer** – VAPT, threat intelligence and security data, proactive hunting for threats, vulnerabilities.

Blue Team Key Responsibilities:

- **SDM Manager** – Responsible for service team delivery.
- **Sr. Security Analyst –** Performs deep analysis and co-relates with threat intelligence, nature of attack, entities effected, remediation and recovery, compliance remediation.
- **Security Analyst -** Monitoring SIEM alerts, alert prioritization, triage to determine the severity of threat/alert/incident



SNP Technologies Inc. helping customers drive business excellence with Microsoft Azure

Microsoft

Advanced Specializations

Analytics on Microsoft Azure | Networking Services | Azure Virtual Desktops | Kubernetes on Microsoft Azure | Modernization of Web Applications to Microsoft Azure | Windows & SQL Server Migrations to Microsoft Azure | Cloud Security

Microsoft

2021 MSUS Partner of the year winner

Business Excellence in Solution Assessments

Microsoft

2019 Partner of the year winner

Intelligent Cloud & OSS on Azure

Mic...

2019 Partner of the year Finalist

Open-Source Applications & Infrastructure on Azure

Microsoft

2019 Partner of the year winner

Solution Innovation on Microsoft Azure Award

Contact us:

Sachin Parikh, VP Business Development, SNP Technologies Inc.

Email: sachin@snp.com

www.snp.com