snp technologies inc.

SNP's Managed Detect & Response Services Powered by Microsoft Sentinel & Defenders (MXDR)

Combines the Power of Microsoft Sentinel with 24/7 Managed Monitoring & Security Operations

SNP's Managed Detection and Response (MDR) for Microsoft Sentinel service, brings integrations with Microsoft services like Microsoft Defenders (MXDR), 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.

SERVICE ENTITLEMENTS	BASIC	ADVANCED	PREMIUM
Security Posture Accurate and unified view of entire multi-cloud landscape and their compliance status to build a secure, compliant, and resilient enviroment	✓	✓	✓
SecOps Unified Visibility into threats, attacks, vulnerabilities and compliance status.	✓	✓	✓
MDR Entire Life-Cycle Management from detection to resolution		✓	✓
SOAR Security Orchestration, Automation and Response		✓	✓
MXDR Advanced Threat Intelligence & Hunting, Vulnerability Testing, Penetration Testing			✓
Service Delivery Management Access to 24*7 Security Analysts, Security Technical Lead, Dedicated Service Delivery Manager	✓	✓	✓

SNP's Manage, Detect Response (MDR) Setup

1 Security Maturity Model

- Infrastructure Setup
- Log Source Ingestion
- Alert Configuration
- SOAR Configuration
- Initial Alert Tuning

2 Manage Detect & Response (MDR)

- Defender for Office 365, Identity & Endpoint
- Cloud App Security (MCAS)
- Integration with SIEM
- Policy Tuning

3 Extended Detection Response (XDR)

- Integration with MDR Monitoring
- Incident Response
- Security Controls & Deployment

Deliverables

- Rationalization Report
- Assessment Report
- Remediation Report
- Sentinel Build-in Document
- Monthly & Quarterly Technical /Business Review
- Compliance Report

Tools

- Defender for Cloud
- Defender for M365
- Defender for Identity
- Azure Sentinel
- Azure Playbooks
- SNP's CMP Portal
- Azure Sentinel
- Metasploit- Pen Test

snp technologies inc.

SNP's Managed Detect & Response (MDR) 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.

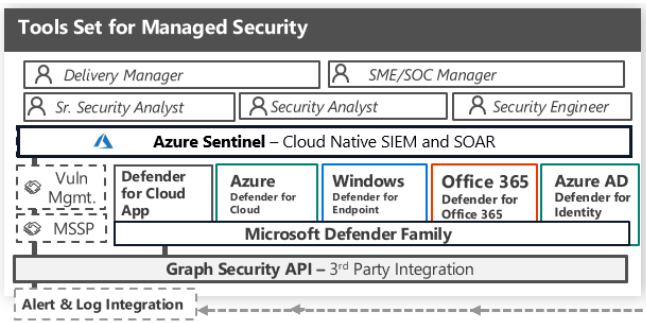
SNP's Manage, Detect Response (MDR) Tools & Responsibilities

Red Team Key Responsibilities:

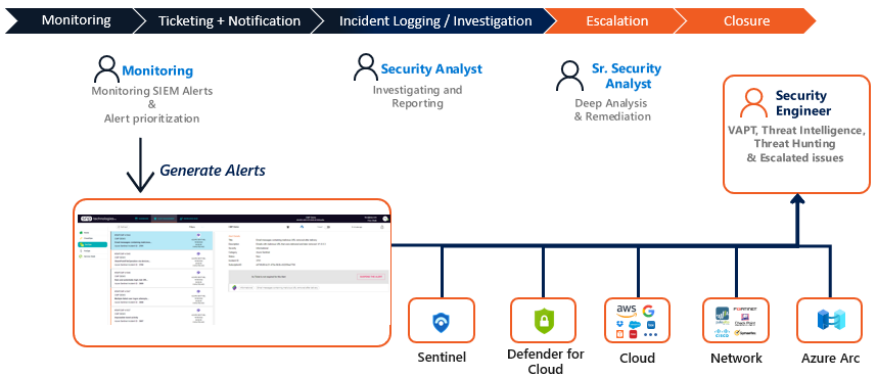
- **Cyber Security Manager** – Responsible for security team delivery.
- **SME/Technical Lead** – Focus on Security design, identifying the tools and solutions, GRC and strategies
- **Security Engineer** – VAPT, threat intelligence and security data, proactive hunting for threats, vulnerabilities.

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
- **Incident/Event Management-** Monitoring SIEM alerts, alert prioritization, triage to determine the severity of threat/alert/incident

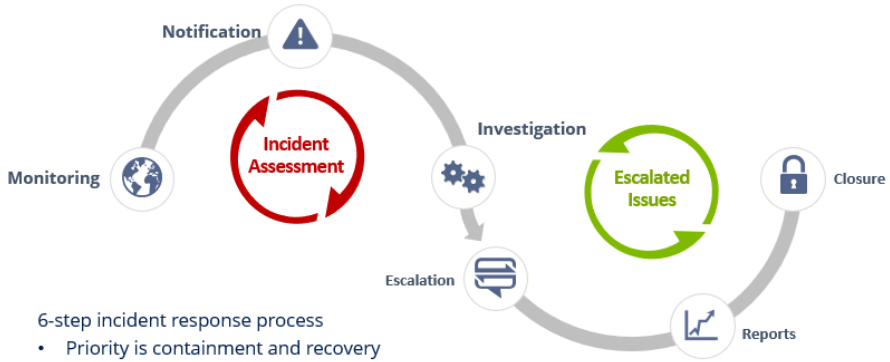


SNP's Manage, Detect Response (MDR) Incident Handling Flow

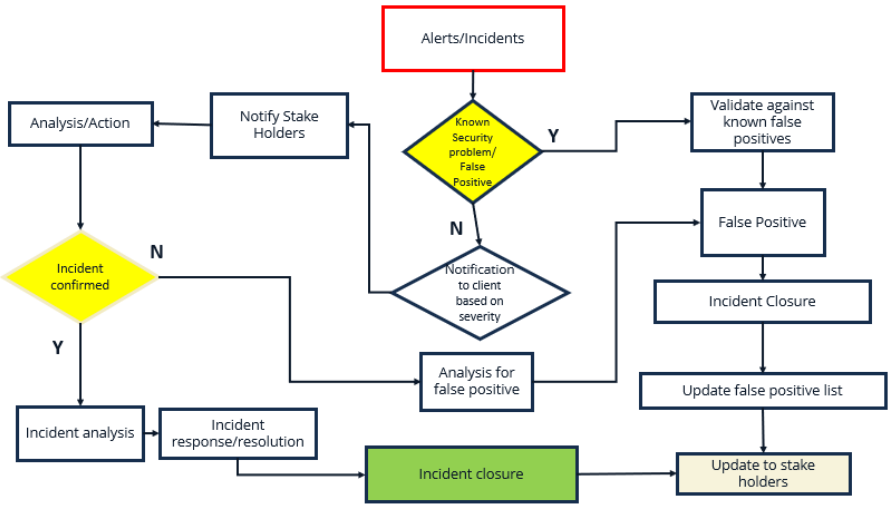


snp technologies inc.

SNP's Managed Detect & Response (MDR) – Incident Process Lifecycle



SNP's Manage, Detect Response (MDR) Incident Analysis Lifecycle



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

Microsoft

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