CISCO SECURE XDR MENTORED POV PLUS

Service Overview:

At Netnology, we specialize in Cisco's Secure XDR solution enablement and implementation services to expedite the adoption of Cisco Secure XDR. As part of this Mentored install service offer, our subject matter experts (SMEs) partner with your team to ensure a smooth deployment of Cisco's Secure XDR solution in a lab / staging environment. Netnology will also provide knowledge transfer to equip your staff with the necessary skills to configure and manage Cisco's Secure XDR solution.

Solution Overview:

Cisco XDR stands for "Extended Detection and Response" and is a unified security solution that integrates and correlates data from multiple security products across an organization's network to detect, prioritize and respond to threats more efficiently and effectively. XDR aims to reduce false positives and provide advanced threat detection, investigation, and response capabilities across an organization's entire IT infrastructure. XDR solutions are meant to help organizations better protect their networks, endpoints, cloud environments, and other digital assets from a wide range of cyber threats, including malware, ransomware, phishing attacks, and more.

- **Flexible integration**: The amount and method of integration with existing security solutions depends on the XDR solution itself, but there is often a way to incorporate security tools, especially endpoint security, into an XDR platform.
- **Centralized view**: XDR would not be much without a central view of the information that it is collecting. XDR looks at most, if not all, of your security environment, and you need a central hub to parse all that information.
- **Machine learning**: XDR platforms offer machine learning powered analysis of security data. This is especially helpful in lowering response times because security personnel have less work to do before they get to solve a security issue.
- **Automation**: Like SOAR solutions, XDR uses automation to reduce SecOps workloads. It only automates simple tasks, but every little bit helps.
- **Simplifying data collection and analysis**: Automate the collection and correlation of security data from across the organization's security environment.
- **Providing better context for alerts:** Progressive disclosure of information helps to quickly determine the scope and severity of a potential threat.

Service Benefits:
Netnology has a team of world class engineers who specialize in Cisco's Secure XDR solution and are passionate about customer success. Netnology will partner with you to provide:

- Step-by-step guidance on Cisco Secure XDR deployment.
- Configuration and documentation of Cisco Secure XDR.
- Knowledge transfer to ensure customer is ready to configure and manage the environment.

Target Audience:

This service is designed for network architects, network-security engineers and administrators who will configure, deploy, and manage the Cisco Secure XDR.

Scope of Services:

As part of the 2-day Mentored POV Plus engagement, Netnology will help with the following:

- Cisco Secure XDR Overview
- Dashboard Customizations
- Integration's Function and Performance Verification
    - o Secure Endpoint
    - o Orbital
    - o Cisco Secure Firewall
    - o Umbrella
- Threat hunting
- Ribbon uses

Prerequisites:

Customer needs to acquire the necessary software licenses for the deployment of Cisco Secure XDR.

Service Deliverables:

No	Deliverable	Service Details
1.	Project Kickoff	• Project Overview • Solution Overview
2.	Dashboard Overview	• Dashboard Creation • Tile Customization
3.	Device Integration	• Secure Endpoint • Orbital • Cisco Secure Firewall • Umbrella
4.	Threat Hunting	• Incident Prioritization • Incident Investigation with Cisco XDR • Incident Creation with XDR Analytics • Walk through incidents
5	Ribbon	• Ribbon overview • Ribbon customization • Use case
6.	Knowledge Transfer	• Explanation of the deployed solution.