

CISCO TETRATION MENTORED POV PLUS

Service Overview:

At Netnology, we specialize in Cisco enablement and implementation services to expedite the adoption of Tetration. As part of this Mentored POV Plus service offer, our subject matter experts (SME) partner with your team to ensure a smooth deployment of the Tetration solution in the lab environment and provide knowledge transfer to equip your staff with the necessary skills to configure and manage the Tetration environment.

Cisco Tetration Solution:

Cisco Tetration delivers workload protection through a zero-trust model with segmentation. An environment enabled with Tetration provides a rapid identification of security incidents, containment and reduced attack surface. The Cisco Tetration Solution is infrastructure agnostic providing supports for both public cloud workload and on-premises workload protection.

- Automated Whitelist policy tracking changes and keeping policy up to date.
- Zero-Trust Model continuous monitoring of workloads identifies any deviations.
- Identification of deviations in process behavior.
- Software vulnerability detection with associated CVEs and specific remedies.
- User Access control through Cisco AnyConnect enables policy segmentation of application access via user and group information.
- Long-Term data retention for deep forensic evaluation, analysis and troubleshooting
- End-Point device telemetry from laptops, desktops, smartphones, printers, HVAC systems, and other IoT devices through Cisco ISE integration.
- Secure Connectors for the ingest if Orchestrator Telemetry (VMWare vCenter, F5 BIG-IP, etc.) using a cryptographically-secure reverse tunnel that can be used by Tetration to reach external orchestrators within the client network.
- Notifications through Edge Appliances supporting alerts through Syslog, Email, Slack, PagerDuty, Kinesis and ISE.

Service Benefits:

Netnology has a team of world class engineers who specialize in the Cisco Tetration solution and are passionate about customer success. Netnology will partner with you to provide:

- Step-by-step guidance from an SME on Tetration solution deployment
- Configuration and documentation of Tetration solution
- Knowledge transfer to ensure customer is ready to configure and manage the lab environment

Scope of Services:

As part of the 5-day Mentored POV Plus engagement, Netnology will help with the following:

- Solution Overview
- Tetration Cluster Deployment (Tetration-V/SaaS⁽¹⁾)
- Software Sensor Deployment (up to 30 sensors and 2 applications)
- External Connectors Enablement (up to 2 appliances)
- Application Mapping & Segmentation (up to 2 applications in dev and/or test environment)
- Exposures & Software Vulnerability Identification
- Identification, Resolution, Monitoring (up to 4)
- Knowledge Transfer

(1) For Tetration-V, additional services required for host environment setup (e.g. Cisco HyperFlex).

Target Audience:

This service is designed for Network Architects, Network Engineers, Systems Engineers, Security Engineers and Administrators configuring, deploying and managing the Cisco Tetration in lab environment.

Prerequisites:

Customer needs to ensure that all equipment and devices are racked & stacked, cabled and powered-up prior to the kick-off. Customer also needs to acquire the necessary software licenses for the deployment of Tetration solution.

Service Deliverables:

No	Deliverable	Service Details
1.	Project Kickoff	<ul style="list-style-type: none"> • Project Overview • Solution Overview
2.	Tetration Deployment	<ul style="list-style-type: none"> • Install and setup Tetration • Setup Email based access, NTP, DNS, Smart Account • Registration for licensing
3.	Software Sensor Deployments	<ul style="list-style-type: none"> • Deploy up to 30 Software Sensors and 2 application <ul style="list-style-type: none"> ○ Windows ○ Linux
4.	External Connectors	<ul style="list-style-type: none"> • Create External Telemetry Ingests <ul style="list-style-type: none"> ○ VMware ○ DNS
5.	Application Mapping & Segmentation	<ul style="list-style-type: none"> • Analysis of Telemetry <ul style="list-style-type: none"> ○ Identify Applications • Create Human Intent Based Policies <ul style="list-style-type: none"> ○ E.g. VMware Telemetry • Create Segmentation and Whitelist policy <ul style="list-style-type: none"> ○ Simulate the policy application enforcement
6.	Exposures & Software Vulnerability Identification	<ul style="list-style-type: none"> • Identify Vulnerabilities <ul style="list-style-type: none"> ○ External Exposures ○ CVE Identification
7.	Identification, Resolution & Monitoring	<ul style="list-style-type: none"> • Software Vulnerability <ul style="list-style-type: none"> ○ Resolving CVE ○ Quarantine • Dashboard Creation • Behaviors <ul style="list-style-type: none"> ○ Long-live Process Identification ○ Resolving mis-dropped, escaped, and rejected flows
8.	Knowledge Transfer	<ul style="list-style-type: none"> • Explain to the customer how to configure and manage the solution in the lab environment