

Ensure Networks for Tetration Analytics

Overview

Ensure Networks for Tetration Analytics is a managed application segmentation offering that provides actionable deliverables helping organizations create, analyze, correlate, and enforce application security policies as business grows and evolves. Ensure Networks for Tetration Analytics is focused on creating an immediate ROI for security vulnerability visibility and recommended mitigation while offering a consistent engagement model to move all your applications to Zero Trust security policies over time.

Whether the application or workload is in the cloud, or on premise, BTA's Ensure Networks service delivers agent installation, application dependency mapping, segmentation policies, as well as enforcement. The BTA team of architects and security analysts leverage years of experience with Tetration implementations to prioritize workload and application patching, provide system level monitoring, and application enforcement reporting. Reporting is delivered weekly, monthly, and quarterly and can be adjusted based on your needs or drivers.

A BTA engagement manager schedules working sessions with your team ensuring your Application Visibility, Segmentation, Enforcement Policies, and Forensic Data collection goals are being met as your business moves to a zero-trust model.

From Application Dependency Mapping, to a full Zero-Trust implementation, the BTA Ensure Networks team is available to guide your organization with your Tetration Analytics journey.

Benefits

- Maximize resources through well planned and implemented application segmentation and workload protection.
- Automate Agent installation and configuration
- Mitigate risk by leveraging experienced architects and proven best practices
- Prioritize application and workload patching through CVE reporting and recommendations.
- Know the applications and ports being used in your infrastructure.
- Identify and protect open ports (used and unused) in your network.

Ensure Networks for Tetration Analytics

Deliverables (High Level)

Ensure Networks Management Services (priced per agent)	Silver	Gold	Platinum
Tetration Care and Feeding	X	X	X
CVE Reporting	X	X	X
Attack Surface Reporting	X	X	X
Agent Installation	X	X	X
Annotations and Scopes (Baseline DNS)	X	X	X
Forensic Enablement		X	X
Infoblox, Vcenter		X	X
Monthly Tetration Webinar		X	X
Service Now Integration		X	X
Post Incident Forensic Analysis			X
ACI Policy Definitions and Deployment			X
24x7x365 Response			X

Ensure Networks Segmentation Services (priced per Application)	Silver	Gold	Platinum
Application Segmentation	X	X	X

Deliverables (Detail)

Application Segmentation

BTA Architects will work with your teams to understand application dependencies. Based on the dependencies, BTA will build the segmentation policies, analyze the policy with live traffic, and enforce segmentation policies. BTA will Analyze Enforced Segmentation Policies and deliver Segmentation Compliance and Enforcement reports.

- Build Segmentation Policy using Application Dependency Mapping
- Live Policy Analysis of Segmentation Policy
- Enforce Segmentation Policy
- Analyze Enforced Segmentation Policy
- Segmentation Compliance and Enforcement Report

Ensure Networks for Tetration Analytics

Tetration Care and Feeding

Tetration Care and Feeding includes reporting on Agent Status and Alerts, updating Agent configuration as needed, and consulting on agent upgrade methodology. BTA architects will verify enforcement and report on its status and provide guidance for Role Based Access Control (RBAC) and how it applies to different users.

- Agent Config, Status, Alerts, and Upgrades
- Enforcement Status
- Users/Roles

CVE Reporting

Common Vulnerabilities and Exposures (CVE) Reporting addresses New, Mitigated, and Modified Vulnerabilities. BTA architects will also provide Patching prioritization guidance to ensure the highest priority vulnerabilities are addressed first.

- New, Removed, Modified Vulnerabilities
- Patching prioritization

Attack Surface Recommendations

Attack Surface Recommendations provide information on Open ports. The recommendations will consider Used and Unused ports, non-compliant traffic, CVEs, and common attack vectors. The BTA team will assist your organization in prioritizing which ports should be closed, and which should be whitelisted within your business.

- New, Closed, Modified, Open Ports
- Used/Unused
- Prioritize closing/whitelist

Agent Installation

EnsureNetworks includes Agent Installation on new Operating Systems (OSs). Consulting will be provided to your automation teams to implement best practices for automating Agent installation. In the event of an installation failure, BTA will help troubleshoot Agent Installation.

- Agent Install on new OSs
- Consult Customer automation of Agent install
- Troubleshoot Agent installation

Annotations and Scopes

BTA will provide Annotation Upload, Scope Tree Design, and configuration. DNS integration – Zone Transfer for a single domain is included along with Scopes and Annotation. Configuration reporting will be provided to you and your teams once the configurations are implemented.

- Scope Tree Design, Configuration, and Reporting
- Annotation Upload
- DNS Integration - Zone Transfer DNS for a single domain

Ensure Networks for Tetration Analytics

Forensic Enablement

BTA Architects will enable predefined MITRE attack and Tetration profiles on all workloads and report on forensic events.

- Configure Forensics
- Report on Forensic Events

Infoblox, vCenter

BTA will work with the customer to integrate Infoblox and/or vCenter external orchestrators to integrate IPAM and vCenter tagging into Tetration Annotations. These annotations can be used for Segmentation Policy, Filters, and flow search.

Monthly Tetration Webinar

BTA Architects provide monthly knowledge transfer sessions to your technical team. The trainings will be one (1) hour in length and be tailored to topics that apply to your business

Service Now Integration

For Organizations using Service Now for CMDB or Change Control management, BTA will integrate Tetration and Service Now. This enables Tetration to reflect the assets managed by the Service Now CMDB and affect segmentation policy changes according to the Asset Management workflows. Additionally, BTA can integrate Tetration with Service now Incident Management workflows based on suspicious activity on the workload detected by the Tetration agent.

Post Incident Forensic Analysis

BTA architects will work with your team to configure, identify and analyze critical forensic security events for suspicious activity. This includes the preconfigured Mitre Attack profile and custom profiles based on customer experience and expectations.

ACI Policy Definition and Deployment

Tetration visibility is used to apply broader Segmentation Policies to enforce in ACI contracts while using Tetraton enforcement for micro-segmentation. BTA's experience in ACI and Tetration is uniquely positioned to provide guidance on which policies to enforce in ACI and in Tetration.

24x7x365 Escalation and Incident Management Support

BTA will provide architectural escalation and incident management support 24x7x365. Response times to escalations and incidents are determined by an agreed upon Service Level Objectives (SLO).