Five Essential Steps to Achieve and Maintain Network Security

Chris Jensen
Public Sector Business Development
Agenda

Tenable Intro

1. It all starts with visibility
2. Be dynamic, not static, and proactive, not reactive
3. Use the right tool for the job
4. Look at your network from the attacker’s perspective
5. Make sure your source of trust can be trusted
TENABLE: FROM VULNERABILITY TO EXPOSURE MANAGEMENT LEADERSHIP

MARKET LEADERSHIP

#1 VM Market Share
3 years in a row

RESEARCH DEPTH

“Tenable has its own research team and is usually able to build new detections within 24 hours of finding new vulnerabilities.”

EXPANDING SCOPE

Leader in Forrester Wave for ICS Security Solutions

Forrester

Named CNAPP & Active Directory Defense vendor

Gartner
MANAGING EXPOSURES ACROSS THE MODERN ATTACK SURFACE

EXPOSURE MANAGEMENT

Visibility across the modern attack surface with intelligence to prioritize preventative actions and communicate risk to all levels of the organization.

SOFTWARE VULNERABILITIES

EXTERNAL ATTACK SURFACE

APPLICATION VULNERABILITIES

PUBLIC CLOUD CONFIGURATION

OT VULNERABILITIES

ACCESS PERMISSIONS

On Prem & Remote IT

Internet-Facing Assets

Web Apps /APIs

Public Cloud

Industrial (OT) Infrastructure

Identity
SIGNIFICANT BREACHES TARGET THE WEAKEST LINK ACROSS THE ENTIRE ATTACK SURFACE

- **WANNACRY**
  - LOG4SHELL
  - SOFTWARE VULNERABILITIES
  - On Prem & Remote IT

- **EQUIFAX**
  - EXTERNAL ATTACK SURFACE

- **PANAMA PAPERS**
  - APPLICATION VULNERABILITIES
  - Internet-Facing Assets
  - Web Apps /APIs

- **CAPITAL ONE DATA BREACH**
  - PUBLIC CLOUD CONFIGURATION
  - Public Cloud

- **OT:ICEFALL**
  - OT VULNERABILITIES
  - Industrial (OT) Infrastructure

- **LAPSUS$**
  - ACCESS PERMISSIONS
  - Identity
3 attributes make the modern attack surface more difficult than ever to defend:

1. RAPIDLY GROWING
2. HIGHLY DYNAMIC
3. INCREASINGLY INTERCONNECTED
PROTECT YOUR MODERN ATTACK SURFACE

- Gain visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent attacks
- Communicate exposure risk to make better decisions
Risk-Based Vulnerability Management

A process that employs machine learning analytics to automatically correlate:

- Assessments of traditional and modern assets across the entire attack surface
- Vulnerability severity
- Threat and exploit intelligence
- Asset criticality

... to identify which vulnerabilities pose the greatest risk.
CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or how quickly they should respond to a vulnerability.”
18K vulnerabilities disclosed in 2020
Nearly 3x more than 2016

57% of all vulnerabilities have a CVSS base score of 7 or above

20% vulnerabilities have an exploit available

CVSS 7+
Remediation Policy
- Wastes 76% of the security team's time
- Leaves 44% of risky vulnerabilities in your environment

Nearly 3x more than 2016
YOU’VE GOT 99 FLAWS BUT ALL THEY NEED IS ONE
Elevation of privilege vulnerability in Windows
Used in 2019 ransomware attacks
Proactive
Web Application Scanning

Dynamic Application Security Testing (DAST): A DAST crawls a running web application through the front end to create a site map with all of the pages, links and forms for testing. Once the DAST creates a site map, it interrogates the site through the front end to identify any vulnerabilities in the application custom code or known vulnerabilities in the third-party components that comprise the bulk of the application. Only a DAST tool can identify runtime flaws, which are not apparent in a static environment.

Static Application Security Testing (SAST): A SAST analyzes static environments, i.e., meaning the source code of an application. Used for periodic assessment, It looks at the application and searches for vulnerabilities in the code.
Dynamic vs. Static App Scanning – Use the Right Tool for the Job
As the modern attack surface continues to grow, most organizations now have a significant number of Internet-facing assets they don’t even realize they have, let alone understand whether they are vulnerable to attack.

These unknown or poorly understood assets create a new dimension of risk, providing threat actors easy targets and the opportunity to access assets without anyone knowing.
People outside know more about the organization’s attack surface than those within.

90,000+ internet-exposed servers are still vulnerable

Exposed Kubernetes Clusters, Kubelet Ports Can Be Abused in Cyberattacks

Organizations must ensure their kubellets and related APIs aren’t inadvertently exposed or lack proper access control, offering an easy access point for malicious actors.

Half of security pros say their public clouds were breached during the pandemic

Steve Zuiser, March 22, 2021

Unknown, unmanaged data is creating cloud risks via Shadow IT
See Your Network as Others See It
SECURE THE IDENTITY SYSTEMS THEMSELVES

“...Directory Services is the underlying infrastructure that supports authentication and authorization. Its compromise would de facto render any zero trust implementation ineffective.”

- NSTAC Report to the President on Communications Resiliency, 2022
But can you trust your identity system?

Trust is a tricky thing.
Secure the Trust Provider

Active Directory holds the keys to everything

- Governs authentication, holds all passwords
- Manages access rights to every vital asset
- Ensures the user is known and managed at all times

"...trusted identity management solutions are unquestionably foundational, as zero trust is based on a continuous cycle of credentialing, verifying, and authorizing identity for person and non-person entities."

-NSTAC Report to the President on Communications Resiliency, 2022
Recent Department of Commerce IG Report
Recommendations to NOAA included:

1. Establish processes and procedures to **periodically review** all active directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.

2. Determine the feasibility of requiring all NOAA line offices to use specialized active directory security tool(s) to conduct **periodic reviews**.

3. Establish procedures to **periodically review** active directories and ensure compliance with account management requirements as stated in the Department’s policy and following industry best practices.
Understanding Common Attack Paths

**Initial Foothold**

**Explore**
Understand the target environment - 
RECON

**Elevate**
Elevate Access - 
PASSWORD SPRAY

**Evade**
Pivot to evade detection - 
DCSYNC

**Establish**
Establish backdoor access & wait… - 
AdminSDHolder

**Exfil**
Extract sensitive data

**Encrypt**
Data encryption and ransom

**PHASE 1:**
PHISH / CVE EXPLOIT

**PHASE 2:**
AD ATTACK – ELEVATE /PERSIST

**PHASE 3:**
EXTRACT/ENCRYPT
Steps to Reduce Cyber Risk

1. Start with comprehensive visibility
2. Take a dynamic, proactive, risk-based approach
3. Use the right tool for the job
4. Get an external view
5. Proactively protect your source of trust
Thank You!