



Vulnerability Management  
Does Not Have to  
Be So Difficult.  
**Let Us Help.**

## What is Vulnerability Management?

- The “continuous practice of proactively identifying, classifying, prioritizing, remediating, and mitigating” software vulnerabilities
- It includes vulnerability scanning, vulnerability validation, patching, configuration management, asset management, and change coordination

## Overcoming Challenges

Companies approach vulnerability management in different ways; many implement a vulnerability management tool to identify known exploits in their infrastructure, and some may purchase tools to update software packages in an effort to limit resource hours spent on these tasks. Despite the chosen approach, various aspects of the vulnerability management process are often overlooked, as organizations are unwilling to invest the significant time and resources required.

Scanning the environment for vulnerabilities is an effective starting point, but a qualified security expert needs to analyze the results to ensure they are valid and to help prioritize the focus for any required remediation. The team applying software updates for the organization must work synchronously with the team performing vulnerability scanning; if not, the result will be a disjointed solution that contains gaps in the security posture, leaving the company susceptible to a potential breach.

Knowing how to prioritize the remediation of vulnerabilities is critical. Identifying, prioritizing, and remediating the seemingly endless number of vulnerabilities within your IT infrastructure is an overwhelming but essential task. Spend time on the wrong vulnerabilities, and you could miss the one that lets criminals into your environment.

## Overview

EITS’ vulnerability management team works with you to identify and categorize all assets/software vulnerabilities, as well as tune any existing vulnerability management processes you may have in place. Additionally, our experts analyze scan results and customize reporting for clear visibility; this ensures properly prioritized remediation of any vulnerabilities identified.

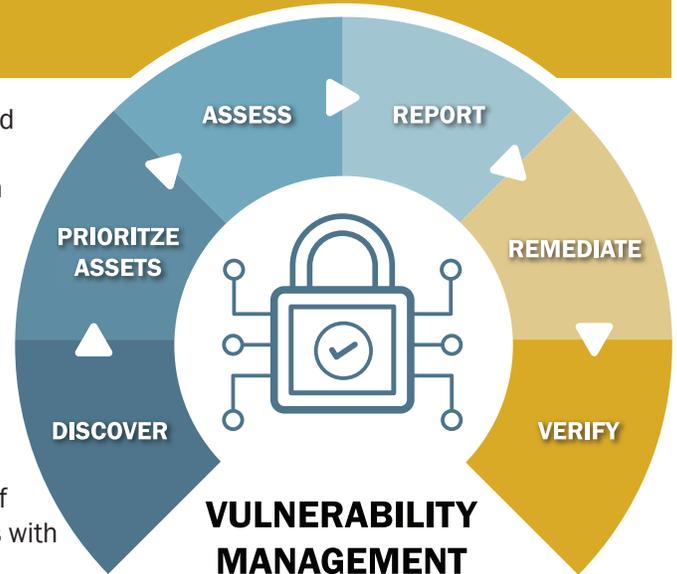
EITS will assist your organization in defining reporting requirements, as tailored to the needs of your business. A deep review of scan data, false positives, and the latest intelligence are regularly communicated to ensure understanding across all levels of the organization. These efforts strengthen your awareness of your security posture.

EITS partners with clients to address concerns surrounding open vulnerabilities and incomplete remediation. We enable you to take action and continuously improve processes to decrease the exploitation of vulnerabilities in your environment. We share our expertise with you, clarifying scan data and focusing on the areas first needing attention.

# EITS Fully Managed Approach

EITS' vulnerability management approach provides an end-to-end solution through the identification and remediation of both existing and new exploits. EITS' security team works directly with you to define key risks, analyze scan results, prioritize threats, and customize reporting according to your organization's specific needs. Our experts will advise your team through intelligence driven analysis and feedback, enabling future management through customized and repeatable processes.

Why spin your wheels in hiring, training and attempting to retain inhouse resources? Let us do this for you. EITS provides personnel with the expertise required to unleash the full value of your cybersecurity investments, and increase their effectiveness with proven best practices!



## Vulnerability Prioritization

Automate the prioritization / ranking of a vulnerability based on the inherent value of the asset and whether it is being weaponized by criminals.

## Reduce Your Attack Surface by Quickly Finding and Fixing Vulnerabilities

EITS' approach enables the quick discovery of weaknesses in your organization's assets through automated network vulnerability scanning and monitoring.

## Maintain Compliance

EITS helps ensure your company achieves and maintains compliance with regulatory mandates, such as the GDPR and PCI DSS.

## Executive Workshops

EITS excels at presenting vulnerability management research and findings to your executive team, in their language. This enables executive-level support for the level of effort required to prioritize and patch vulnerabilities.

## False Positive Analysis

A thorough analysis eliminates false positives, which greatly reduces the time and energy spent on applying the fix.

## Visualize All of Your Assets

- Eliminate Guesswork - Define customized reporting criteria and requirements to ensure precise and relevant data
- Program Acceleration - Ensure quick results through collaboration between EITS and customer teams in all phases of management
- Risk Assessment - Assess your potential for vulnerabilities with on-demand scanning
- Remediation Tracking - EITS will manage discovered vulnerabilities through to escalation or closure
- Custom Reporting - Structured review cycles and custom reports allow you to assess the reliability and maturity of your program
- Requirements Intelligence - Expert advice from EITS' experienced security professionals will direct your organization's end-to-end solution through to remediation

## End-to-End Support

Unlike traditional vulnerability management programs, we offer end-to-end support from scan initiation to remediation; this allows you to effectively address vulnerabilities with a systematic approach.

## Remediation Tracking

Vulnerability management doesn't end once a scan is completed; a program can only be validated as effective through continued quality of remediation, as well as taking corrective action to avoid recurrence. EITS diligently tracks every vulnerability until it is brought to closure.

## Benefits of Using EITS Services

- Operational time savings
- Vulnerability scan validations
- Vulnerability prioritization
- Policy, procedure, and process development
- Dedicated security advisor
- Contextualized vulnerability reporting
- Program risk and ROI analysis
- Simplified regulatory compliance
- Proprietary threat intelligence