EITS
Enterprise IT Security

Vulnerability Management
A Best Practices Approach to Overcoming Challenges

SOLUTION BRIEF

KEY BENEFITS

- Identify, classify, remediate and mitigate software vulnerabilities

- Reduction of the attack surface

- Maintain compliance

- Remediation tracking

Reduce your organization's cyber risk by identifying and categorizing network weaknesses and potential entry points for attackers. Our methodology ensures that you have clear visibility into the vulnerabilities that pose the biggest risk to your organization.

Companies approach vulnerability management in diverse ways; many implement a vulnerability management tool to identify known exploits in their infrastructure, and some purchase tools to update software packages to limit resource hours spent on these tasks. Despite the chosen approach, various aspects of management are often overlooked, as organizations are unwilling to invest the 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. Root cause analysis and process changes ensure security configurations are implemented as systems are built. The team applying 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 can be an overwhelming but essential task. Spend time on the wrong vulnerabilities, and you could miss the one that lets the bad actors into your environment.

## A Fully Managed Approach to Vulnerability Management

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

Benefits of Using EITS for Vulnerability Management

- 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

ASSESS
REPORT
REMEDIATE
VERIFY
DISCOVER
PRIORITIZE ASSETS
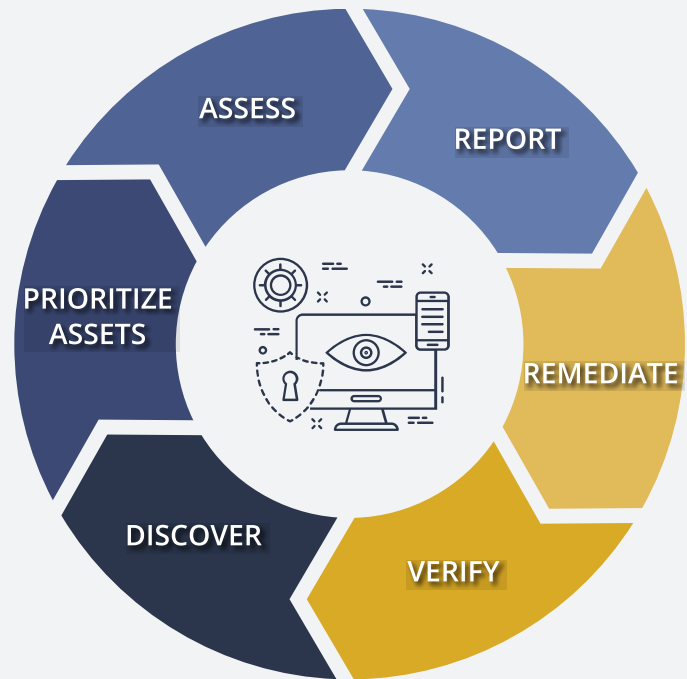
The EITS team of experts can help whether you are considering a review of your current vulnerability management program or implementing a program from scratch. Let our team of experts help you meet every aspect of NIST Cybersecurity Framework PR.IP-12. This includes NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 and ISO/IEC 27001:2013 A.12.6.1, A.18.2.2. Our team is well versed in vulnerability management metrics, key performance indicators, and key risk indicators.

EITS
Enterprise IT Security

EITS helps businesses, education and government agencies build and manage secure IT environments for a changing world. We secure what matters most: their business, their IT environment, their intellectual property and their reputation. Our holistic approach addresses the Architectural, Operational and Organizational facets of Information Security applying a proven architecture blueprint for scalable, agile, manageable IT environments, hardened to DOD-level security standards. Agencies and businesses who have suffered severe data breaches have tapped EITS to remediate their issues, and to dramatically lower the risk of future events. We are driven by our culture of Excellence and Substance: We Always Make Mission.