BLUE GOAT
CYBER

Vulnerability Assessment Services

Our vulnerability assessment services check for missing patches and misconfigurations on operating systems and applications.

Steps to Schedule Your Vulnerability Assessment:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

A Vulnerability Assessment is a process of evaluating assets in an enterprise for missing patches and misconfigurations. Often the vulnerability assessment is in support of regulatory compliance or compliance with a standard. The process identifies and prioritizes vulnerabilities based on criteria such as the likelihood of the vulnerability being exploited and the severity of the vulnerability – what the vulnerability provides the attacker when used. These criteria are used to categorize the vulnerability as Critical, High, Medium, Low, or Informational.

We assess systems using vulnerability scanning tools and manual methods to identify and prioritize findings based on the criticality of system vulnerabilities. We scrub findings to eliminate false positives and prioritize risk based on existing security controls for your environment. The Vulnerability Assessment looks for missing patches and existing vulnerabilities for each system. We use authenticated scans wherever possible to reduce false positives and improve accuracy.

We typically perform a Vulnerability Assessment on an internal enterprise environment and a Penetration Test against the external, public-facing systems. We can, however, perform a Vulnerability Assessment against your external systems and wireless systems as well.

BENEFITS / RETURN ON INVESTMENT (ROI)

The majority of attacks take advantage of unpatched or misconfigured systems or applications.

Our Vulnerability Assessment service helps you identify vulnerable systems and applications. We provide prioritized, risk-based step-by-step actions to fix the identified vulnerable systems and applications.

Our Vulnerability Assessment not only looks for unpatched systems but checks for misconfigured systems, applications, and unnecessary services. Our Vulnerability Assessment service also helps ensure your IT assets are compliant with policy and standards, such as the following:

- PCI DSS
- HIPAA
- FISMA
- DISA STIGs
- GLBA guidelines
- OWASP
- NIST

WHAT YOU GET / DELIVERABLES

You get three items:

1. Vulnerability Assessment Report

Our **Vulnerability Assessment Report** includes the devices (IP addresses, applications, URLs, etc.) tested, vulnerabilities discovered, steps taken during the assessment, and prioritized recommendations. Our report has many useful elements such as an Executive Summary, Top 5 Findings, Top 5 Vulnerable systems, etc.

We make every effort possible to produce a report free of false positives and easy to understand. Our aim is to provide value to you for the purpose of making your environment more secure.

2. Vulnerability Assessment Report Findings Review

We schedule an online session with you where we walk through the report with your team and answer any questions about the findings, our methods, or the steps required for remediation. Many competitors deliver a confusing lengthy report at the end of the assessment for you to decipher. Our vulnerability assessment report review adds tremendous value because we can clarify findings and remediation steps.

3. Discounted Rerun Option

How do you know the steps you took to fix our vulnerability assessment report findings actually worked? Validation removes the guesswork. When you're ready, after fixing the issues identified in the vulnerability assessment report, we offer a deep discount to rerun the same vulnerability assessment. This is a crucial and often overlooked step in this process. Validating security controls, patches, and other fix actions is extremely important. We have discovered numerous organizations that thought they fixed a finding we identified, only to discover after another assessment that the finding was still there.