VULNERABILITY ASSESSMENTS

Routine Vulnerability Assessments are a key component of any organizations security program. At a minimum Vulnerability Assessment's shed light on issues present on systems that could be targeted and leveraged by a malicious threat. These issues range from missing patches and the use of insecure services, to misconfigurations. Vulnerability Assessment data can also provide insight on issues within the organizations processes and procedures, which if not addressed, can continue to negatively impact the organizations Security Posture through the accumulation of **Security Debt.** Specifically, when considering the age of a vulnerability and when a given system was deployed, vulnerability assessment data can highlight problems with patch management, change management and/or hardening processes, all of which when taken in context can better help organization focus their remediation efforts by focusing on the core problem, rather than the individual issues. Contextual Security Solution's Vulnerability Assessment Element attempts to assist organizations better understand their areas of concern through the use of **Security Metrics**.

BENEFITS

Per the most recent "Cost of a Data Breach Report" , which is an annual report created by the IBM / Ponemon Institute, and included data from over 500 organizations that suffered a breach in 2019/2020, **routine vulnerability testing reduced the cost of a breach on an average by $172,817.**

In addition, Vulnerability Assessments are a key activity found in the **Center for Internet Security's (CIS) Top 20 Controls.** Specifically, Control 3 "Continuous Vulnerability Management", which is a Basic control within the framework, recommends that all organizations (Implementation Groups 1, 2 and 3) perform Vulnerability Assessments to identify, remediate, and minimize the window of opportunity for attackers.

BREACH SAVINGS

$172,817

For organizations that conduct routine Vulnerability Assessments

COMPLIANCE CONTEXT

In addition to the benefits listed above, Vulnerability Assessments are in most cases required by organizations that store, process or transmit cardholder data (**Payment Card Industry Data Security Standard** Requirement 11.2 – Run internal and external network vulnerability scans at least quarterly and after any significant change in the network).

Per the **National Institute of Standards and Technology (NIST)** special publication 800-53 (Security and Privacy Controls for Information Systems and Organizations), Control RA-5 states that organizations should monitor and scan for vulnerabilities in systems and hosted applications. Furthermore, vulnerability monitoring should include scanning for patch levels; scanning for functions, ports, protocols, and services.

VULNERABILITY ASSESSMENT PROCESS

Initial Vulnerability Assessment

- ✓ **Establish Baseline**
  - ✓ **Inventorying of Systems**
  - ✓ **Identification of Services and Protocols in Use**
- ✓ **Identification of Vulnerabilities**
  - ✓ **Categorization of Vulnerabilities (Risk by CVSS, Cause, Remediation)**
  - ✓ **Calculation of Key Metrics (e.g. Security Debt)**

Subsequent Assessments

- ✓ **Provide Continuous Monitoring of the Organizations Security Posture**
- ✓ **Provide Trend Data (Previous Assessments, Industry Averages)**
- ✓ **Provide Effectiveness of Remediation Efforts**
- ✓ **Enhanced B.A.S.E. Package Includes Two (2) Additional Assessments**