Virginia Information Technologies Agency

VITA

Vulnerability Scanning and Intrusion Detection System (IDS) Reporting FAQs

Vulnerability Scanning Reporting FAQs:

1. What systems need to be reported on?

- Public facing sensitive systems

2. What is the definition of a public facing system?

- IT system or application that is accessible via the internet from outside of an organizations internal network

3. Do the vulnerability scans performed by the Partnership meet the SEC501, RA-5 and SEC 520 Vulnerability Scanning requirement?

- The partnership scans meet part of the requirements. The partnership scans only includes the server, OS, network hardware layers. The partnership vulnerability scans do not include application layer vulnerability scanning.

4. What if the partnership manages my server?

- Agency must still submit the web application vulnerability scan results to CSRM CommonwealthSecurity@vita.virginia.gov, server/OS scans are already sent to CSRM.

5. What are the scans that the partnership performs and how often are they performed?

- The partnership performs monthly vulnerability scans of the partnership agencies servers and network infrastructure.

6. Does VITA offer the web application vulnerability scans required by SEC501 and SEC 520? What are the costs and the scope?

- Web application scans can be done in house, by a third party, or by VITA. Details for VITA's vulnerability scans can be found at: http://shop.vita.virginia.gov/ProductDetail.aspx?id=6442472344&TX_ID=6442469742

7. What if we use the VITA web app scanning service?

- If the scans performed included all public facing sensitive systems please notify CommonwealthSecurity@vita.virginia.gov. It is not necessary to include copies of scans performed by VITA.

8. What if we don’t have public facing sensitive systems?

- Notify CSRM CommonwealthSecurity@vita.virginia.gov

9. What if we are not part of the partnership or this particular system is outside partnership infrastructure?

- Submit server/OS scan results and Application vulnerability scans to CSRM CommonwealthSecurity@vita.virginia.gov

10. What if we outsourced the hosting of our sensitive public facing system?

- Check with your vendor for PCI, SSAE16 reports and the agreements in place between your organization and the vendor, request associated reports from the vendor and submit to CSRM CommonwealthSecurity@vita.virginia.gov if available. *Please note*: Outsourcing the hosting and administration of sensitive applications does not shift risk to the vendor without specific language stated in contracts or agreements.

11. What do I need to report?

- Report the following:

  1. Date of Scan

  2. Host Name

  3. IP or DNS Entry

  4. Vulnerability description

  5. Severity level/Risk Rating (high, medium, low)

  6. Common Vulnerability and Exposure (CVE) reference

  7. Remediation action (e.g. what’s needed … disable port, etc.)

  8. Results of follow-up scan after remediation action is taken

12. How often must we submit these reports?

- Once every 90 days (quarterly)

Intrusion Detection System (IDS) Reporting FAQs:

1. What must be reported?

- Please report the following:

1. Date Range for the Report (example: Jan. 1, 2013 – March 31, 2013)
2. Total number of attacks per month (example: Jan 2013 = 1,000,000, Feb 2013=1,500,000, March 2013= 1,250,000)
3. Total number of high attacks per month
4. Total number of medium attacks per month
5. Total number of low attacks per month
6. Top 10 high attacks & number of attacks seen (example: SSH Brute Force, total: 100 attacks)
7. Top 10 Source IPs
8. Top 10 Destination IPs
9. Top 10 countries of origin of attacks with percentages per month (example: Jan 2013: US – 80%, China =4%, Russia = 3%, Canada = 3%, U.K. = 3%, India=2%, Brazil=2%, Germany=2%, Ireland=2%, Sweden=2%)
10. Top 10 types of attacks (example: Denial of Service, Privilege Escalation)
11. Top 10 inbound attacks by protocol/service/port (http/www/80)
12. Top 10 outbound attacks by protocol/service/port (http/www/80)

2. How often must these be reported?

- Quarterly

3. What if the partnership provides our IDS capabilities?

- The partnership IDS reports are submitted to CSRM monthly on your behalf. Agencies must submit IDS reports for any connections that not maintained by a partnership IDS.

4. What if my agency is a partnership customer but maintains another network outside of the partnership?

- Submit IDS reports quarterly to CSRM CommonwealthSecurity@vita.virginia.gov for network(s) that are not maintained by the partnership

Risk Assessment Plan FAQs:

1. What are the requirements?

- Develop or update as necessary a three year risk assessment plan for the agency’s sensitive IT systems and submit the plan to CommonwealthSecurity@vita.virginia.gov

2. How often must a risk assessment plan be submitted?

- Annually

3. Where do I find the risk assessment template?

- On the VITA website: http://vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/IT_Risk_Assessment_Plan_Template.docx

4. What if my agency does not have any sensitive IT systems?

- Send an email notification to CommonwealthSecurity@vita.virginia.gov that your agency does not have any sensitive IT systems, this email can serve in lieu of both the agency IT risk assessment plan as well as the agency IT security audit plan