LSA DIGITAL
Lean Scaled Architects

CASE STUDY

EXPOSING THE MOST IMPORTANT SECURITY VULNERABILITIES WITH EA INFRASTRUCTURE ANALYSIS

CONTEXT

As part of an Application and Infrastructure rationalization, LSA Digital helped a DoD agency to identify IT assets and recommend improvements. An important value outcome was the identification of key security risks to the infrastructure, and prioritization of remediation actions. Read more to learn how assets were identified and analyzed to focus resources on the most important risks.

CLIENT CHALLENGE

The client had multiple security enclaves and a complex set of IT infrastructure assets to support mission-specific applications and technology. Infrastructure redundancy and associated maintenance costs were a "technical debt" concern, but would take more effort to analyze and resolve. The top priority was to "stabilize" the environments, especially considering security impacts - and many of the environments had outdated, unpatched technology components.

OUR (AGILE) APPROACH

After understanding the pain points and priorities, we used an agile approach starting with one secure enclave environment - collecting and analyzing data to make better decisions about "where to put our time" to update IT assets.

SNAPSHOT

Ent. Architecture, Infra. Analysis, Cybersecurity

US Dept of Defense

ARIS

PAIN POINTS

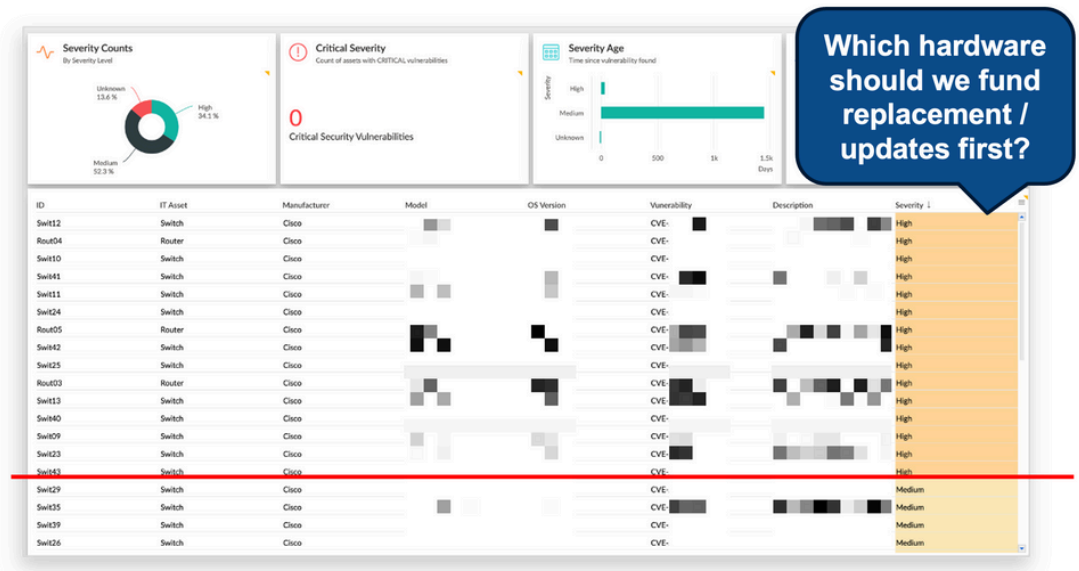
- Complex security enclaves containing outdated IT infrastructure equipment
- Growing technical debt and no data to evaluate infrastructure value

RESULTS

- Basic prioritization of resources to remediate the most immediate public CVE-advised security risks
- Improved, local-context prioritization through iterative learning, such as data sensitivity
- Re-usable asset library to improve IT Service Management with IT asset data - e.g., security risk trends

LSA DIGITAL
Case Study

In the secure enclave, we loaded the ARIS Enterprise Architecture repository (see our ARIS Platform case study) with all relevant infrastructure component inventory key data (e.g., router firmware version). We then combined this data with publically available CVE data, using a dashboard to highlight hot security vulnerabilities "in the wild" that put specific components at security risk (e.g., because of un-patched firmware).



ARIS
Digital EA repository & dashboard

RESULTS & BENEFITS

Leveraging a digital EA repository allowed for both immediate and scaled benefits:

- **Immediate prioritization** of resources to upgrade / patch existing equipment to avoid the most pressing security risks
- **Iterative approach and rapid lessons learned** to collect additional data for better prioritization (e.g., contextual data sensitivity)
- **Repository of re-usable assets** for other purposes - e.g., IT Service Management / ServiceNow CMDB for to understand a particular vendor's technology footprint and security risk trends, and technical debt

servicenow

WORDS OF ADVICE

The secure enclaves were "inside a secure perimeter", but from a Zero-Trust principled perspective, it's still important to prioritize patching the most important IT assets. While such security focused efforts can have important immediate benefits, it's also advised to evaluate the IT portfolio from its overall technical condition and business/mission value - and this can result in retiring of non-value adding IT equipment, lowering both security risk and technical debt at the same time (see our App Portfolio Rationalization case study).