imagineX consulting

Qualys

EASM Solution Service Offering

CSAM

Reduce Mean Time to Remediation with Qualys CSAM

CSAM 2.0

Protecting external attack surfaces is essential because these are the points at which an attacker can access an organization's systems, data, and networks. External attack surfaces can include websites, email systems, network connections, and mobile applications, among others.

CyberSecurity Asset Management (CSAM) is a cloud service that allows organizations to continuously discover, classify, remediate, and measurably improve their cybersecurity posture for internal and external IT assets before the attackers can — and with the same actionable intelligence that the attackers use. It discovers all known and previously unknown internet-facing assets for 100% visibility and improved cyber risk management.

Qualys CSAM 2.0 includes External Attack Surface Management, which adds "defense-in-depth" to update an organization's cybersecurity posture. It provides the ability to continuously discover and classify previously unknown assets with a Red Team-style asset and vulnerability management solution for full 360-degree coverage.

- Complete asset and software visibility across distributed hybrid environments
- Improve threat prioritization with asset criticality ratings (Reduce MTTR)
- Reduce technical debt with real-time EOL/EOS software tracking compliant with CISA guidelines
- Synchronized with CMDB for comprehensive inventory of managed and unmanaged assets

Why ImagineX

ImagineX Consulting pairs best-of-breed security products with boutique consulting services to deliver top-of-the-line security programs for our customers.

ImagineX has worked with top 500 enterprise firms to improve their Qualys implementations since 2016.

Our Qualys specialist consultants have over 50 years of collective experience as former Qualys employees and platform customers. We have a deep understanding of how to operate a successful vulnerability management program by maximizing people, processes, and technology.

ImagineX and Qualys

Our numbers speak for themselves

20+

IX employees who are Qualys alumni or former customers

35+

Qualys customers served

100+

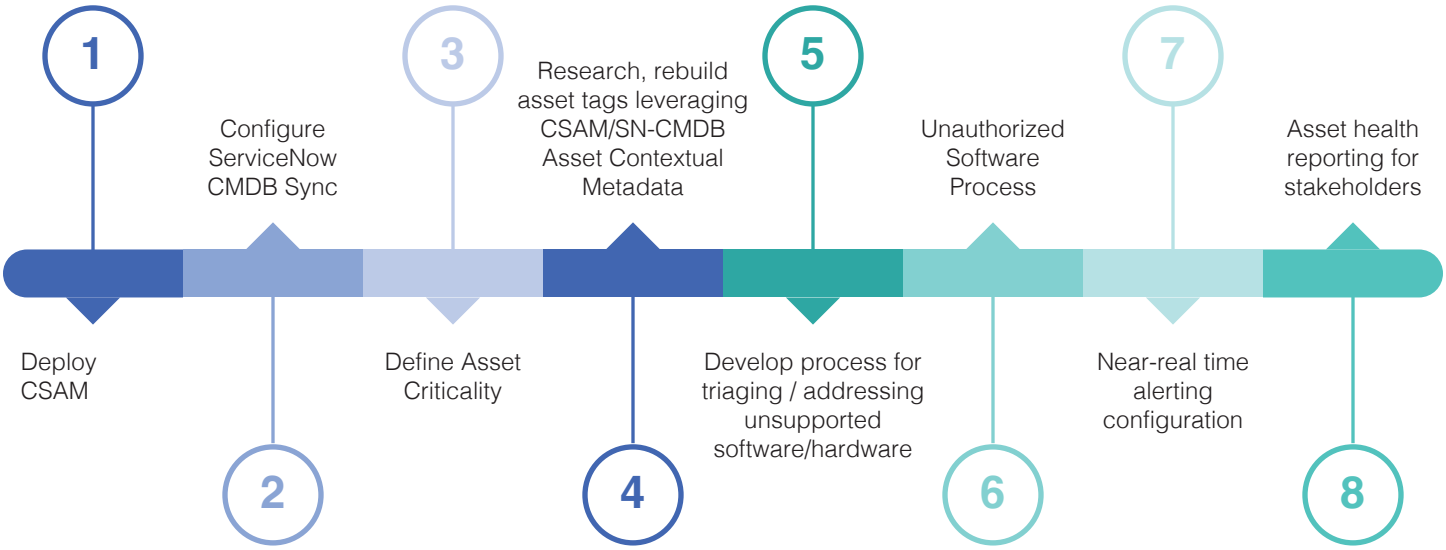
Qualys and Qualys-related projects

Learn more at www.imaginexconsulting.com/qualys or Qualys@imaginexconsulting.com

Methodology

An effective implementation of Qualys CyberSecurity Asset Management (CSAM) will enable organizations to manage their cybersecurity posture continuously. Steps in this methodology include: defining the assessment scope, configuring the CSAM platform and sensors, and analyzing data to identify cybersecurity issues. Remediation of any issues coupled with ongoing monitoring ensures that your environment remains secure.

8-Week Implementation Plan



IX CSAM SERVICES

We work with our client stakeholders, tailoring our services to address the specific needs of our clients in three key areas: Discovery, Detection, and Reporting.

Discovery and Inventory

- Architecture and deployment plan for multiple sensor implementation optimized for continuous discovery if IT, OT, and IoT assets
- Deploy cloud agents, scanners, cloud connectors, and container sensors
- Integration with Shodan.io for external attack surface management
- Normalize, categorize, and organize assets via tagging design and implementation
- Provide asset contextualization and criticality, threat intelligence, TruRisk and ServiceNow CMDB sync for risk prioritization

Detect and Monitor

- Setup tracking for authorized and unauthorized hardware, OS, and hardware product lifecycle information
- Configure the management of authorized and unauthorized software
- Establish detection for misconfigurations such as unsanctioned open ports, open servers, expired certs, and old applications

Report and Respond

- Configure IT health reports and dashboards
- Configure IT health alerts and responses to proactively manage EOL and EOS software