Deloitte.

Attack Surface Management

Collaborative Journey in Reducing Organizational Risk

April 2024

Attack Surface Management

Enabling secure operations—achieving mission success

Challenges

Vast threat exposure, limited resources. Inability to keep pace with remediation activities. Generative AI fueling more sophisticated cyberattacks.[1] Ransomware remains profitable.

Attackers are looking for ways to target hybrid and multi-cloud environments.[2]

Incomplete understanding of inventory, configurations and owners. Supply chains being exploited for the targeting third-party vendors to achieve their goals.[2]

Addressing the problem

Program Assessment, Audit, Design and Build

Deloitte designs and deploys industry leading Attack Surface Management (ASM) programs with a focus on helping clients understand their threat exposure.

Operationalization and Managed Services

Deloitte operates and continuously refines ASM programs, including either a managed service or in a collaborative model jointly with your organization.

Key Statistics

28,902 CVEs published[3], **87** zero-day vulnerabilities[4]

84% increase in ransomware attacks[5]

6,077 recorded data breaches (over **60%** within the U.S.[5])

1 in 4 organizations shut down OT cyber attack[6]

Hackers scan for vulnerabilities within **15 minutes** of disclosure[7] while on average, the mean time to remediate (MTTR) is **58 days**[8]

84% of organizations have network perimeter high-risk vulnerabilities[8]

Approximately **40%** of attacks on OT environments resulted from compromised IT systems that allowed attackers into OT/ICS networks[9]

Services

Governance, Compliance, Reporting

Program policy, standard and procedures | Remediation service level agreements (SLAs) | Communications plan | Operational model | Runbooks | Secure baseline configurations | Service metrics | Reporting

Vulnerability Management

Attack surface, vulnerability, and maturity assessments | Deploy, configure and manage technology solutions | Asset intelligence | Vulnerability risk quantification and prioritization | Remediation validation | End-of-life tracking

Remediation Management

Qualification, testing, packaging | Change management | Remediation scheduling | Remediation deployment

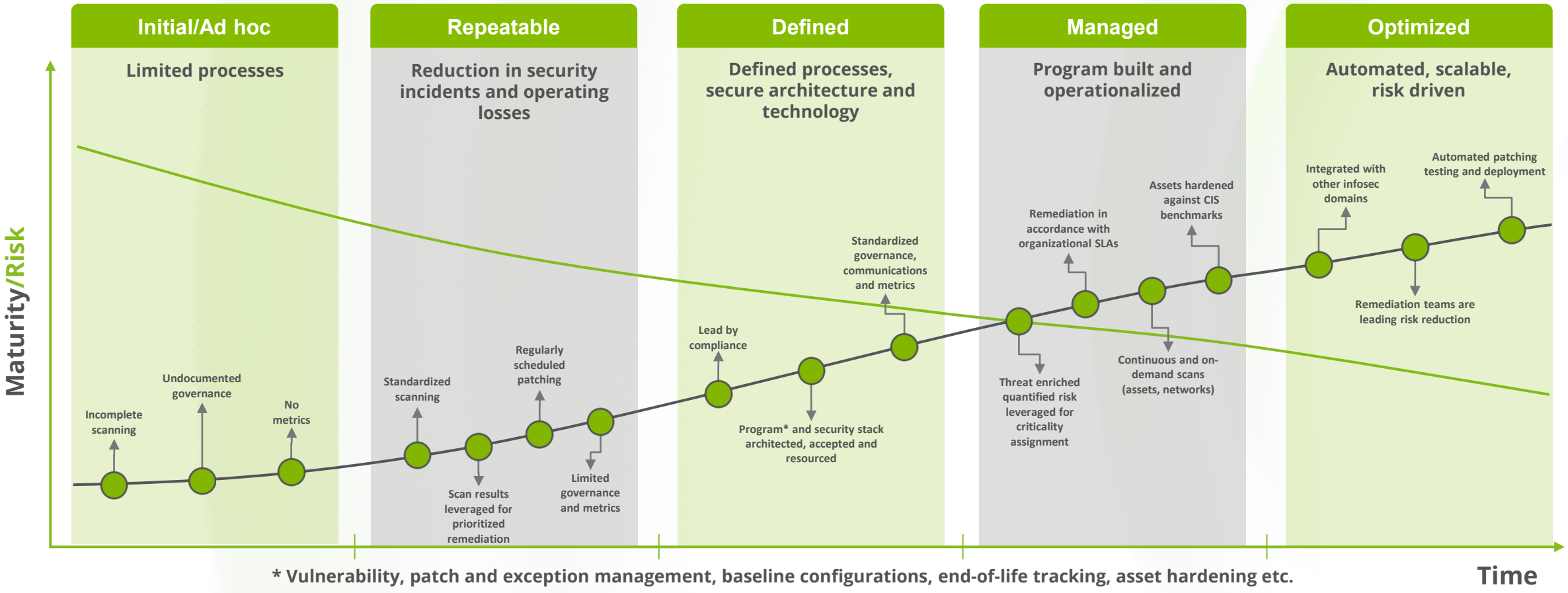
Outcomes

- Change the conversation from the boardroom to the business units
- Bridge business, IT and security teams
- Increase situational awareness, vigilance, workflow automation, collaboration and threat focused risk reduction
- Reduce uncertainty, and impact on organizational staff, decreasing the Mean-Time-to-Remediate

[1] https://antidos.com/blog/7-reasons-why-generative-ai-is-fueling-cyberattacks/
[2] https://www.informationweek.com/cyber-resilience/7-security-trends-to-watch-heading-into-__2024?_mc=NL_IWK_EDT__20231219&cid=NL_IWK_EDT__20231219&sp_aid=120002&elq_cid=24980267&sp_eh=3c3b81__5e97263d1b5fab05cdcabecf625616be7cfb90782e2bb5fd5b4db389d8&sp_eh=3c3
[3] Browse cve vulnerabilities by date (cvedetails.com)
[4] https://www.securityweek.com/vulnerability-handling-in-2023-28000-new-cves-84-new-cnas/
[5] https://www.securityweek.com/threat-indicators-show-2024-is-already-promising-to-be-worse-than-2023/
[6] https://www.securityweek.com/1-in-4-organizations-shut-down-ot-operations-due-to-cyberattacks-survey/
[7] https://www.bleepingcomputer.com/news/security/hackers-scan-for-vulnerabilities-within-15-minutes-of-disclosure/
[8] 25+ Cyber Security Vulnerability Statistics and Facts of 2023 (comparitech.com)
[9] Why the manufacturing sector must make zero trust a top priority in 2023 (venturebeat.com)

Operational capability maturity model

Evolutionary path for increasing organizational effectiveness and performance



Beginning a maturity journey first begins with understanding. The ASM capability maturity model provides organizations an objective understanding of current maturity while providing a reference plan looking to add and enhance operational capabilities throughout the ASM lifecycle, both on-premise and in the cloud.

The ASM lifecycle

Promoting a logical and careful approach in managing an organization's attack surface

Understand

- Environment, inventory, asset priorities, and stakeholders
- Security stack capabilities, and configurations

Assess

- Multiple source vulnerability identification
- Triage vulnerabilities, testing, and assigning criticality severity rating

Address

- Ratify remediation activities addressed identified vulnerabilities
- Remediate vulnerabilities (e.g., patching, configurations)

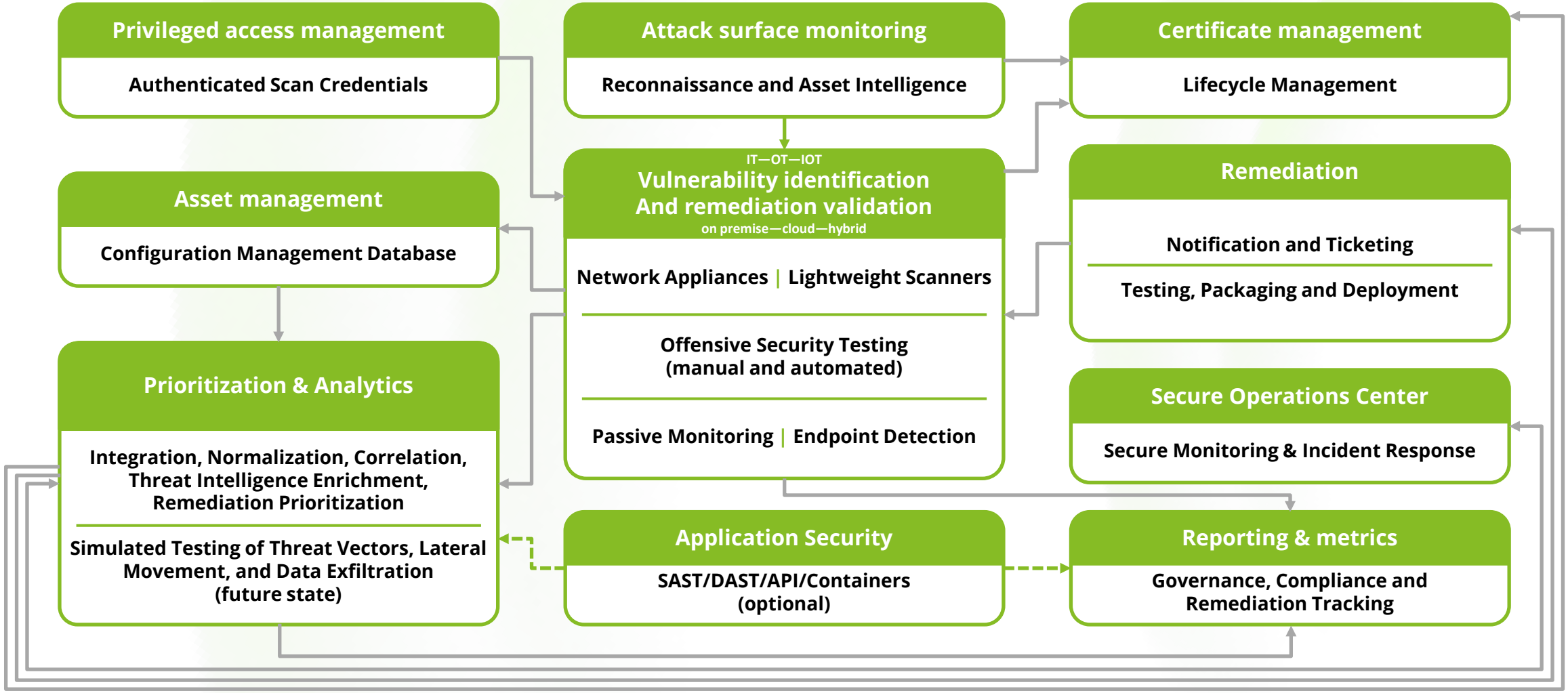
Inform

- Notification prompting risk reduction activities
- Ongoing stakeholder collaboration, reporting and metrics

Our methodology is based on industry leading and standardized, repeatable practices, and through our experience helping clients reduce risk throughout the lifecycle.

Illustrative reference architecture

A broad attack surface architecture facilitates automation and decreases mean-time-to-harden



Cybersecurity architectures are often overlooked, loosely coupled, or unmanaged, resulting in organizations not being able to properly understand, monitor, or defend their attack surface. Conversely, mature ASM architectures go beyond traditional vulnerability scanning and patching solutions, leveraging a strong-unified technology stack for discovery, vulnerability identification, threat enriched prioritization, and tailored reporting.

 |

Start the conversation

Our team of seasoned and skilled professionals provide cross-industry experience and insights

Andrew Douglas

Managing Director
Deloitte & Touche LLP
andouglas@deloitte.com

Chuck Littmann

Managing Director
Deloitte & Touche LLP
clittmann@deloitte.com

Tucker Pettis

Senior Manager
Deloitte & Touche LLP
tpettis@deloitte.com

We have strong leadership and provide an evolving, dynamic team with a focus on providing an insightful, collaborative, and results-driven experience for our clients by helping them reduce the risk of a cyber breach.

Deloitte.

Thank you.