



Advanced Enterprise Vulnerability Management Overview

Achieving Enterprise Cyber Vigilance

March 2023

Advanced Enterprise Vulnerability Management

Hosted by the BSides Sofia team



Evgeni Sabev
Attack Surface Reduction Team
at SAP SE

Agenda

Topics	Time (40 mins)
Definitions and Statistics	3 mins
Attack Surface	2 mins
EVM 101 – Bad Habits, Caveats, DO's and DON'Ts	15 mins
Advanced Vulnerability Management – One EVM View	10 mins
Roadmap to Successful EVM Program	5 mins
Q&A	5 mins

Definitions

Great vulnerability management is often hard to quantify, as the best measure of its success is that which never happens

Definitions

“Vulnerability management (VM) is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities”

- Park Foreman

“Good vulnerability management is the process of identifying, evaluating, prioritizing and mitigating vulnerabilities in a timely and effective manner to reduce the risk of exploitation”

- ChatGPT

Definitions

Vulnerability management is not just running a vulnerability assessment scanner!

Definitions

“Using vulnerability scanners to identify unpatched software is no longer enough. Keeping devices, networks, and digital assets safe takes a much broader, risk-based vulnerability management strategy – one that includes vulnerability assessment and mitigation actions that touch the entire ecosystem.”

- Balbix

Definitions

“Unlike legacy vulnerability management, risk-based vulnerability management goes beyond just discovering vulnerabilities. It helps you understand vulnerability risks with threat context and insight into potential business impact.”

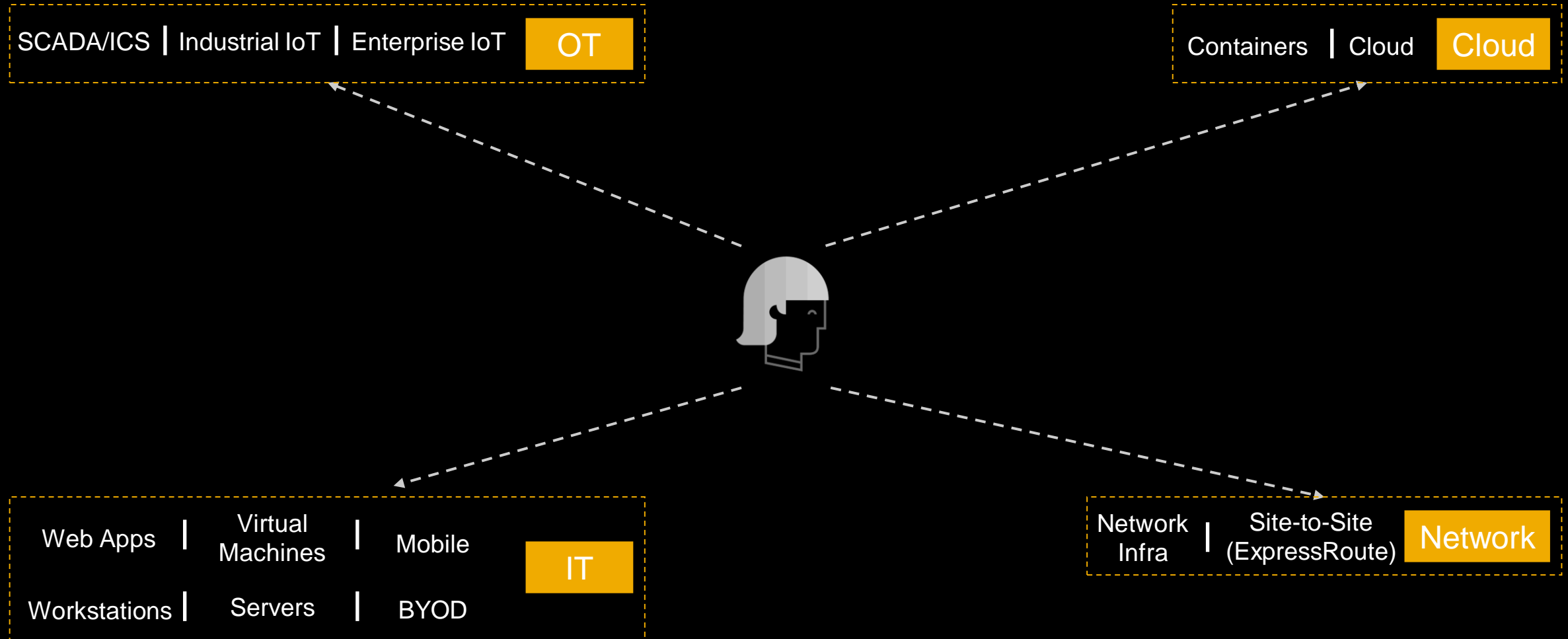
- Tenable

Hidden Truth



Attack Surface is Dramatically Expanding

Through constant application, network, technology addition



How to Start Your EVM Program and Advance it

Companies struggle to start their own EVM program and advance it



Organization

Understand the organization's environment

What is the software fingerprint on **each asset**
What % is SaaS and Cloud?
What about On-Prem?
Understand the High Level Network Architecture -> detect potential **Shadow IT** gaps



Organizational Lifecycle

Companies are constantly growing and changing their portfolio

How are **assets / software / technologies** introduced to the organizational environment?
Change Management?
M&As onboarding -> **runbooks** from global security



Organizational Complexities

Large companies tend to have very complex budgeting

Unite with **Global Procurement** and make them best friend
Follow the spending by **cost centers** to **detect** and **predict** new technologies and assets before they have been added to the environment

Bad Habits, Caveats

Deep-dive



Vulnerability Management is a stakeholder-centric process. Multiple stakeholders, tools, processes, and priorities need to be accommodated and aligned to achieve one common goal. The EVM Engineer should have the ability to influence and help the business to create realistic patching mechanisms and timelines. Also they would need to know when to push and when to protect the business units

Bad Habits

- ✍ People tend to email Vulnerability assessments. Don't do that it should be flagged as Confidential information from your Information Classification Program
- ✍ Don't create a culture of exceptions
- ✍ Lack of EVM program backup by Policy and Standards
- ✍ Not giving credits and appreciation to the Ops/Devs Teams – incl KPIs
- ✍ No Senior Leadership Team (SLT) buy-in
- ✍ Lack of tabletop exercises to simulate response to emergency

Caveats

- ✗ Every VA* tool is different and might produce different results
- ✗ Not every tool can cover all technologies, you might need different tools
- ✗ Every VA tool is reporting differently! Don't just add up numbers from different tools!
- ✗ Everyone sees the technology stack through their own understanding:
 - Executives -> Business Risk
 - Developers -> packages/libraries
 - Administrators -> configurations/updates/patches
 - Security -> vulnerabilities/exploits

Central Asset Management Platform

Deep-dive

DOs



Keep all the Information around assets on a central asset management



Have a complete asset information which includes at least the following:

- Asset Criticality
- Asset Location
- Internet facing or Internal
- Business purpose of the asset
- Deployment stage – PROD, TEST, QA
- Regulatory requirements – KRITIS, GDPR (PII), HIPAA (PHI)

DON'Ts



Use the VA for asset management




Example Issues/Exploitations

- Shadow IT begins to grow.
- Users plugin personal devices into the network.
- Remediation efforts are not directed towards key assets first.




Patching

Deep-dive

DOs

-  Adopt regular patching cadence
-  Consider remediations that cause less fatigue and dread
-  Utilize risk score card that considers:
 - Age
 - Assets Criticality
 - Exploit Maturity and Public Availability*

DON'Ts

-  Patch only when its urgent and a vuln is considered emergency
-  Try reduce count of vulns only by number
-  Prioritize only based on CVSS

*Exploit Prediction Scoring System (EPSS) - <https://www.first.org/epss/>

Scanning Architecture and Frequency

Deep-dive

DOs

- ✔ Carefully perform PoC of each type of target systems to ensure business continuity
- ✔ Deploy enough scanners / consider target resources
- ✔ Monitor the scanner/agents resources to ensure full scanning is always completed
- ✔ If environments are fully agent based still consider starting discovery scans to detect orphans and have uncredentialed network scans
- ✔ Consider scanning with Agents and Scanners **(Note: This might lead to double licensing the same asset)**
- ✔ Don't trust asset management by default
- ✔ Let the BUs to define the most suitable during the week to be scanned
- ✔ Scan weekly or even daily where possible



DON'Ts

- ✗ Follow the guidelines for minimum resources by deployment of VA solutions
- ✗ Ignore the network bandwidth
- ✗ Share scanners for multiple BUs
- ✗ Scan only once per month
- ✗ Use default template and un finetuned scans
- ✗ Leave less "critical" systems unscanned – e.g. Printers, IP Cameras, RFID readers
- ✗ Only scan a static list provided by BU
- ✗ Assume all Agents are always up-to-date


Credentialed vs Non-credentialed Scans

Deep-dive

DOs

-  Use keys/certificates
-  Monitor authentication failures to ensure full scans

DON'Ts

-  Use passwords

Exceptions

Deep-dive

DOs

- ✔ Understand the current Risk Management Process of the company
- ✔ Plug in to already existing and approved Risk Management Process
- ✔ Create a status of each unique vulnerability per asset
- ✔ Create a review process for all exception
- ✔ Automate the exception process

DON'Ts

- ✗ Remove any vulns from the reporting
- ✗ Exclude all assets, all ranges due to issues with only one asset
- ✗ Exclude an asset if particular port is causing issues
- ✗ Grand permanent exception -> always set timeframes
- ✗ Consider a mitigation control is going to last forever*

*<https://www.darkreading.com/application-security/ransomware-attackers-bypass-microsoft-mitigation-proxynotshell-exploit>

Reporting only with Defined Ownership

Deep-dive

DOs

- ✔ Define and document in central asset management explicit the ownership for each software type that resides on a system: App1 owner, App2 owner, DB owner, OS owner
- ✔ Identify Patch Management gaps
- ✔ Organize the scopes based on groups/BUs with tags
- ✔ Create RACI and define accountability and how it will be tracked –
- ✔ Software Bill of Materials – and defined ownership of each library/component – helps in cases like Log4Shell

DON'Ts

- ✗ Send reports as CSV/XLSX via email !!!
- ✗ Assume ownership based on verbal appointing
- ✗ Send emails to everyone just because you can
- ✗ Send email for each single vulnerability

SLAs/TRTs

Deep-dive

DOs

- ✔ Define different types of TRTs for the each asset class
- ✔ Set the TRTs based on the company maturity - force the spirit not the letter in non mature programs
- ✔ Define the TRT per asset/app importance and criticality

DON'Ts

- ✗ Set the same TRTs for everyone
- ✗ Depend on patch availability
- ✗ Start with too harsh TRTs

Container Scanning

Deep-dive

DOs

- ✓ Scan containers regularly like everything else
- ✓ Shift security left -> Scan the base container images
- ✓ Consider them as immutable -> Garden Linux
- ✓ Instantiate clear labeling on who builds the image for owner tracking

DON'Ts

- ✗ Exclude containers from scanning
- ✗ Consider containers are secure by default
- ✗ Treat like VMs and deploy agents/scanners

Web App Scanning

Deep-dive

DOs

- ✓ Integrate into EVM program
- ✓ Scan for basics XSS, SQLi, etc
- ✓ Fine tune each scan – no two web apps are the same

DON'Ts

- ✗ Assume all SaaS are allowed to be scanned

Compliance Scans

Deep-dive

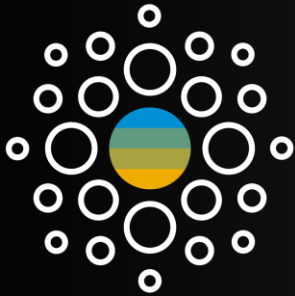
DOs

- ✓ Use already existing frameworks - ISO27001, NIST, CIS
- ✓ Fine tune for specific environment

DON'Ts

- ✗ Assume compliance scans cover vulnerability topics
- ✗ Neglect them completely as they could potential reduce the attack surface

Threat Intelligence



VULNERABILITY EXPLOITATION STATUS

Wild | Weaponized | Complexity



EXPLOITATION IN THE WILD

APTs | Governments | Hacktivists

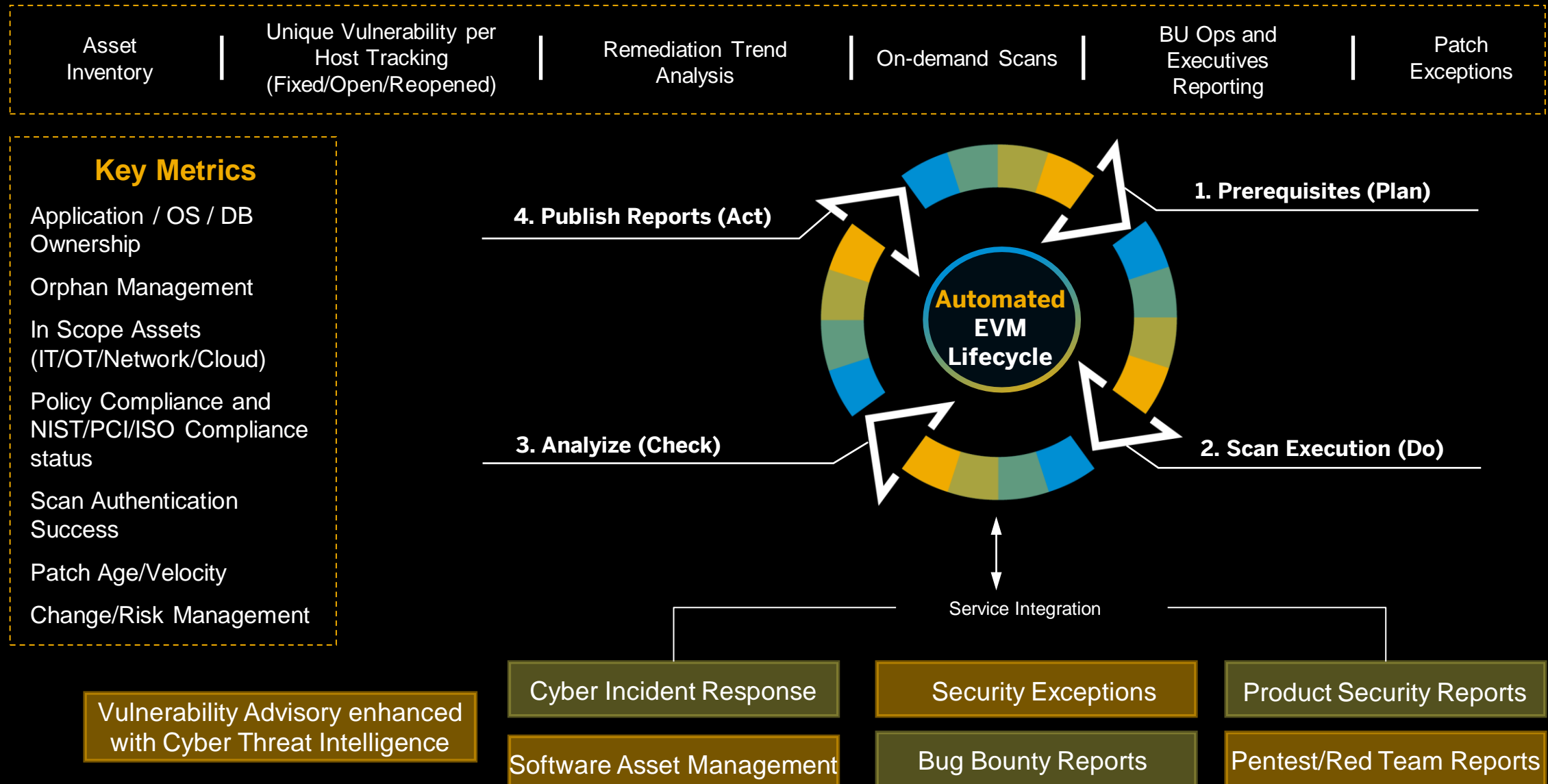


DELIVER THREAT INTELLIGENCE

Integrated | Filtered | Mitigation

Take advantage of cyber threat intelligence and consolidate data directly to BUs reporting to drive valuable insights and remediation efficiency.

Advanced Vulnerability Management – One EVM View



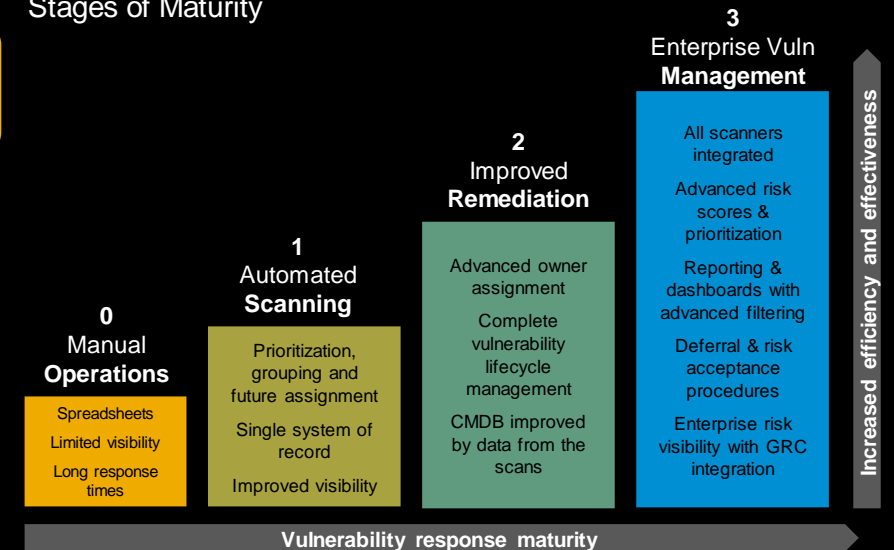
Advanced Vulnerability Management – One EVM View (Continued)



The benefits of having advanced enterprise vulnerability management program are:

- Faster implementation and time to value
- Awareness of key security risks and guidance to mitigate them
- Enhanced efficiency and quality of the scanning results
- Clear ownership definition that reduces reaction time to minimum
- Single system of record and dashboard for all BUs

Advanced Enterprise Vulnerability Management Stages of Maturity



Key steps

1. Set VM vision and outcomes
2. Assess team readiness
3. Choose an implementation partner
4. Plan for implementation
5. Design, build, and test scanning
6. Implement all scanners
7. Plan go-live
8. Analyze results and mitigate/remediate

Roadmap to Successful EVM Program



1 | OPERATIONAL ALIGNMENT

Align the operational teams and their executives. Align the processes needed to work together, such as available headcount, budgeting, KPIs and dashboards



2 | PEOPLE ALIGNMENT

Align organizational structures, roles and career paths



3 | TOOL AND PROCESS ALIGNMENT

Align different tools, processes, strategic programs and timelines

Q&A and Thank you.

Contact information:



SAP SE
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany

Evgeni Sabev
Attack Surface Reduction Team