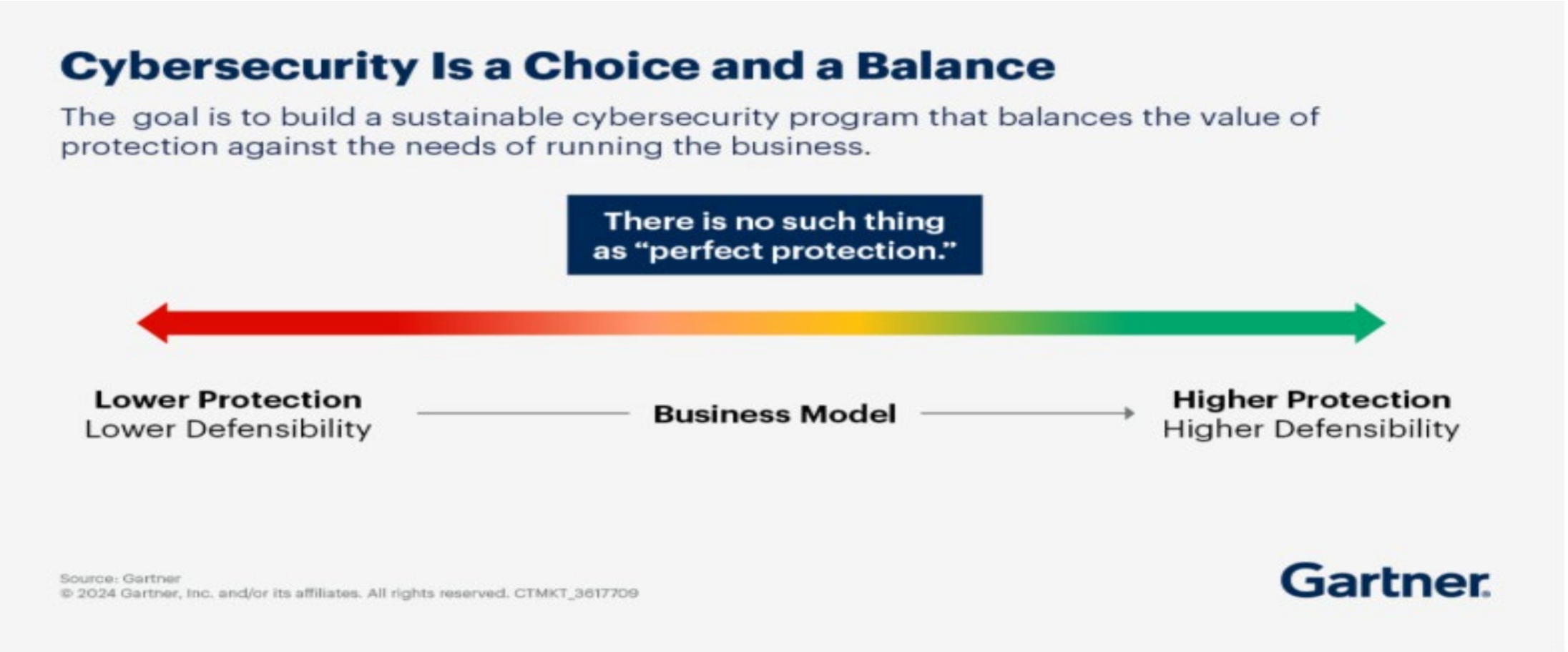
Mainframe Penetration Testing 101: A Critical Layer in Vulnerability Mgmt.

Ray Overby

Distinguished Engineer, Security

Rocket® software

Cybersecurity: It is a Strategic Choice



https://emt.gartnerweb.com/ngw/globalassets/en/cybersecurity/images/infographics/cybersecurity-is-a-choice-and-a-balance.png

Mainframe Pen Testing: What are the Components

Code & Configuration

At the operating system layer you are looking at code

- SVC's
- PC Routines
- APF Libraries
- Home-grown exits that make SAF calls

The configurations you should be looking at are:

- Security parameters in 3rd party products
- ESM's (RACF, CA ACF2, CA Top Secret)
- Hardware configurations
- IPL parameters
- Over privileging
- Excessive access
- APF Libraries

- Security Policy Mgmt.
- Change Mgmt. Procedures
- Patch Mgmt. Procedures
- Resi;ency

Evolving Regulation's

- **PCI DSS Requirement 11.3 addresses penetration testing, which is different than the external and internal vulnerability assessments required by PCI DSS Requirement 11.2.**

- **Annual penetration testing is required under CA-8 of NIST SP 800-53 and is mandatory for FedRAMP authorization.**

Why is Mainframe

Pen Testing so Important

It takes 20 years to build a reputation, and five minutes to ruin it.

WARREN BUFFET

Mainframe penetration testing is a critical, proactive security process that simulates real-world attacks (e.g., RACF, z/OS, TN3270) to identify and exploit vulnerabilities.

It is a manual process with the use of tools provided by the Pen Tester.

It should be done by individuals who have an in-depth understanding of z/OS, security intercepts and the External Security Manager you are using (CA ACF2, RACF, CA Top Secret).

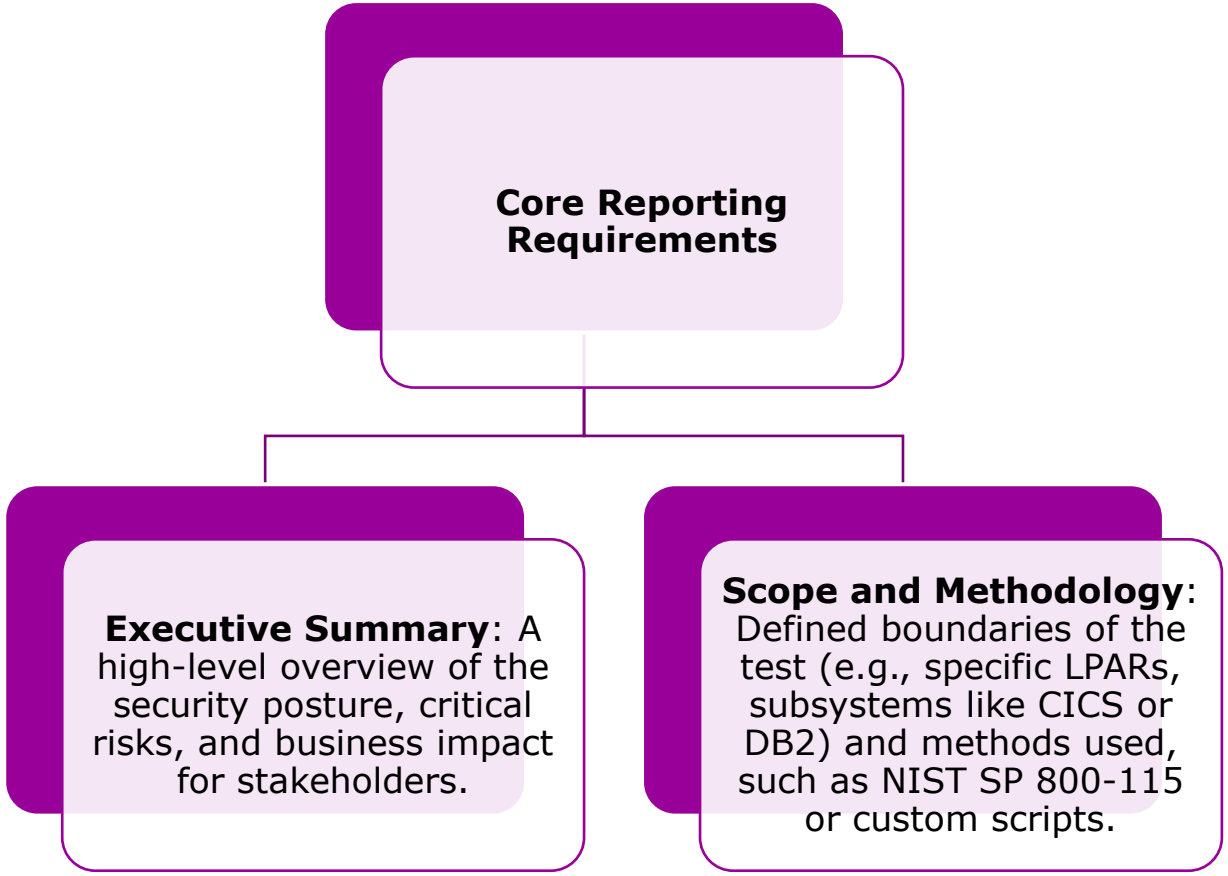
Reporting?

- Mainframe penetration testing reports must deliver actionable, risk-ranked findings focusing on z/OS security, ESM configurations, and privileged access.

- Key requirements include detailed vulnerability descriptions, proof-of-concept exploit steps, remediation plans, and alignment with compliance standards (PCI DSS, NIST, ISO 27001).

- Reports should be encrypted, secure, and include a clear scope and executive summary for remediation.

Reporting?



Reporting?

- **Detailed Findings & Risk Assessment:** A categorized list of vulnerabilities (High, Medium, Low) with evidence, such as:
  - **RACF/Security Server Misconfigurations:** Over-privileged users, weak identity mgmt., or improperly protected datasets.
  - **Subsystem Vulnerabilities:** Weaknesses in CICS, IMS, or DB2.
  - **TSO/USS Exploitation:** Misconfigurations allowing privilege escalation.

Reporting?

- **Remediation Recommendations:** Specific, actionable advice to fix findings, including configuration changes or patching.

- **Compliance Mapping:** Documentation linking findings to regulatory requirements (e.g., HIPAA, PCI DSS, NIST, DORA) at the request of the customer.

Reporting?

- **Confidentiality & Control:** Reports must contain a confidentiality statement, a controlled access list, and be delivered via secure, encrypted methods.
- **Evidence of Testing:** Detailed logs or screenshots showing how vulnerabilities were identified or exploited.
- **Periodic Review:** Reports should reflect regular (e.g., annual) testing, particularly after significant system changes.

Mainframe Penetration Testing Critical Exposures List

Authorization

Access Control Misconfigurations:

Profile configurations in (RACF/Top Secret/ACF2) often allow users to access unauthorized data.

Authentication

Privilege Escalation:

Vulnerabilities often enable standard users to gain elevated rights, such as APF (Authorized Program Facility) authorization or supervisor state (SVC).

Code Based Vulnerabilities

Unpatched Software/Legacy Systems:

Outdated operating systems and software components leave known, unpatched vulnerabilities exposed

Thank you

roverby@rocketsoftware.com

Rocket® software