Anatomy of a Mainframe Hack (And How to Defend Against Them!)

Ray Overby, CTO and Co-Founder, Key Resources Inc
Christopher Perry, Lead Product Manager, BMC AMI For Security

We asked: What are your top five mainframe priorities for the next year?

95% say the most concerning ramification of mainframe security is a breach of customer data.

1) Data Breach Prevention

2) Compliance

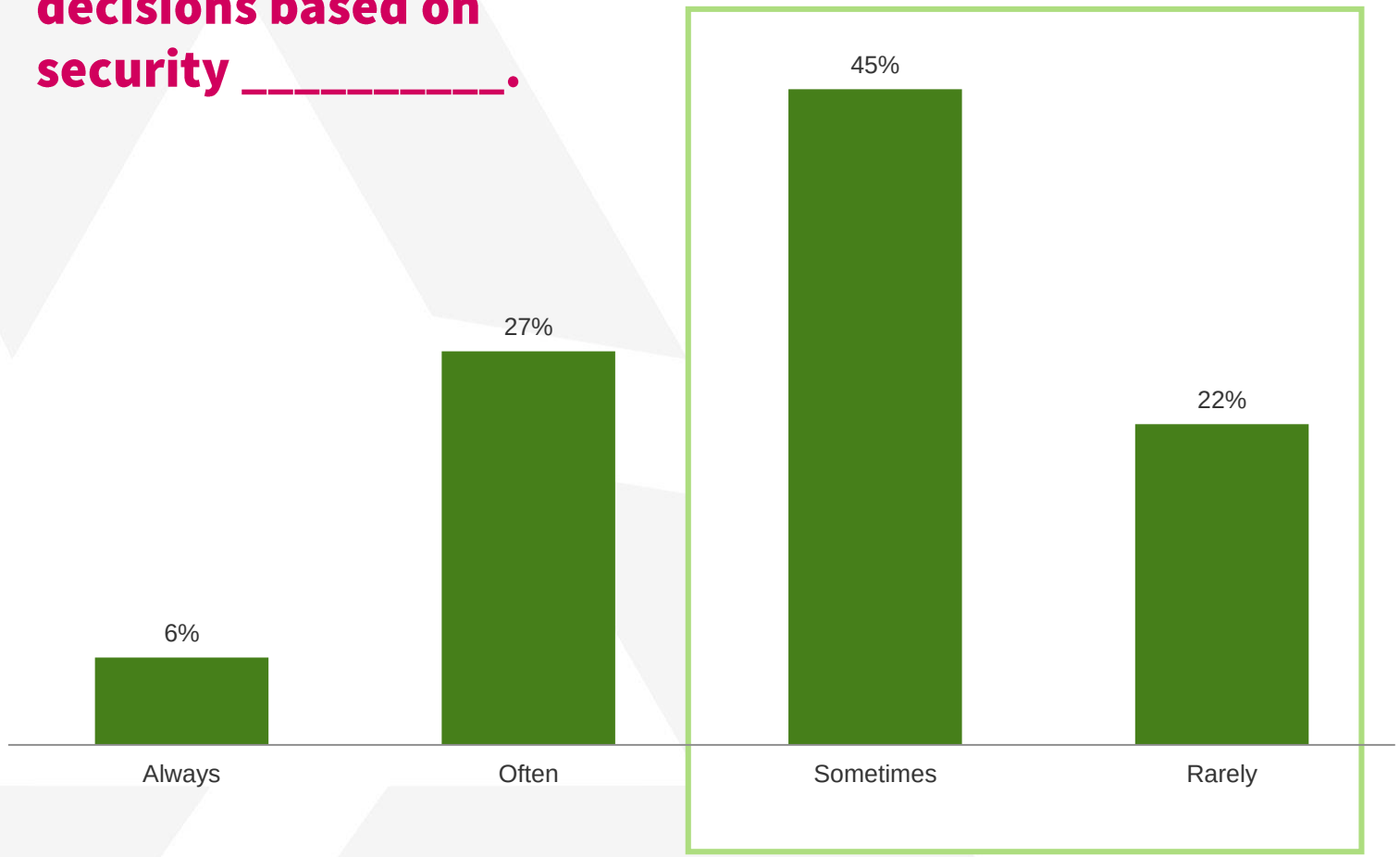
3) Risk Management

4) IT Cost Reduction / Optimization

5) Application Availability

Although 85% say mainframe security is a top priority (Q1), 67% of companies only either sometimes or rarely make mainframe decisions based on security.

My team and I make mainframe environment changes or process decisions based on security _____.



Source: “KRI Opportunity Snapshot”, a commissioned study conducted by Forrester Consulting on behalf of KRI, February 2019

Myth 1

SHARE
EDUCATE • NETWORK • INFLUENCE

“We don’t really need extra security because our mainframe is behind the firewall”

- Head of Mainframe Operations

Myth 2

“I’m not worried, we use RACF to secure our users and datasets from malicious threats"

- Senior System Programmer

Myth 3

“Only two of my most loyal sysprogs have access to system datasets, I trust them.”

- Head of Mainframe Operations

Mainframe Attack Surface

External Threat

Customer Information Control System (CICS)

HTTP (and Shadow Web Server)

Network Job Entry (NJE)

File Transfer Protocol (FTP)

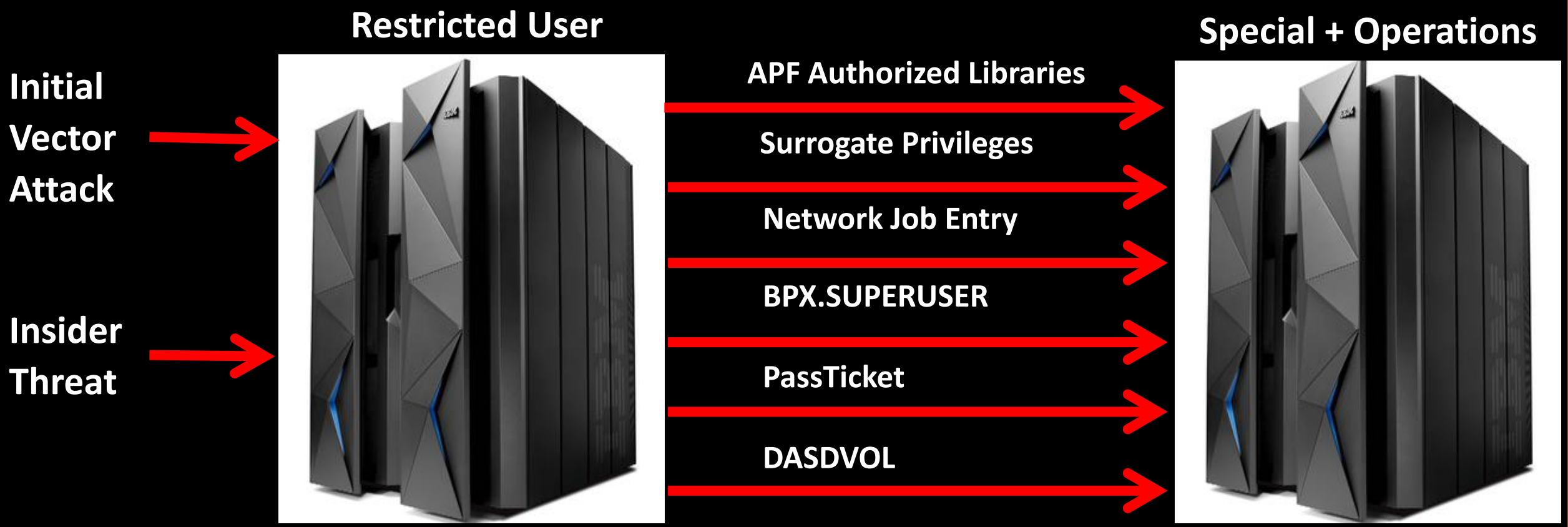
Secure Shell (SSH)

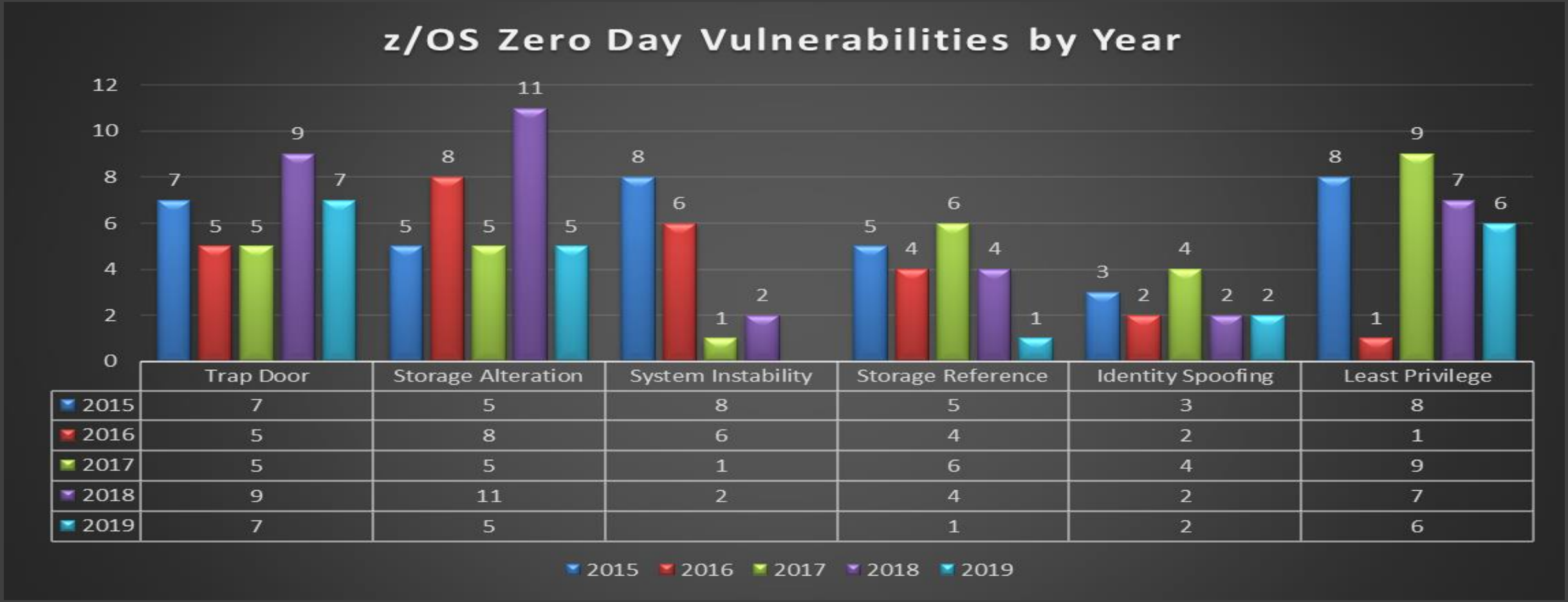
TN3270

Initial Access

Every service running on your mainframe is a potential vector for a threat actor to use to compromise the system.

Privilege Escalation On z/OS





The Scariest – Software vulnerabilities

- ❑ New Software Vulnerabilities by Year and Category
- ❑ These are the ones KRI found; not all of them
- ❑ There will always be vulnerabilities as long as humans are writing code

Myth 4

“If hacking a mainframe is so possible then why has it never happened before?"

- VP of Mainframe

Real-Life Mainframe Attacks

NEWS

Pirate Bay co-founder charged with hacking IBM mainframes, stealing money

By Loek Essers

Amsterdam Correspondent, IDG News Service | APR 16, 2013 9:05 AM PT

Gottfrid Svartholm Warg and three associates were charged with hacking the mainframes of the Swedish IT Firm Logica and the Nordea Bank and stealing over 800K.

Only caught because greed in transferring too large a sum of money triggered a flag, not because of IT security solutions

Unnamed Bank victim of first known case of mainframe ransomware

A bank fell victim to a ransomware in a 4 part attack:

1 – Spear Phishing attack against system programmers of the mainframe

2 – Keylogged their windows computer to pilfer mainframe credentials

3 – Submit a JCL job through FTP to scan for sensitive datasets

4 – Submit a second JCL job through FTP to encrypt datasets with custom ransomware

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

“Alright, you have my attention. So how do I defend against these threats?”

- Most of you, probably

National Institute of Standards and Technology (NIST) Cyber Security Framework

In order to effectively defend your mainframe you need to be able to effectively accomplish ALL 5 steps of the NIST model for every computer on your network – especially the mainframe

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management
- Strategy

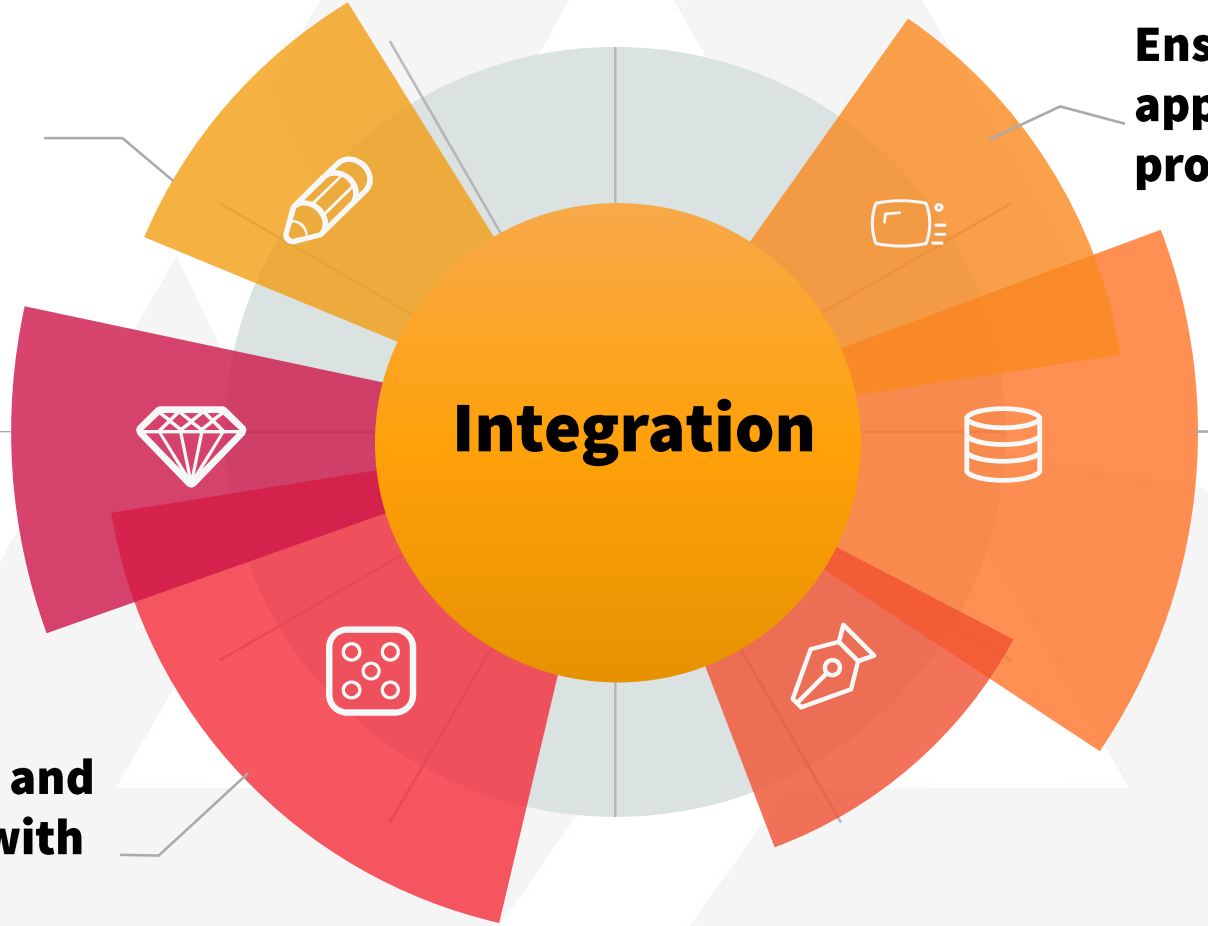
Reasons why a mainframe security architect is essential and what their role entails.

SHARE
EDUCATE • NETWORK • INFLUENCE

Continually review and enhance current security policy and procedures based on standards.

Review the security policy and procedures to take advantage of new ESM features

Ensure new applications and software that interface with MF do not compromise individual accountability.



Ensure Integrity – choosing the appropriate security tools and processes.

Ensure coverage by implementing new ESM security interfaces.

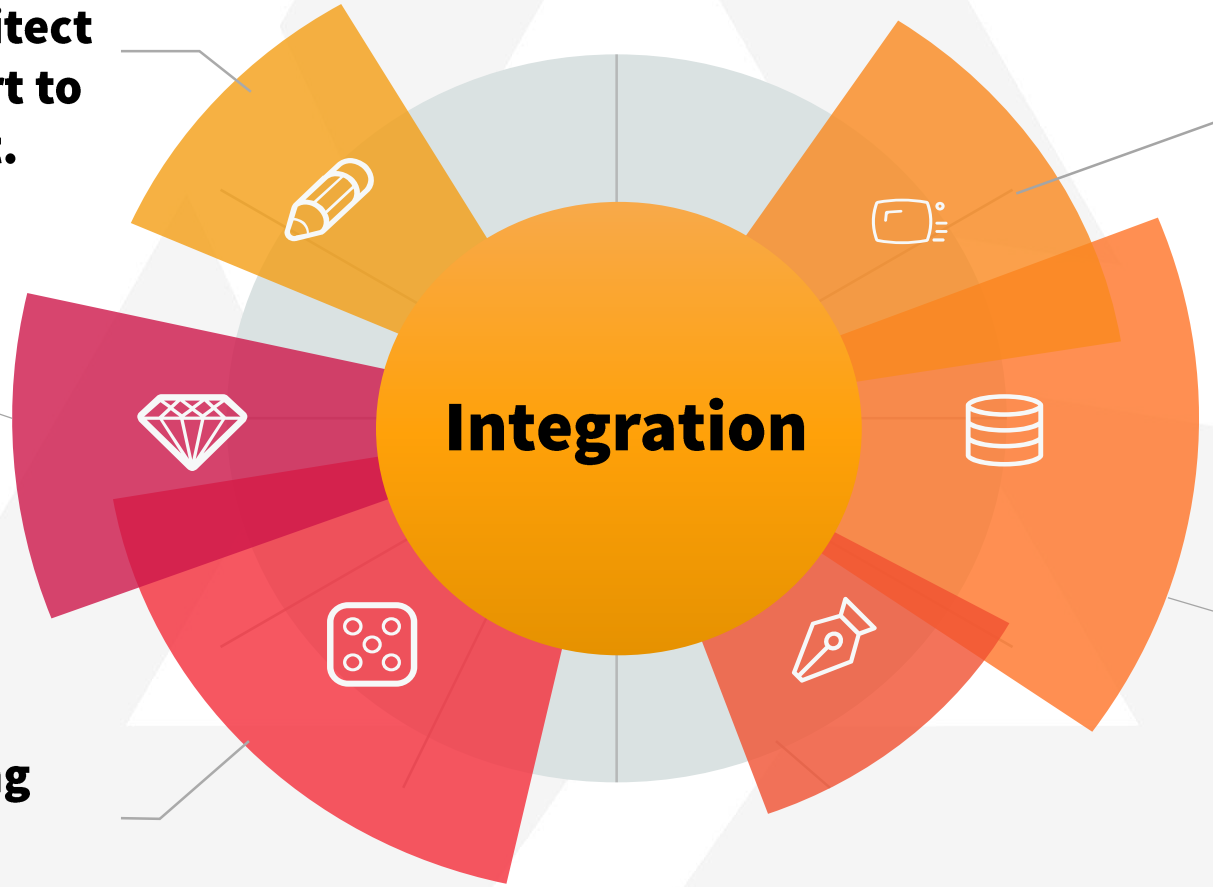
Reasons why a mainframe security architect is essential and what their role entails.

SHARE
EDUCATE • NETWORK • INFLUENCE

MF Security Architect should NOT report to Operations Mgmt.

MF Security Architect is a good example of where the separation of function is critical.

Security Architect responsible for designing and choosing the appropriate tools.



With the integration of platforms, with security high on the agenda, the organization needs an individual that understands both worlds.

Data ownership is NOT the responsibility of the Security Architect, nor Operations.

Why Separation of Function?

- Correct SoF is designed to ensure that individuals are not responsible for reporting on themselves or their manager(s). SoF, as it relates to security, has two primary objectives:
  - The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors.
  - The second is the detection of control failures that include security breaches, information theft and circumvention of security controls.
- New regulations such as GDPR now require that you pay more attention to roles and duties on your security team.
- The person(s) responsible for designing MF security must not be the same as the person(s) responsible for implementing, testing, conducting audits, or monitoring and reporting on MF security.
- The reporting relationship of the individual responsible for MF security should no longer be to the CIO, as has traditionally been the case.

Why Separation of Function?

- Possible Solutions as defined by GDPR:
  - Have an individual responsible for ALL of Information Security report to chairman of the audit committee.
  - Use a third party to monitor security, conduct surprise security audits and security testing. The reports go to the board of directors or the chairman of the audit committee.
- A CISO, responsible for all information security, who reports to the board of directors.
- A CISO report to internal audit, as long as internal audit does not report thru the CFO.

Protect

- Access Control
- Awareness & Training
- Data Security
- Info Protection Process & Procedures
- Maintenance
- Protective Technology

Understanding the risks of not including excessive access checking in your security check processing.

- It's a matter of compliance – DISA STIGS requires government agencies to do excessive access checking (EAC).
- In a fashion GDPR now requires corporations to do EAC. Some organizations are averse to excessive access checking. These checks can uncover hundreds of thousands of findings, which the organization then must address.
- Doing manual excessive access checking finds which groups have access to data sets or resources, but you don't drill down to the user level. So, you won't know if there's a user in a group who shouldn't have access.
- Automation drills down into the detailed level of what people have access to, dramatically reducing the time it takes to verify compliance. Automation can help your organization stay on the right track, so you don't suddenly find 250,000+ issues to resolve at once.

Understanding the risks of not including excessive access checking in your security check processing.

- The new GDPR regulations require data ownership. This entails knowing who owns the data, who gave approvals to access the data, and who has access to your data.
- Security should not be making access decisions. They do NOT own the data.
- This access must be periodically reviewed as defined by your security policy.
- The point is that as excessive access increases, so do the risks to the organization.

Why scan BOTH application and operating system code?

Application and vendor software releases are hurried with less testing; developers do not always have the skillset necessary to write integrity-based software. Let's face it. Software has holes; not just distributed software.

IBM's System Integrity architecture is the reason mainframes are highly secure, but vulnerabilities in OS level code will allow breaches (without the Enterprise Security Manager (ESM) issuing any type of log entry or warning).

Without integrity you cannot have security; once the OS layer is breached the hacker has access to all data and all application layer code.....

ESM's: RACF, CA ACF2, and CA Top Secret are essential for establishing permissions and access control, but they were not architected to protect against operating system integrity vulnerabilities.

Differences between Distributed and Mainframe Pen Testing and Vulnerability Scanning

SHARE
EDUCATE • NETWORK • INFLUENCE

Mainframe Pen Testing

Mainframe pen testing is specifically focused on finding ways to elevate standard user privileges, gain access without permission, or exfiltrate data, by looking for vulnerabilities in the hardware/infrastructure and software.

Standards Definition of Vulnerability Scanning

The Standard definition of vulnerability scanning: Search for known vulnerabilities, be they misconfigurations, missing patches, weak versions of crypto, and default or weak passwords.

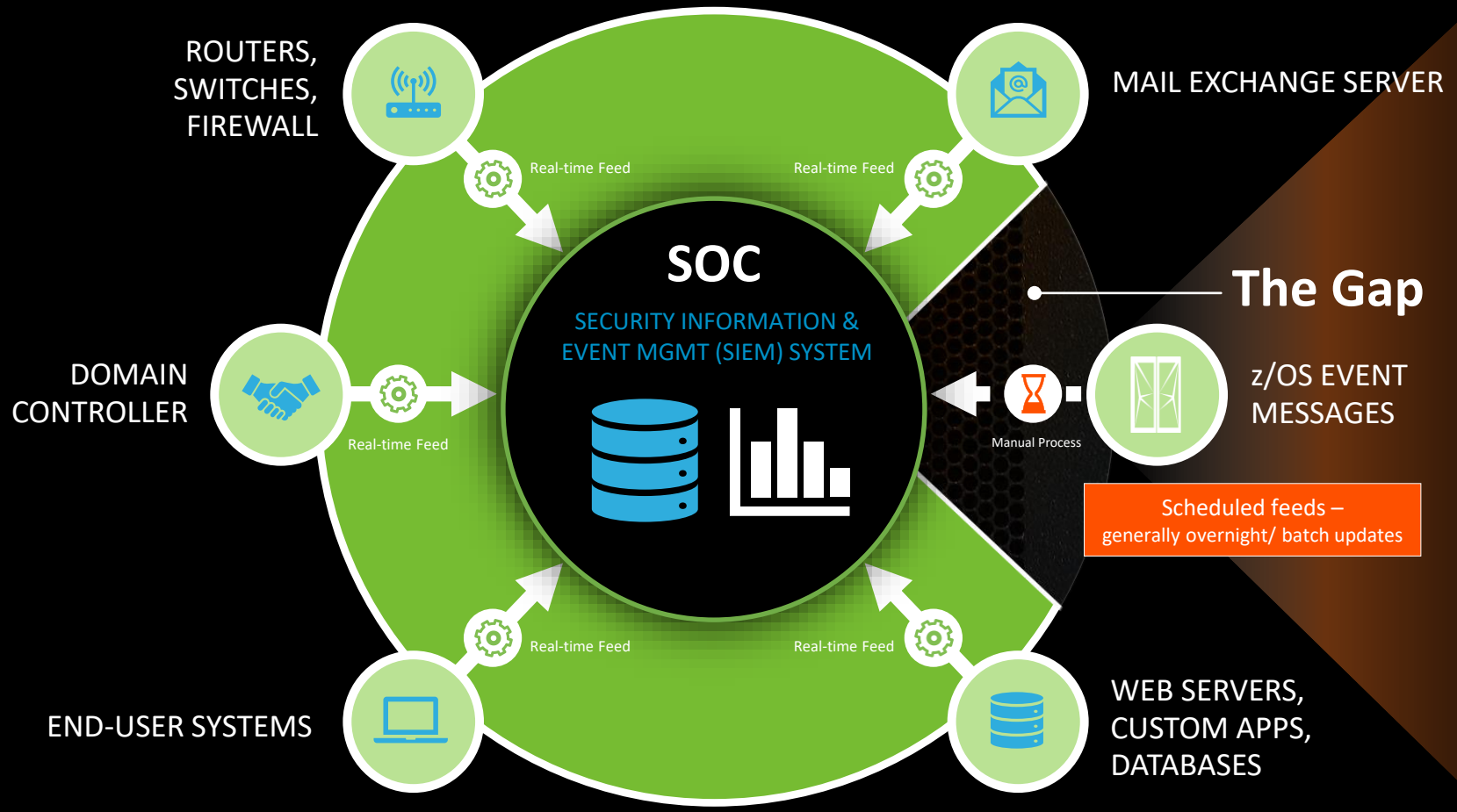
Mainframe Vulnerability Scanning

Vulnerability scanning in a mainframe context is about scanning code delivered by your application / software vendors, as well as and in-house developed code, to identify any zero-day vulnerabilities that could be exploited.

Detect

- Anomalies & Events
- Security Continuous Monitoring
- Detection Processes

Mainframe Security Gap



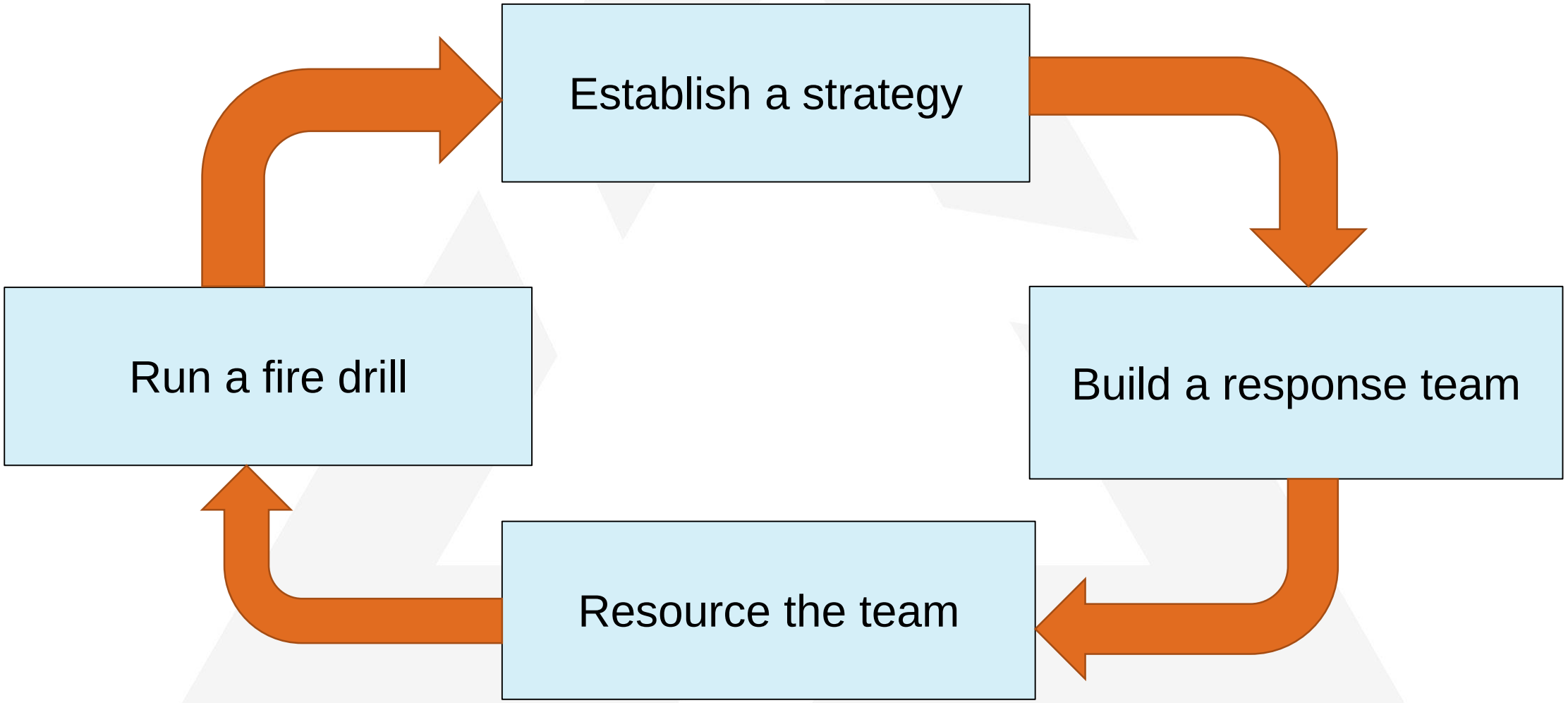
Mainframe Attack Surface

- Enumeration to identify user ID's and passwords
- Establish Reverse Shell
- Exploit poorly protected APF authorized libraries
- Unauthorized user privileged escalation
- Webserver probe for vulnerabilities
- Exploit vulnerabilities in Network Job Entry

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Incident Response



Recover

- Recovery Planning
- Improvements
- Communications

Key Takeaways

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

- The mainframe is just as vulnerable to attack as any other TCP/IP connected computer
- Companies should follow the NIST framework to apply good security hygiene to the mainframe
- A mainframe security architect is a vital role for designing and securing the backbone of the enterprise
- Excessive access checking is a core part of protecting the mainframe from malicious activity
- The ability to detect and respond to Indicators of Compromise in real time can prevent a catastrophic breach

Complete your session evaluations for a chance at daily prizes!

To complete, visit
www.share.org/evaluation
and see your progress on the leaderboard!