Did You Set It and Forget It?

JULIE BERGH
ROCKET SOFTWARE
JBERGH@ROCKETSOFTWARE.COM

Abstract

- Mainframes continue to provide the utmost security capabilities. It is an ongoing challenge to detect threats and remain compliant with the latest industry regulations for PCI, finance, healthcare and government standards. As new applications and workloads are hosted as z systems, it is imperative that the latest security enhancement are fully deployed.

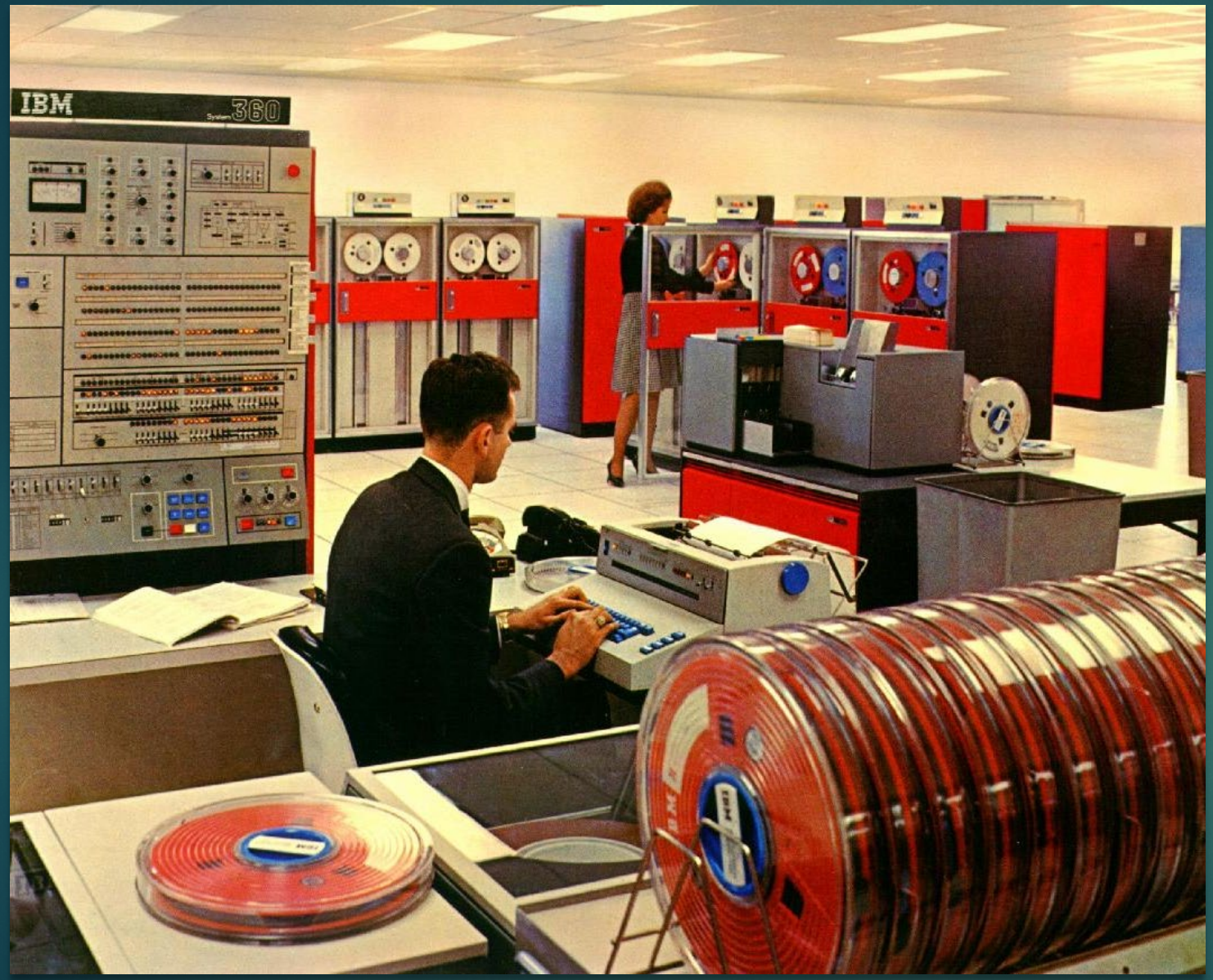
  This session will focus on recent mainframe security functions that improve security intelligence to identify threats; monitor security options to demonstrate compliance; analyze entitlements to detect potential identity governance exposures; and enhance authentication capabilities.

Why Am I Explaining This?

Security Maturity -

55+ years

40+ years



A Picture is Worth a Thousand Words….

Nearly all data in the computer center

All users of the system are “known”

No way to access the system, except from company locations

A Picture is Worth a Thousand Words….

Nearly all data in the computer center

All users of the system are “known”

No way to access the system, except from company locations

A Picture is Worth a Thousand Words….

Data growth significant. Some data moving to other platforms

Number of users is growing dramatically

Remote access to computer

Figure 1-1 The IBM z14

A Picture is Worth a Thousand Words….

Enormous explosion in data as internet becomes widely available.

24 x 365 availability is common, and expected

Hundreds of thousands of users, and all aspects of z/OS access

Remote access to computer systems is normal and expected

Users operate anywhere and everywhere; in legal jurisdictions you didn't know existed

Have you talked to a ‘mainframe’ today?

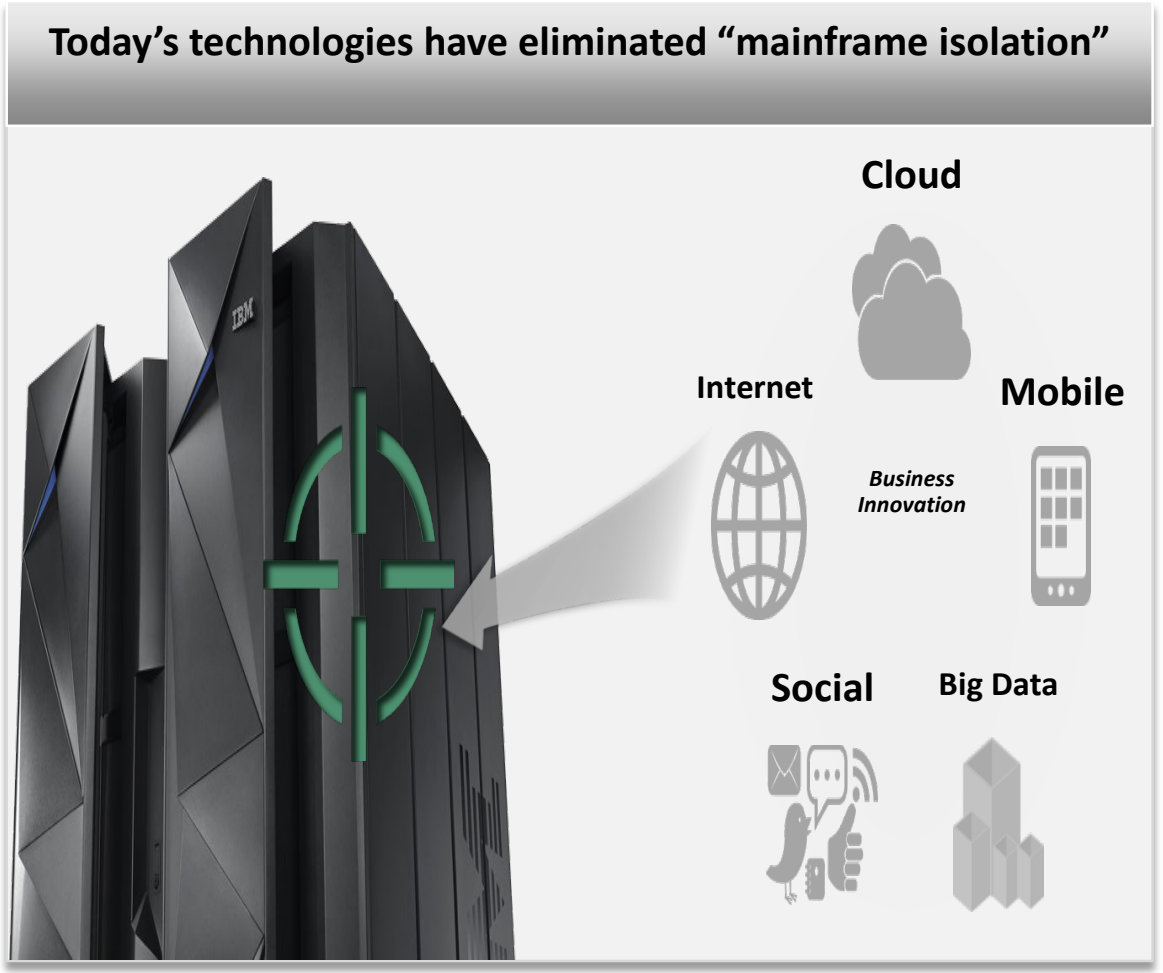
… at some point in these daily transactions, you likely touched a mainframe

- **Did you know you have probably interacted with a mainframe on a regular basis and did not know it.**
- **Did you withdraw cash out of a bank’s ATM?**
- **Did you make a purchase at a major retail store?**
- **Did you make a bank to bank transfer locally or internationally?**
- **Did you make an airline ticket reservation?**
- **Did you use a credit card?**

Mainframe

Banking	Insurance	Retail	Healthcare	Public Sector	Transport	Telecoms
Core Banking	Internet Rate Quotes	On-line Catalog	Patient Care Systems	Electronic IRS	Rolling stock inventory	Network infrastructure
Wholesale Banking – Payments	Policy Sales & Management (e.g. Life, Annuity, Auto)	Supply Chain Management	On– line Claims Submission & Payments	Web based Social Security	Track progress of transport to/from destination	Customer billing
Customer Care & Insight	Claims Processing	Customer Analysis		Tax processing	Ticketing	Broadband availability

The increasingly desirable target of the mainframe



In today's world, where everything is connected to everything, the Mainframe faces a new set of challenges. Mainframe customers must ask themselves several questions:

- **What are you doing about this new interconnectedness?**
- **Can hackers get to their mainframe data?**
- **How will you know if they were attacked?**
- **Will you be alerted in time?**
- **When did they last re-design their security? Was it in 1980 or 1990?**

What happens in a Minute in 2019

but . . . .

What happens on the mainframe

Mainframes help . . .

Mainframes process roughly 30 billion business transactions per day, including most major credit card and banking transactions, stock trades and money transfers, manufacturing processes and ERP systems worldwide.[1]

1.3 million CICS® Transactions. Every Second. Every Day.[1]

[1] www.share.org/p/bl/et/blogid=2&blogaid=234

[2] www.share.org/p/bl/et/blogid=2&blogaid=234

[3] http://blogs.ca.com/innovation/2012/10/18/the-mainframe-and-innovation-not-mutually-exclusive/

[4] http://www.datacenterdynamics.com/focus/archive/2013/12/research-reveals-mobiles-mainframe-impact

[3] http://www.nerdwallet.com/blog/credit-card-data/credit-card-transaction-volume-statistics/

Mainframes help . . .

- $6 Trillion in card payments to execute annually[2]
- 23 Billion ATM transactions processed a year
- Up to 3 Billion passengers take flight a year; with 2x that expected by 2030[1]
- And think about the sheer number of medical records and UPC barcodes being produced, scanned stored and accessed every day, every year

[1] http://www.icao.int/Newsroom/Pages/annual-passenger-total-approaches-3-billion-according-to-ICAO-2012-air-transport-results.aspx

[2] http://www.statisticbrain.com/atm-machine-statistics/

[3] http://www.nerdwallet.com/blog/credit-card-data/credit-card-transaction-volume-statistics/

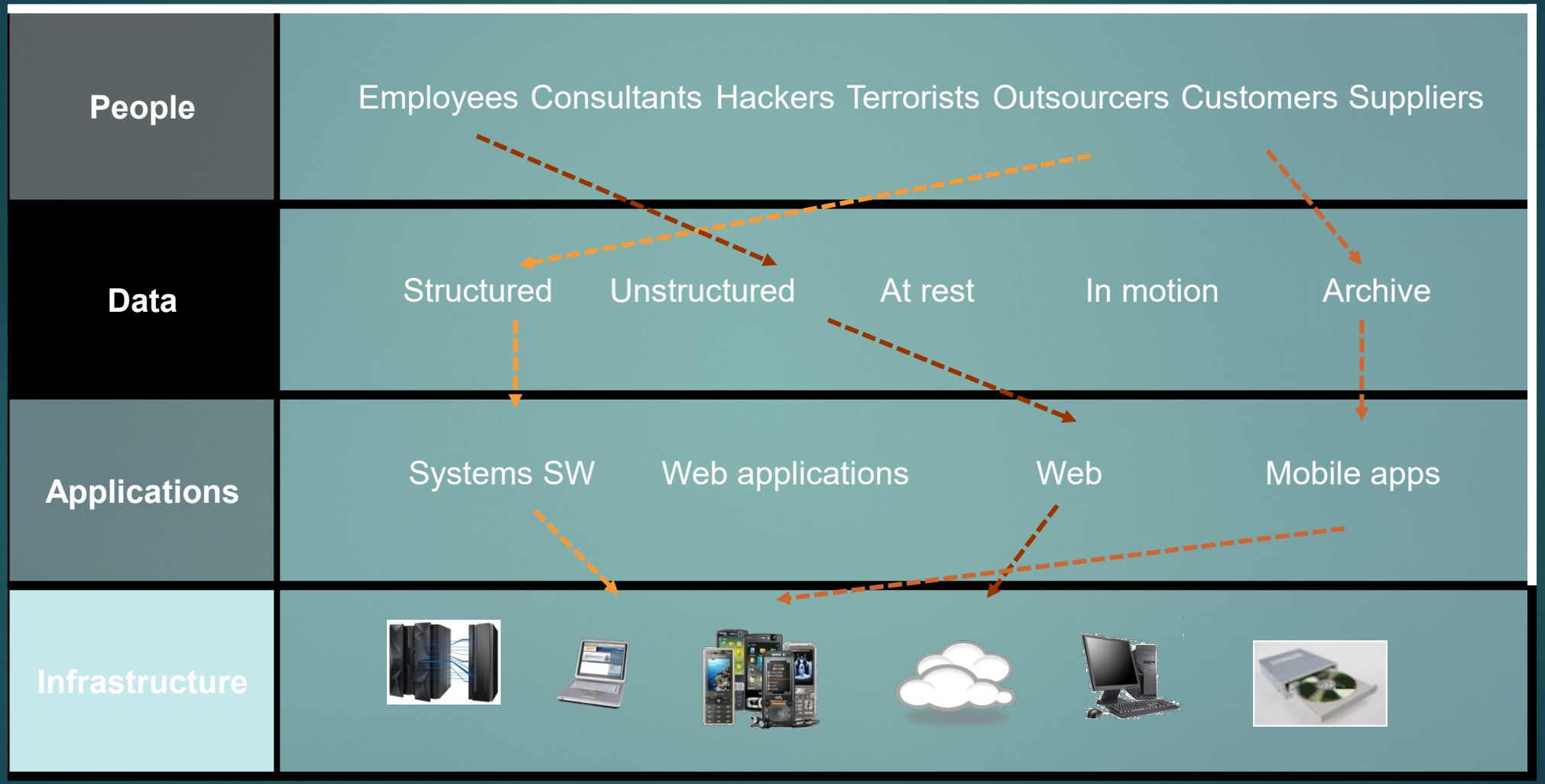
Security Maturity

- Do you have an overall view of how effectively your security plan is working?
- Are the right IT security controls in place to protect the information that is critical to your business?
- Controls must cover all aspects of your business, including mechanisms used by hardware and software systems, networks, databases and human resource systems.

General

- **What are your regulatory requirements around monitoring user access on the mainframe (e.g., SOC1, SOX, GDPR, HIPAA, ISO2700-1, STIG)?**
- **Does the enterprise architecture and the enterprise security architecture appropriately include mainframe in the work product(s)?**
- **Are threat risk assessments specifically tailored to mainframe controls (put an example)?**
- **Is there an incident response plan and does the incident response plan include contacts for mainframe resource owners?**
- **Does the application inventory include assets residing on z System? If so, is the inventory regularly reviewed for completeness and accuracy?**
- **Does the organization monitor for mainframe specific vulnerabilities and notify test and operational teams?**

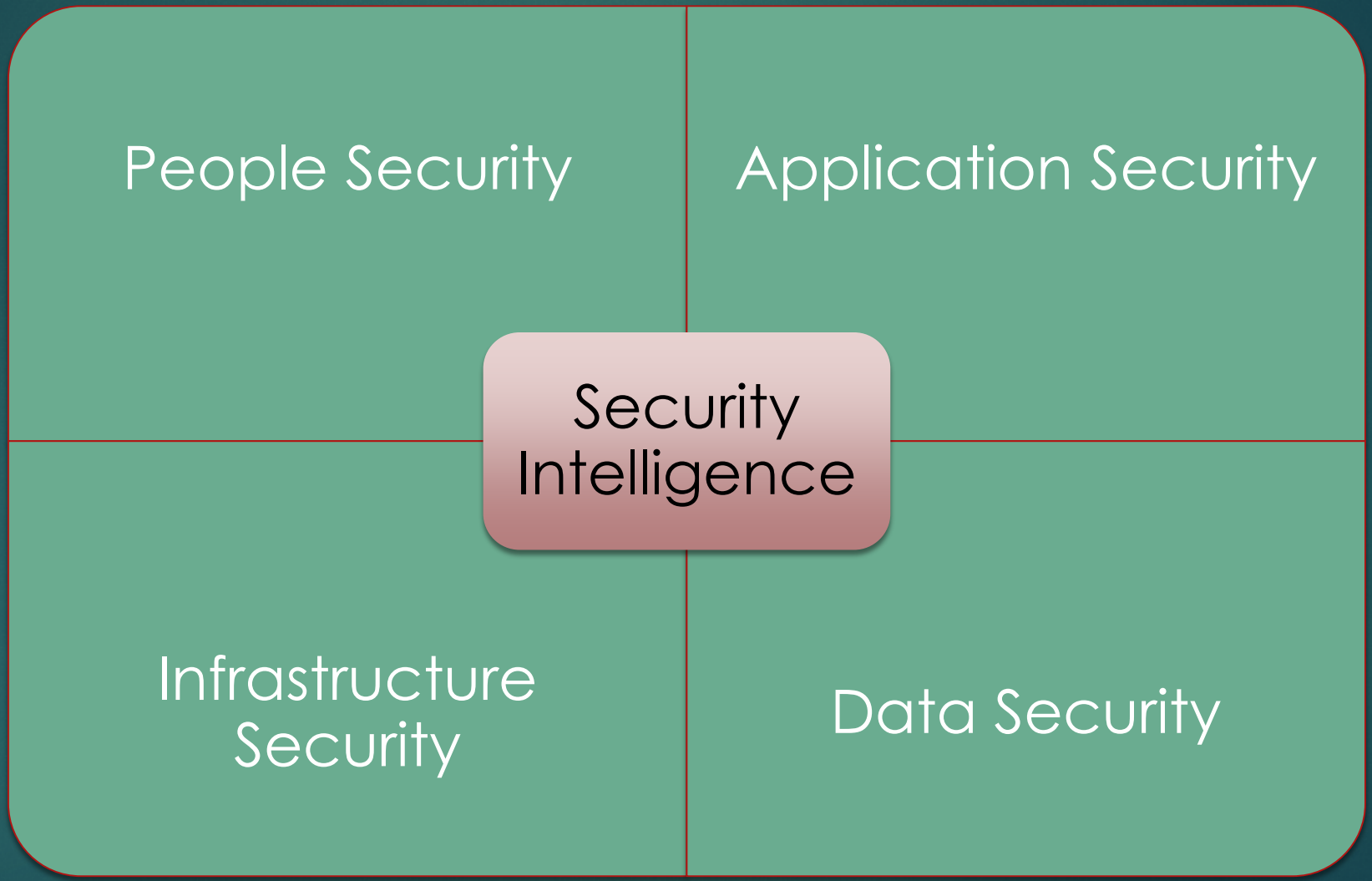
How will we talk about Security?



How will we talk about Security?

- People - Address the risks associated with user access to corporate resources
- Data - Categorize, classify and protect information in flight and at rest. Deploy controls for access to and usage of sensitive business data both structured and unstructured.
- Application - Help keep applications secure, protected from malicious or fraudulent use, and hardened against failure
- Infrastructure - Optimize service availability by mitigating risks to network, physical and server infrastructure as well as distributed endpoints

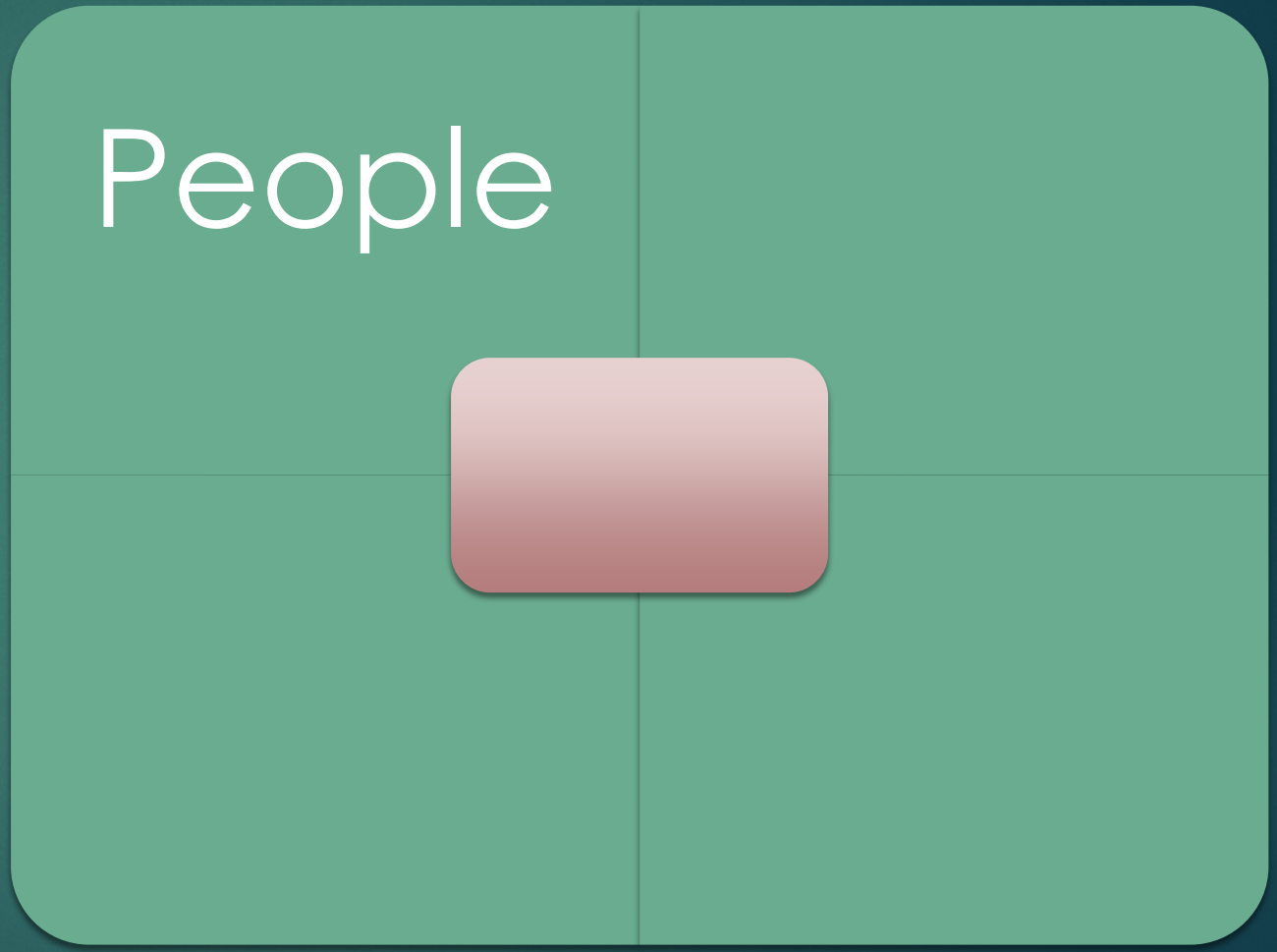
Security Immune System



Security Immune System

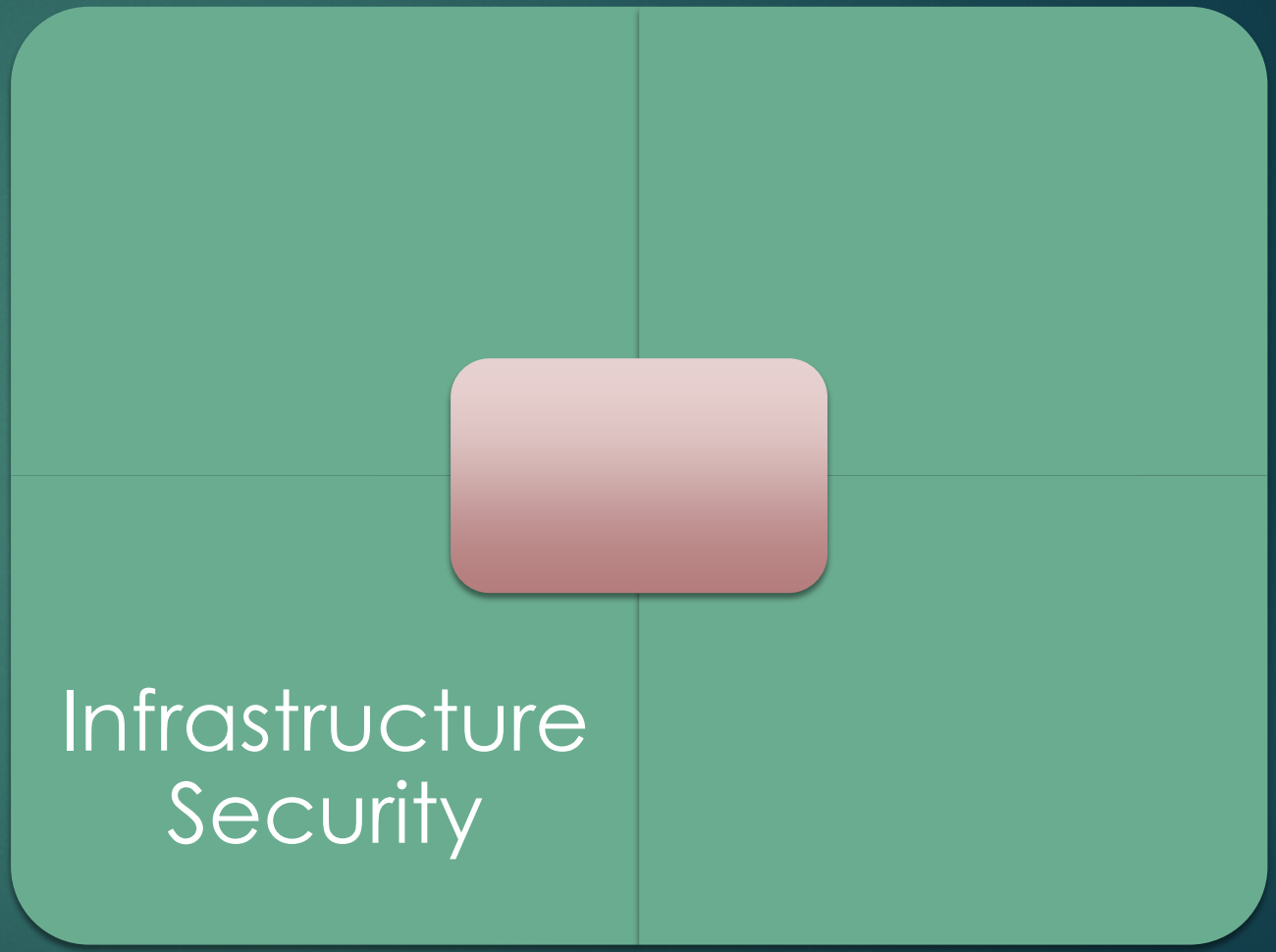
User Community:

- Your users
- Vendors
- Contractors
- Branch User
- Mobile
- Customers
- Service Accounts
- Started Task
- Privileged Users
  - DBAs
  - Admins
  - Others

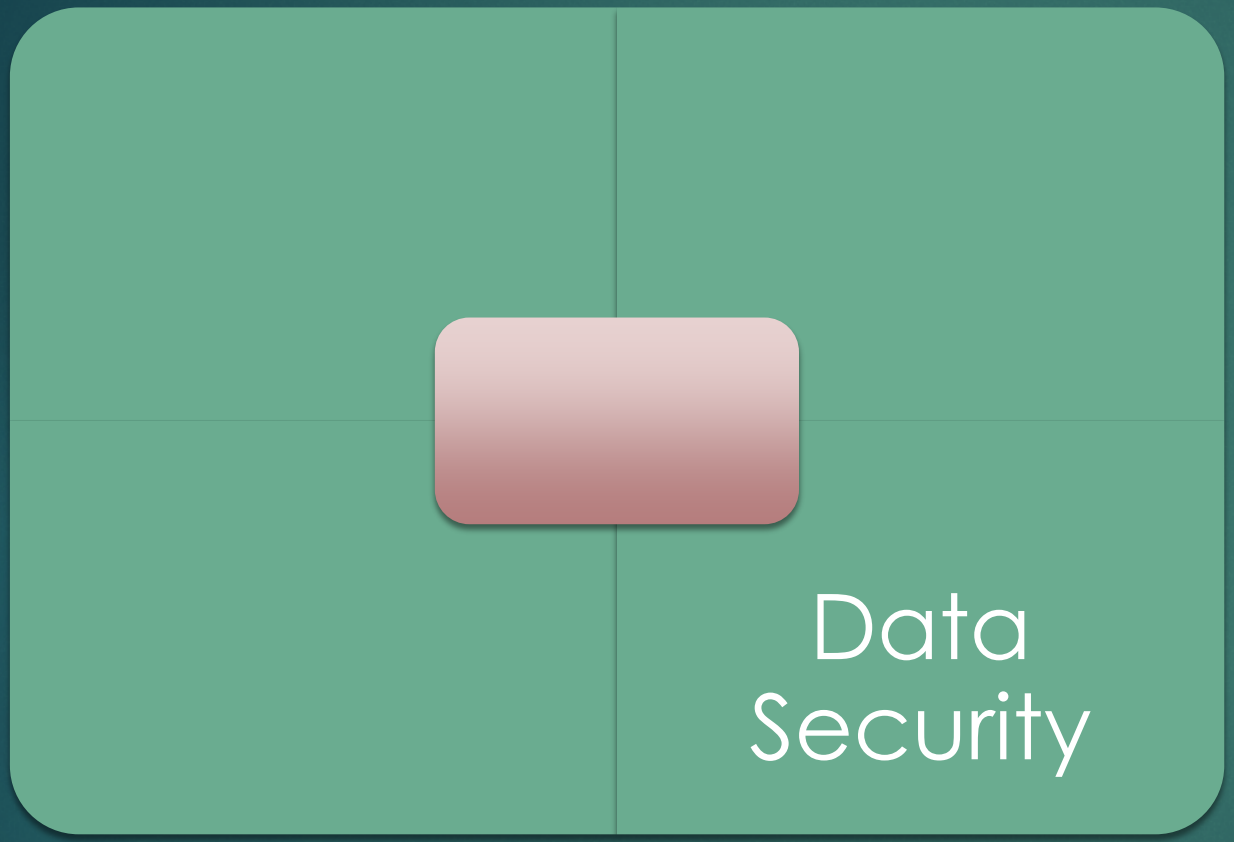


Security Immune System

- **Infrastructure**
- **z/OS**
- **File Manager**
- **Communications Server**
- **TCPIP**
- **UNIX System Server**
- **Subsystems:**
  - **DB2**
  - **IMS**
  - **CICS**
  - **MQ**
  - **Etc**

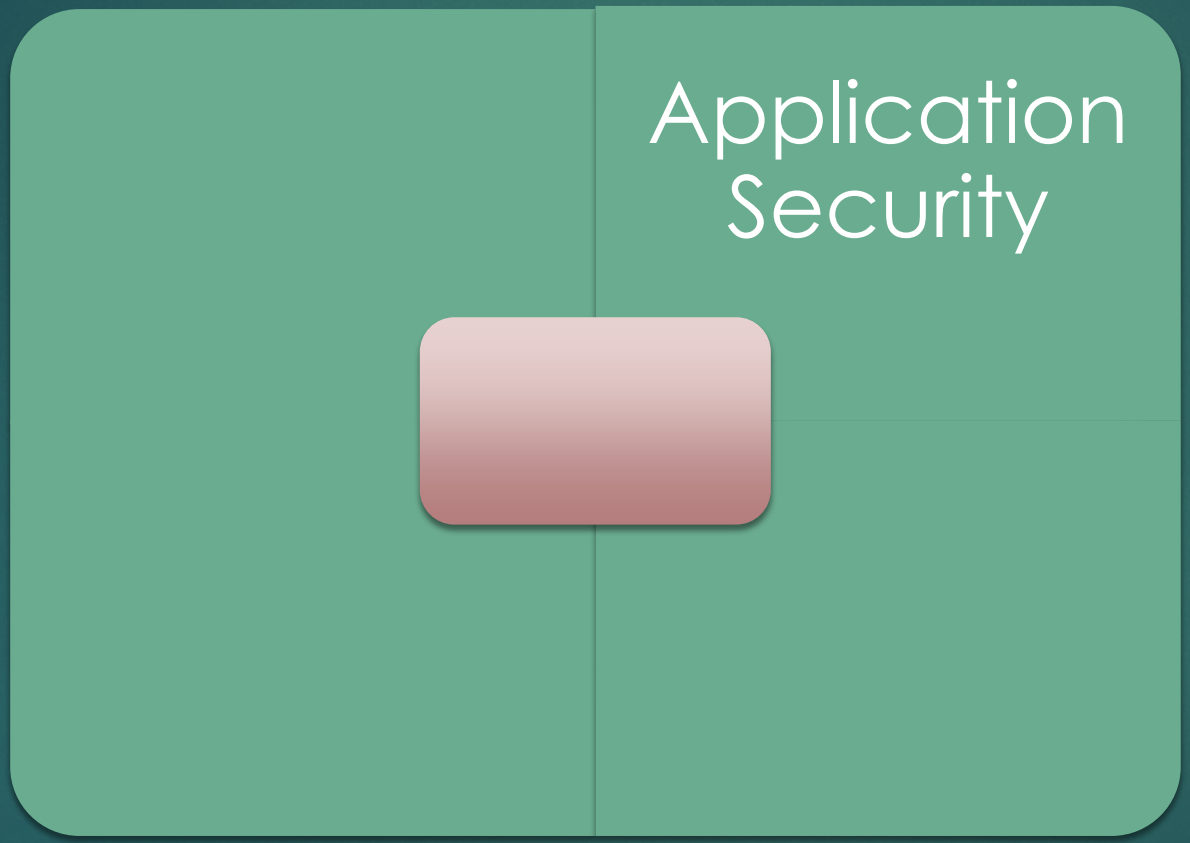


Security Immune System



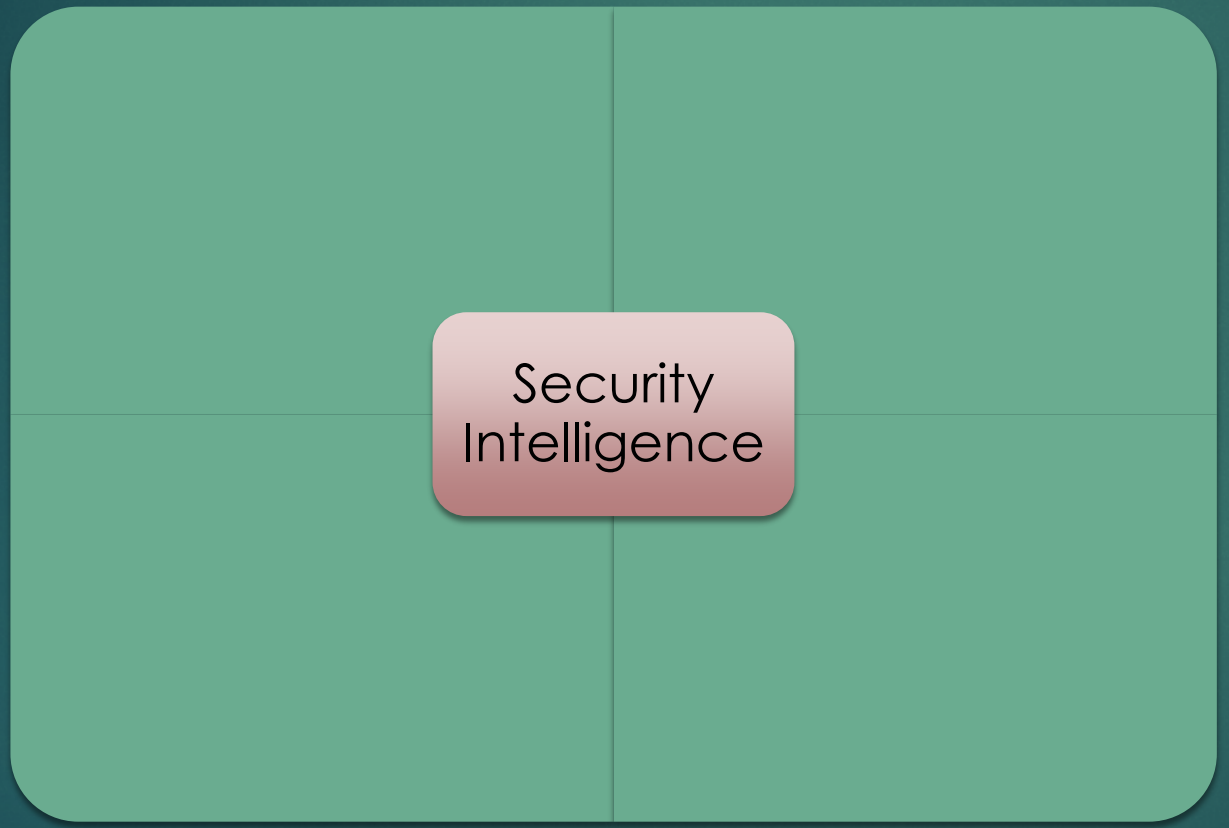
- Data
- Monitor/Audit
- Find/Identify
- Enforce/Protect
- Assess/Harden
- Encrypt

Security Immune System



- Applications
- Scan for Vulnerabilities

Security Immune System

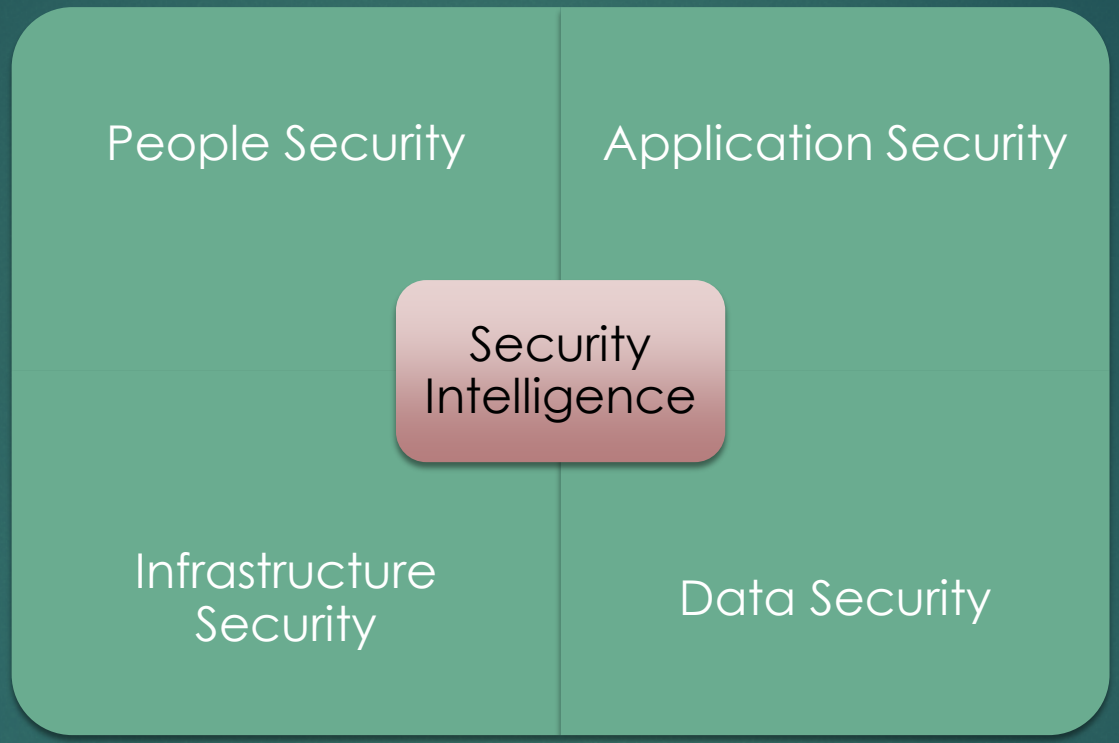


- Security Intelligence
- Network Flows
- Risk Management
- Vulnerability Manager
- SIEM
  - Search, Collect, Analysis, Mitigate

Security Immune System

User Community:

- Your users
- Vendors
- Contractors
- Branch User
- Mobile
- Customers
- Service Accounts
- Started Task
- Privileged Users
  - DBAs
  - Admins
  - Others
- z/OS
- File Manager
- Comm Server
- TCPIP
- UNIX System Server
- Subsystems:
  - DB2, IMS, CICS, MQ, ETC



- Scan for Vulnerabilities

- Monitor/Audit
- Find/Identify
- Enforce/Protect
- Assess/Harden

- Network Flows
- Risk Management
- Vulnerability Manager
- SIEM

Wikipedia Definition

- Security Information and Event Management (SIEM) software products and services combine security information management (SIM) and security event management (SEM).
- They provide real-time analysis of security alerts generated by network hardware and applications.
- The acronyms SEM, SIM and SIEM have been sometimes used interchangeably.
- The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as security event management (SEM).
- The second area provides long-term storage as well as analysis and reporting of log data, and is known as security information management (SIM).

What is Security Intelligence?

Security Intelligence

--noun

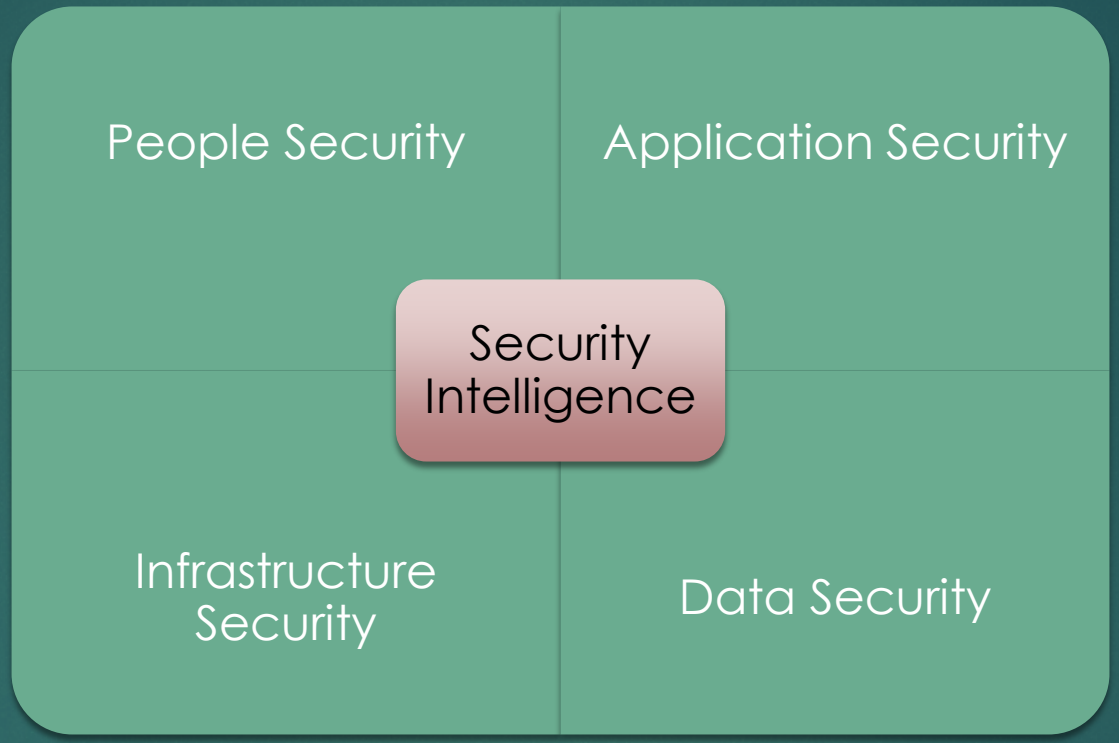
1. the real-time collection, normalization and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

Security Immune System

User Community:
- Your users
- Vendors
- Contractors
- Branch User
- Mobile
- Customers
- Service Accounts
- Started Task
- Privileged Users
  - DBAs
  - Admins
  - Others

- z/OS
- File Manager
- Comm Server
- TCPIP
- UNIX System Server
- Subsystems:
  - DB2, IMS, CICS, MQ, ETC



- Scan for Vulnerabilities

- Monitor/Audit
- Find/Identify
- Enforce/Protect
- Assess/Harden

- Network Flows
- Risk Management
- Vulnerability Manager
- SIEM

Challenges

- Perception mainframe is secure
- No security standards
- No trending analysis
- Not keeping up with current security controls
- Not adapting to least privilege
- Inactive users with elevated privileges
- Inactive users not deleted or access removed
- Too many user with UNIX super user authority (UID0)
- Excessive number of users with no password interval
- Excessive number of users with elevated privileges

Challenges

- Separation of duties lacking
- Obsolete information in security database
- People with console authority through SDSF, TSOAUTH
- Excessive access on system critical resources
- Lack of appropriate security in subsystems (e.g., CICS, SDSF, TCP/IP, DB2)
- Too many users circumventing controls
- Excessive utility access allows security policy bypass
- Inadequate attention to monitoring, alerting, and reporting

Challenges

- Reporting haven't changed in the last 15 years. Not adding new ones or changing existing
- Reporting on violations and not updates to critical system and application resources not being done
- Data shared between production and test environments.
- Weak password control - Same password rules used in last 15 years
- Little control over UNIX systems services
- Software products still using internal security interface (e.g., SDSF, CA1, HSM, DFDSS)
- Obsolete information in RACF database not cleaned up
- Copying production data for test

Summary

- Better understand whether IT security controls currently in place protect the information that is critical to their business.
- Better understand if their overall view of how effectively your security plan is working.
- Better understand if their security processes are protecting them from the latest and future threats.

Thank You