

IBM zSystems and
LinuxONE

Jacksonville Z Customer Council

zSystems Security Update

David Rossi
Cybersecurity Architect
dzrossi@us.ibm.com



Why is Mainframe a Target?

Large target for critical infrastructure

A single mainframe can process more than **19 billion** transactions daily

World's top **92/100** banks

Top **23/25** airlines

10/10 of the top **10** insurance providers



DEPARTURES

TIME	DESTINATION	FLIGHT	GATE	REMARKS
12:39	BERLIN	BA 903	31	CANCELLED
12:57	SYDNEY	QF5723	27	CANCELLED
13:08	TORONTO	AC5984	22	CANCELLED
13:21	TOKYO	JL 608	41	CANCELLED
13:37	HONG KONG	CX5471	29	CANCELLED
13:48	MADRID	IB3941	30	CANCELLED
14:19	LONDON	LH5021	28	CANCELLED
14:35	NEW YORK	AA 997	11	CANCELLED
14:54	PARIS	AF5870	23	CANCELLED
15:10	ROME	AZ5324	43	CANCELLED

Agenda

Threat Management

- ✓ Security Intelligence

Vulnerability Management

- ✓ Compliance
- ✓ Quantum Safe Systems

Threat Management

Key Findings of interest Ponemon Data Breach Report 2022

USD 3.05 M Average

cost savings associated with fully deployed security AI and automation

Breaches at organizations with fully deployed security AI and automation cost USD 3.05 million less than breaches at organizations with no security AI and automation deployed. This 65.2% difference in average breach cost — between USD 3.15 million for fully deployed versus USD 6.20 million for not deployed — represented the largest cost savings in the study. Companies with fully deployed security AI and automation also experienced on average a 74-day shorter time to identify and contain the breach, known as the breach lifecycle, than those without security AI and automation — 249 days versus 323 days. The use of security AI and automation jumped by nearly one-fifth in two years, from 59% in 2020 to 70% in 2022.



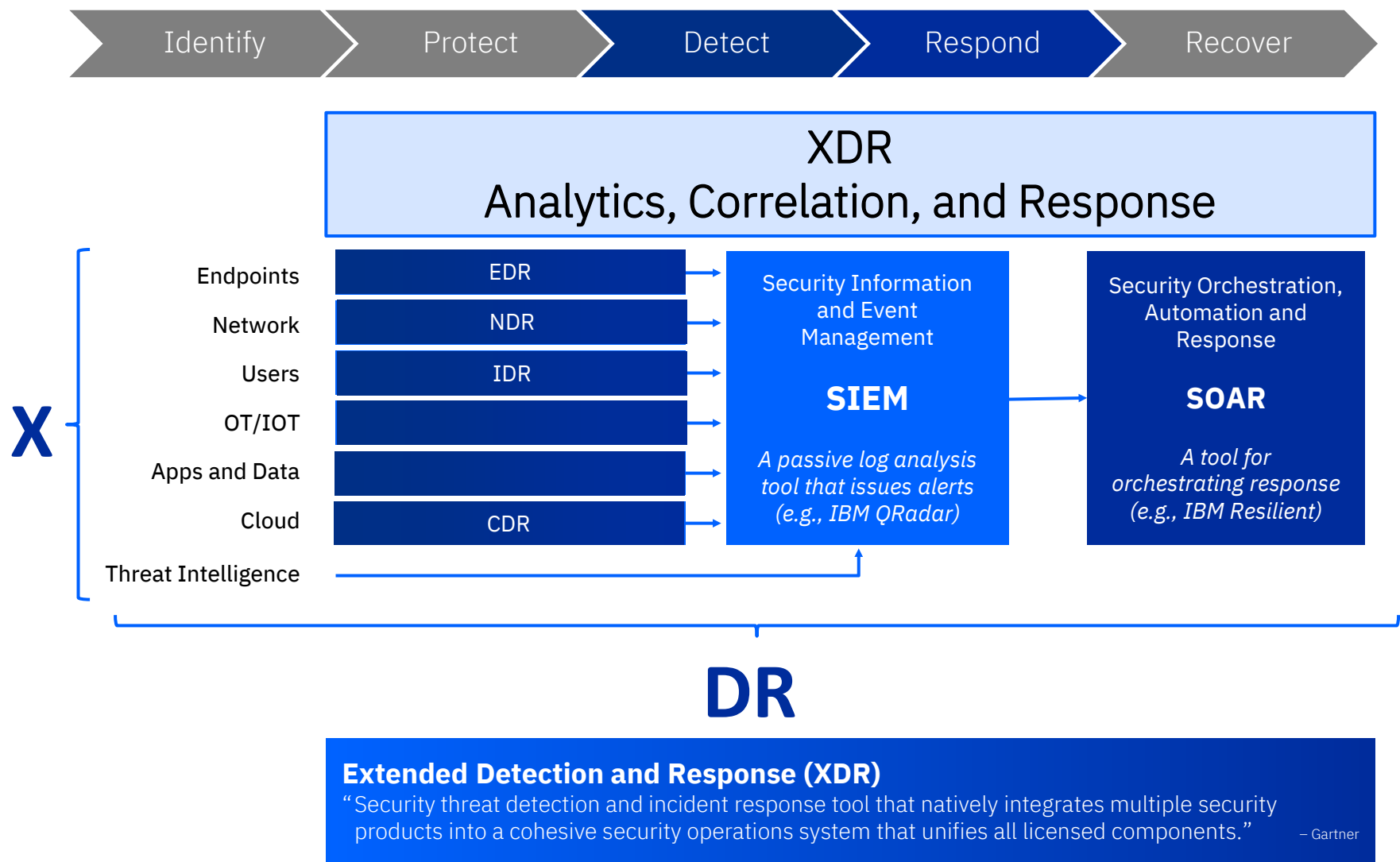
29 days

Savings in response time for those with extended detection and response (XDR) technologies

XDR technologies were implemented by 44% of organizations. Those organizations with XDR technologies saw considerable advantages in response times. Those organizations with XDR deployed shortened the breach lifecycle by about a month, on average, compared to organizations that didn't implement XDR. Specifically, organizations took 275 days to identify and contain a breach with XDR deployed versus 304 days without XDR deployed. This figure represents a 10% difference in response times.

<https://www.ibm.com/security/data-breach>

Evolution to eXtended Detection and Response (XDR)



Design principles

- **Intelligent threat management workflows** produce high-quality incident context and prioritization.
- **Federated data stitching** keeps multi-source and data scale problem under control.
- **Automated Response playbooks** accelerate time and precision to remediate.

Positioning

- **XDR critically builds on EDR**
Endpoint data is essential but not sufficient for XDR.
- **XDR leverages SIEM’s threat management capabilities**
Focus on threat-facing incident response, log and event storage, and detection.
- **XDR leverages SOAR automation**
XDR needs automation to function but does not need to be a full SOAR platform.

Trend to use Mitre Att@ck Framework a starting point

Inputs for Security Intelligence

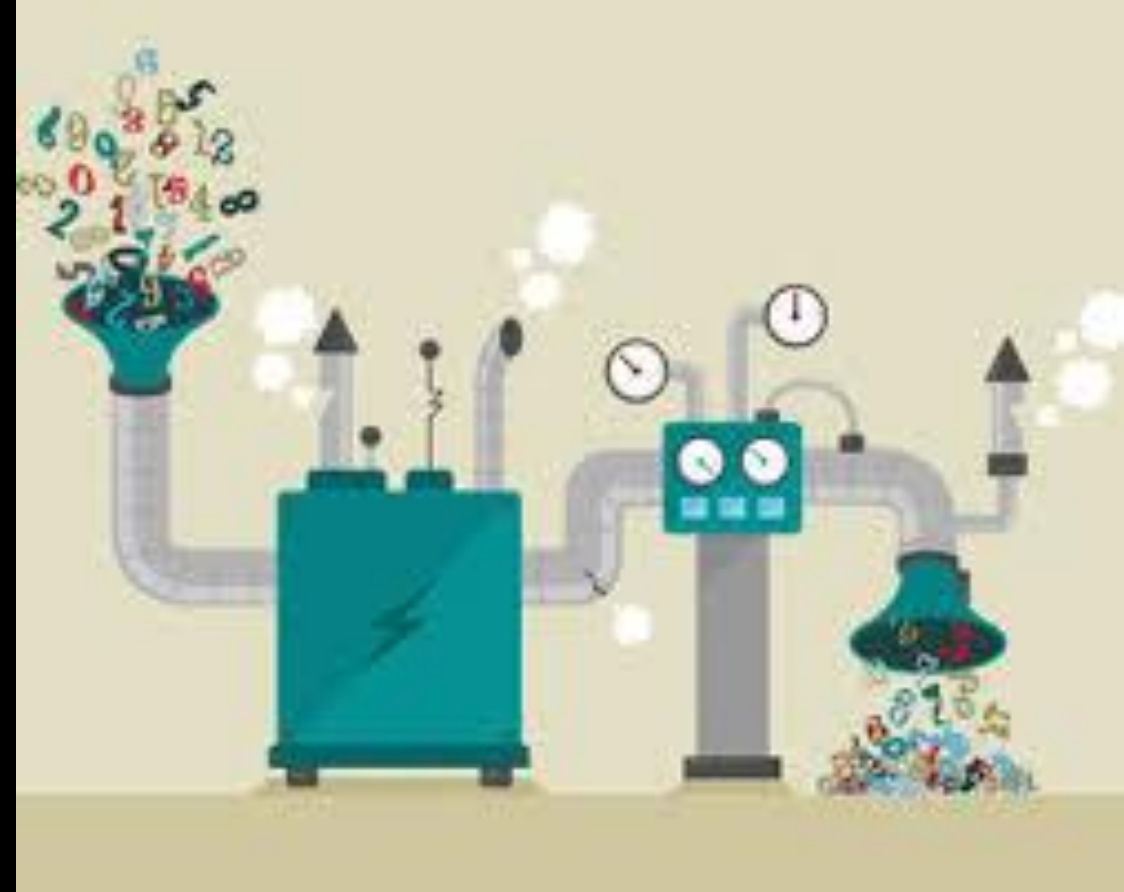
Cyber Events

- Meaningful and/or Actionable
- Credible
- Inclusive of Enterprise

Collection and processing

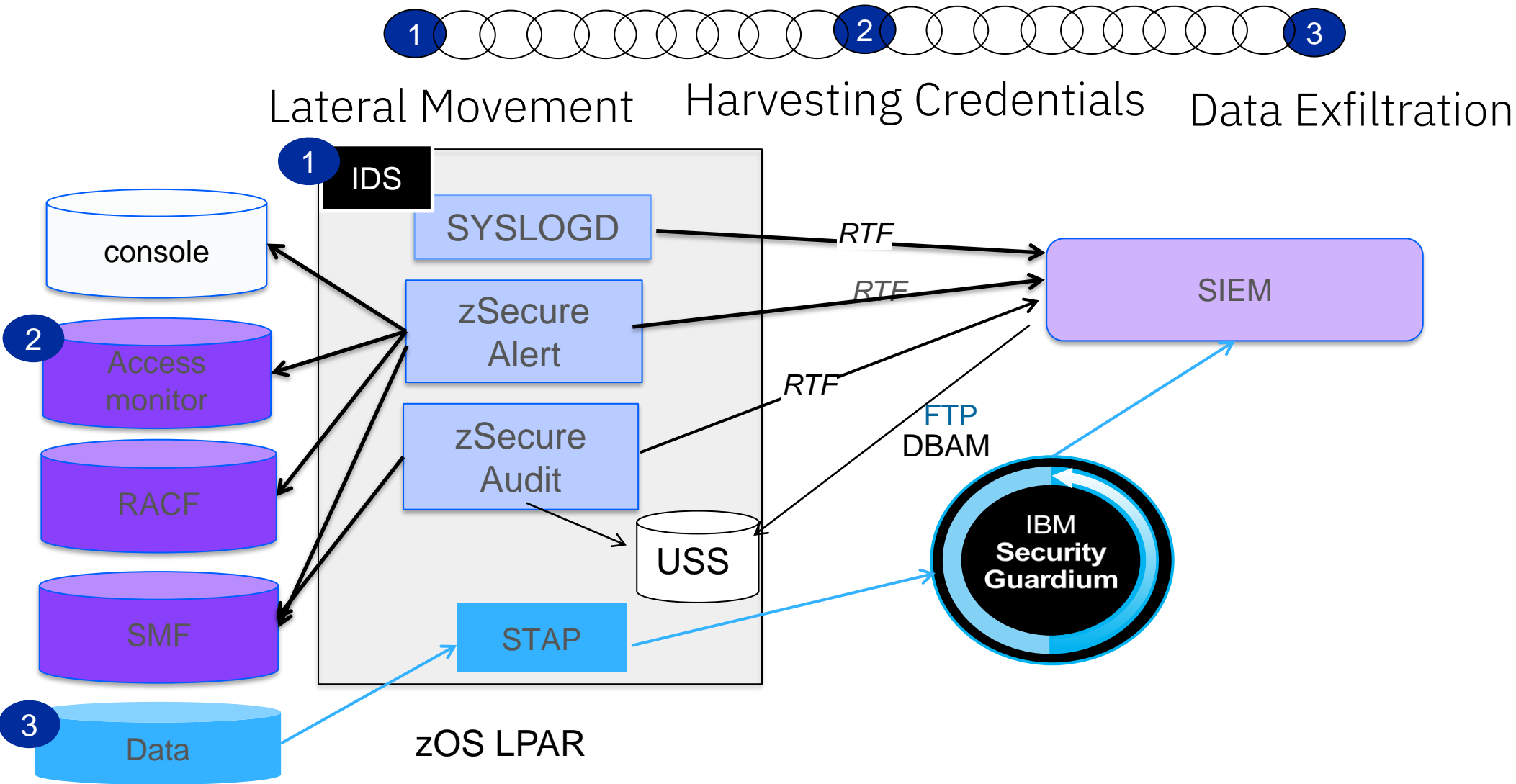
- Locally processing raw events
- Externally processing raw events

Security Intelligence is applying intelligence to cyber events collected from enterprise to assess and react to risk.



z/OS security events RACF environment

Kill Chain of common adversary attack



Mainframe Events in XDR engine

Poll Audience



XDR with z events

- ✓ **Extended**
Incorporated network, logs and identity from all systems in enterprise including zSystems.
- ✓ **Detection**
Correlation of multiple events to recognize pattern of adversary behavior.
- ✓ **Response**
Defense responses that can be automated with Ansible (defacto) or other automation products.
 - Blocking network traffic
 - Halting processes
 - Disabling accounts

Vulnerability Management

IBM Z & LinuxONE – Security design, architecture & integration

Security architected into all levels of the stack

- Processor
- Firmware
- Hypervisors
- Network
- Operating systems
- Applications & Middleware

IBM Z & LinuxONE security innovation and leadership




- Pervasive encryption
- Confidential computing with Secure Service Container & Secure Execution
- IBM Cloud Hyper Protect Services
- Hyper Protect Data Controller
- Integrated hardware encryption and compression
- Extensive security certifications including EAL5+ *Common Criteria* and *FIPS 140-2 L4*

Focus on leveraging IBM Z & LinuxONE technology and solutions to reduce human error and simplifying the processes of securing workloads with the goal of protecting data.






Security integration provides a more seamless solution, serves to reduce attack points, and yields a more robust security model.

IBM Z and LinuxONE security leadership

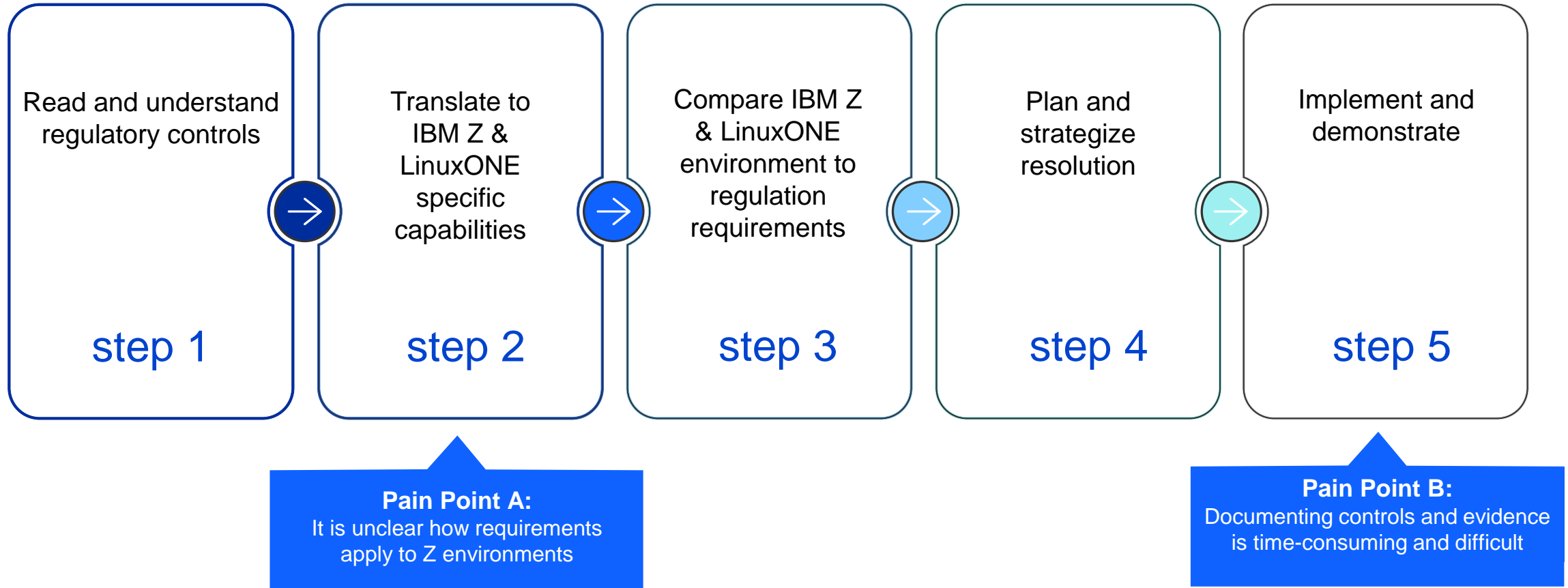
Foundation	z14 	z15 	z16 
Security Heritage	Data Protection	Data Privacy	Continuous Compliance
Integrated crypto hardware	Pervasive Encryption	DP for Diagnostics	IBM Z Security and Compliance Center
Bulk encryption via CPACF	Confidential Computing	Secure Execution for Linux on Z	Hyper Protect 2.0
Workload Isolation	Secure Service Container	Quantum Safe Cryptography	Quantum Safe System New QS Crypto APIs Crypto Discovery
Disk and tape encryption		Fully Homomorphic Encryption	HE Layers SDK
		FHE & toolkit on IBM Z	

IBM Z security leadership

Foundation	z14 	z15 	z16 
Security Heritage	Data Protection	Data Privacy	Continuous Compliance
Integrated crypto hardware	Pervasive Encryption	DP for Diagnostics	<div>IBM Z Security and Compliance Center</div>
Bulk encryption via CPACF	Confidential Computing		
Workload Isolation	Secure Service Container	Secure Execution for Linux on Z	Hyper Protect 2.0
Disk and tape encryption		Quantum Safe Cryptography	Quantum Safe System New QS Crypto APIs Crypto Discvoery
		Fully Homomorphic Encryption	HE Layers SDK
		FHE & toolkit on IBM Z	

Z & Linux on Z Compliance Specific Pain Points

Sourced from the Z Design Council and IBM's Sponsor User Program(s)





Payment Card Industry Data Security Standard (PCI-DSS) 3.2.1

Applicable to all entities that store, process, and/or transmit cardholder data.

Typical clients:

- Banking
- Financial
- Insurance
- Retail
- Mortgage



National Institute of Standards & Technology (NIST) SP 800-53

Applicable to all US federal government agencies and contractors; referenced by local governments and private industry regulations such as PCI-DSS.

Typical clients:

- Federal govt
- State / local govt



Center of Internet Security (CIS) Benchmarks

New Guidelines available:

- z/OS 2.5 with RACF
- Db2 for z/OS
- CICS TS
- Red Hat Enterprise Linux 8.0 for IBM Z

Applicable to organizations in all industries and geographies including government, business, industry and academic institutions.

Typical clients:

- Banking
- Financial
- Insurance
- Retail
- Mortgage
- Federal govt
- State / local govt

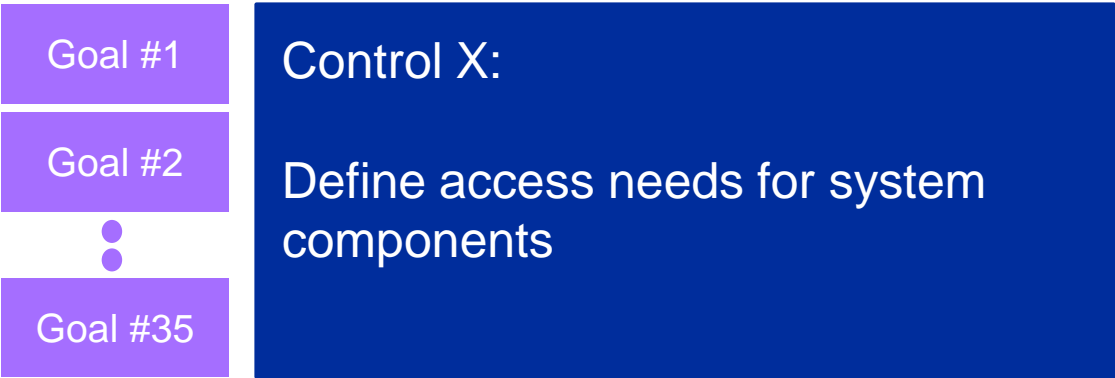
IBM Z Security and Compliance Center Terminology

A *goal* is a specific technical check that can be run on data to produce a pass or fail

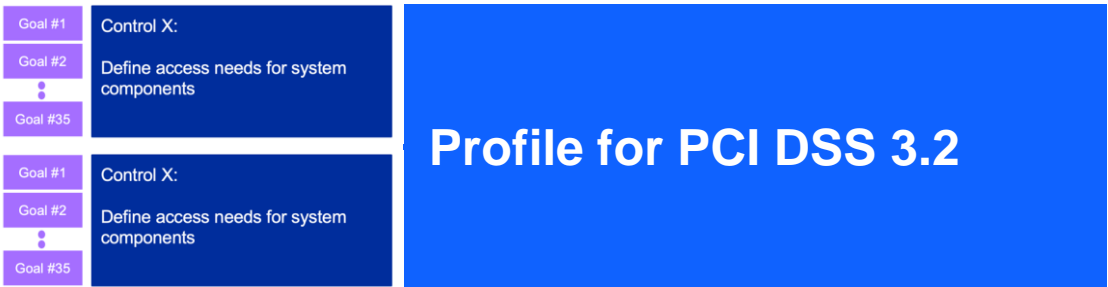
Goal #1

“Check whether only authorized users can access Db2 from CICS”

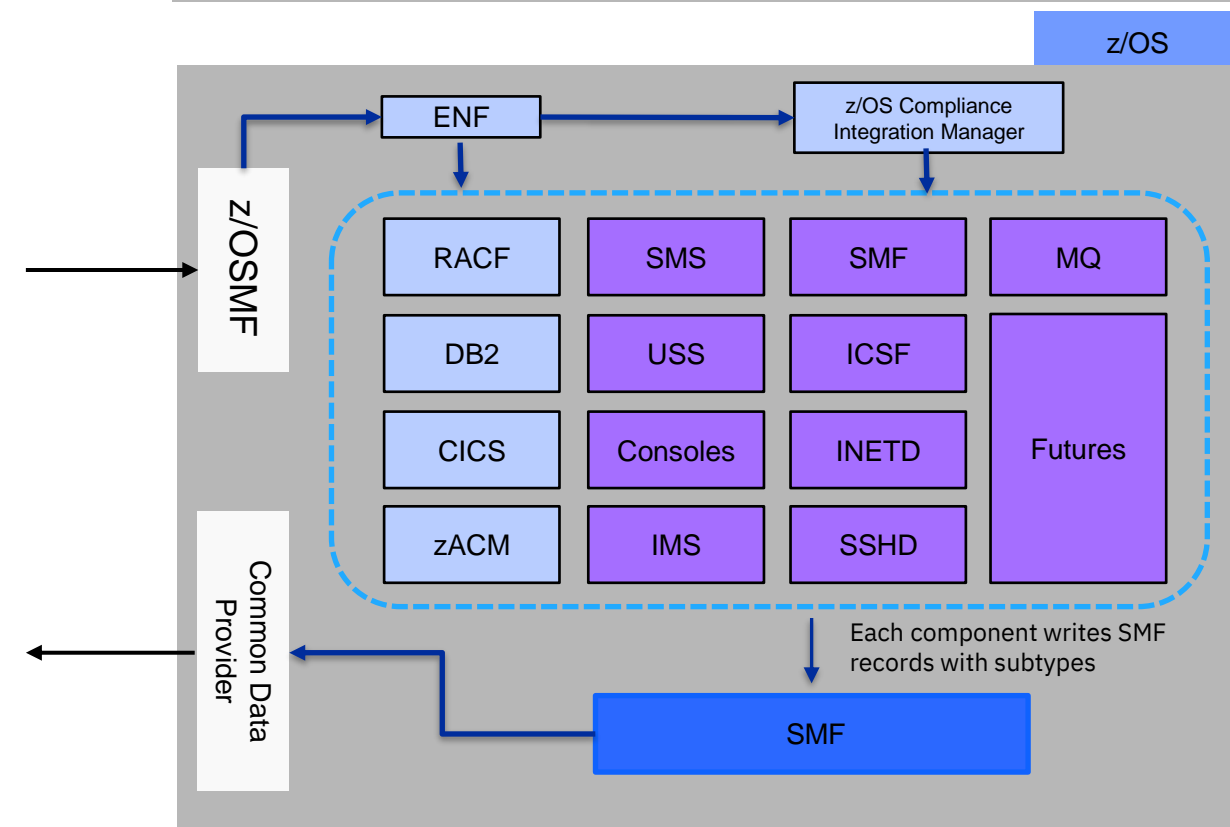
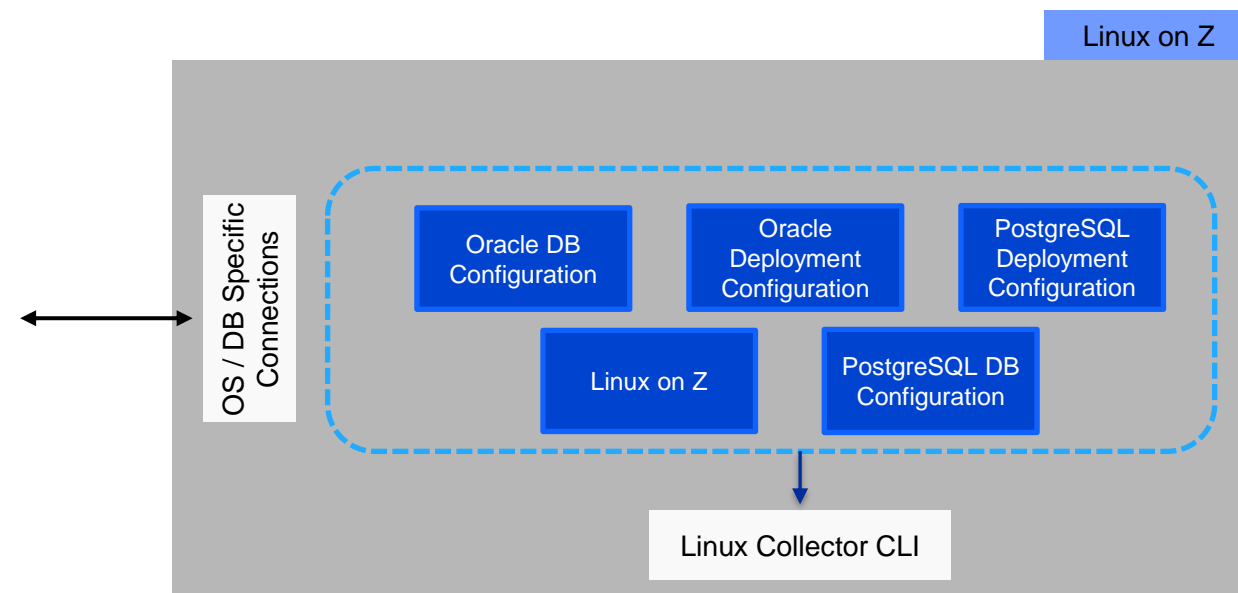
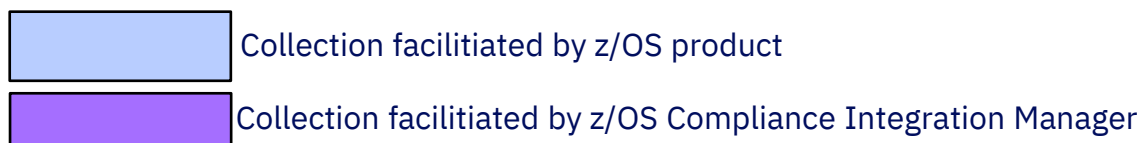
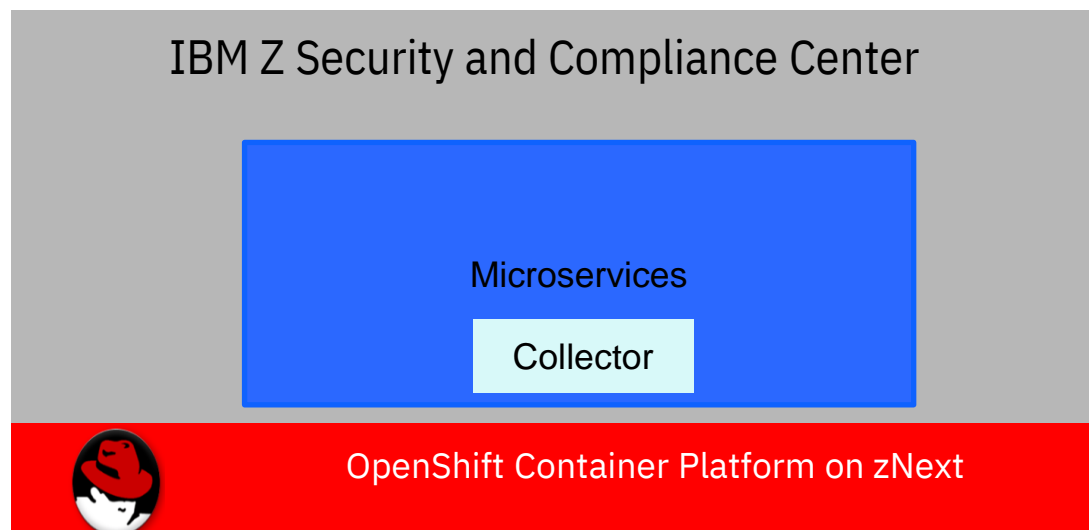
A *control* is a group of goals around a common theme which typically to a defined rule



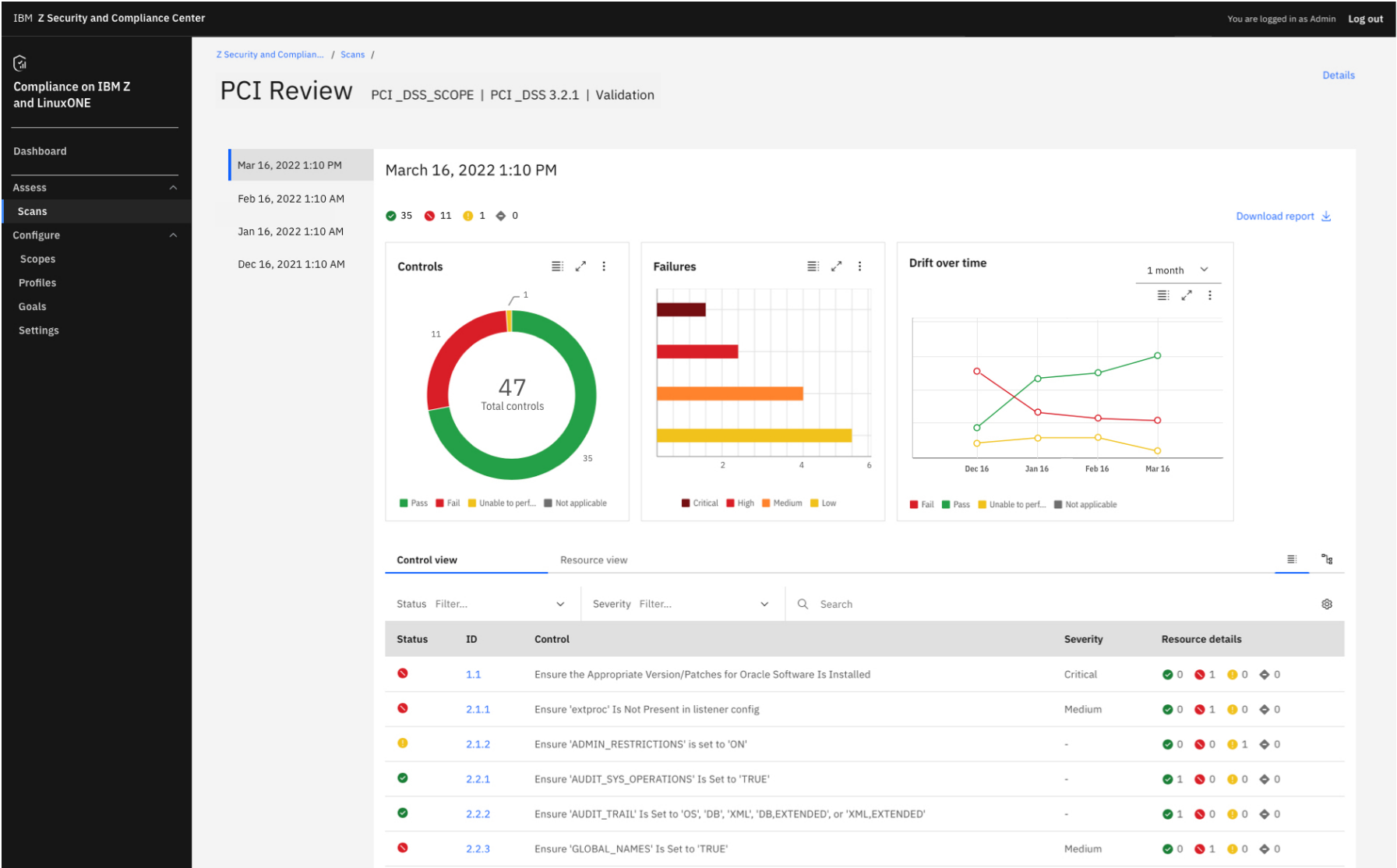
A *profile* is a group of controls which will be match applicable regulatory frameworks



Evidence Provider View






IBM Z Security and Compliance Center dashboard

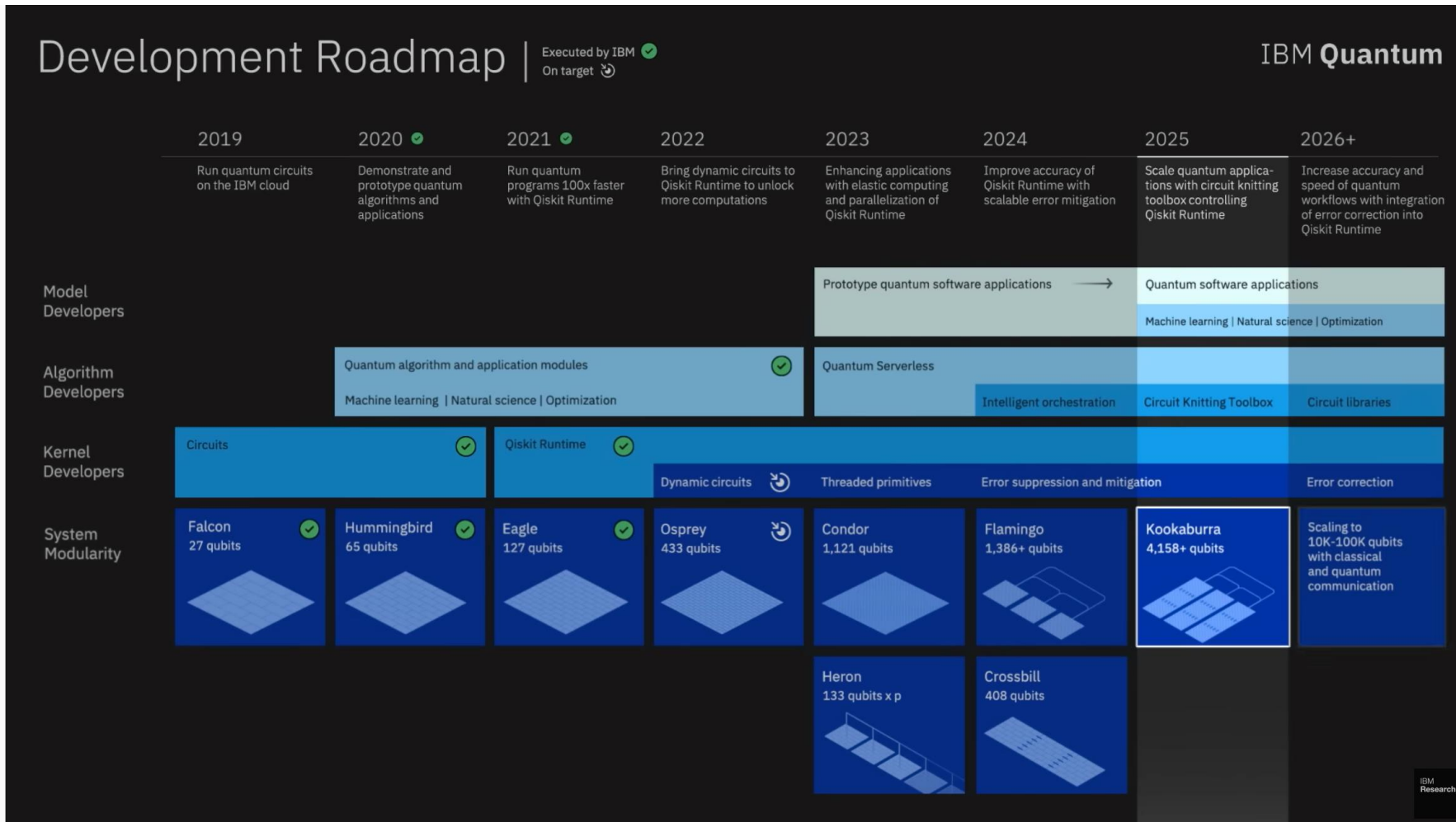


IBM Z security leadership



Foundation	z14 	z15 	z16 
Security Heritage	Data Protection	Data Privacy	Continuous Compliance
Integrated crypto hardware	Pervasive Encryption	DP for Diagnostics	IBM Z Security and Compliance Center
Bulk encryption via CPACF	Confidential Computing	Secure Execution for Linux on Z	Hyper Protect 2.0
Workload Isolation	Secure Service Container	Quantum Safe Cryptography	Quantum Safe System New QS Crypto APIs Crypto Discvoery
Disk and tape encryption		Fully Homomorphic Encryption	HE Layers SDK
		FHE & toolkit on IBM Z	

IBM Quantum Development Roadmap



Quantum computing applications in the real world.

- Artificial Intelligence & Machine Learning
- Computational Chemistry
- Drug Design & Development
- Cybersecurity & Cryptography
- Financial Modelling
- Logistics Optimization
- Weather Forecasting.

<https://www.ibm.com/quantum>

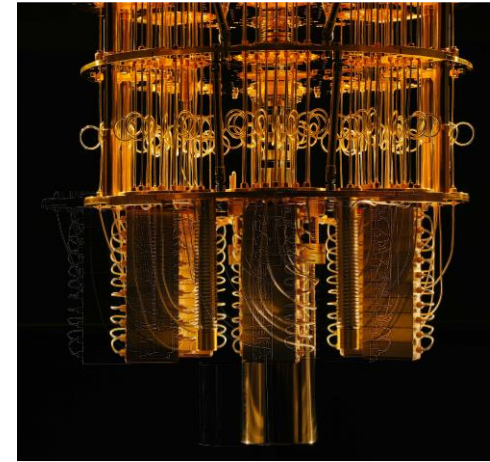
What does this mean for classical crypto algorithms?

Shor's algorithm for factoring and discrete logarithms can completely break the RSA and Diffie-Hellman cryptosystems, and their elliptic-curve-based variants

- To address an attack using Shor's algorithm, we need new Math/Algorithms for classical computers.

Grover's algorithm could be used to speed up an exhaustive search for symmetric keys or reverse engineer a cryptographic hash.

- To address an attack using Grover's algorithm, we need to grow the key and message digest sizes.



Algorithm	Purpose	Impact from quantum computer
DES, TDES	Encryption	No longer secure
AES-256	Encryption	Secure
SHA-256, SHA-3	Hash Functions	Secure
RSA	Signatures, Key Establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Signatures, Key Exchange	No longer secure
DSA (Finite Field Cryptography)	Signatures, Key Exchange	No longer secure

What will a cyber criminal be able to do?

Manipulate updates
and forge
transactions



through fraudulent
authentication

Decrypt lost or
harvested
confidential historical
data



through cracking
encryption keys

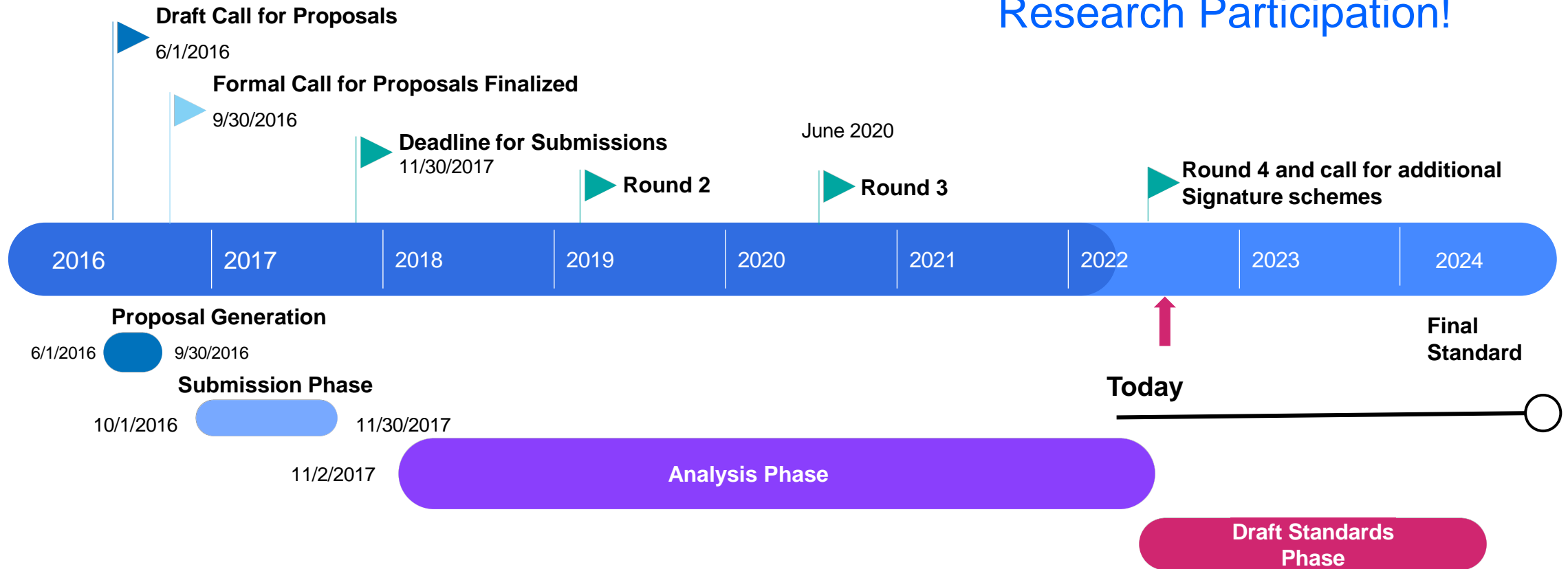
Manipulate legal
history



by forging digital
signatures

NIST standardization for quantum safe cryptography

3 of the 4 Finalist have IBM Research Participation!



- National Institute of Standards and Technology(NIST) initiates process
- Industry communication protocols and other industry specific standards updates will follow based on the publication of the NIST standards
- This will drive client requirements

IBM z16 industry-first quantum-safe system



Quantum-safe technology and key management services were developed to help protect data and keys against a potential future quantum attack like harvest now, decrypt later

Quantum-safe System

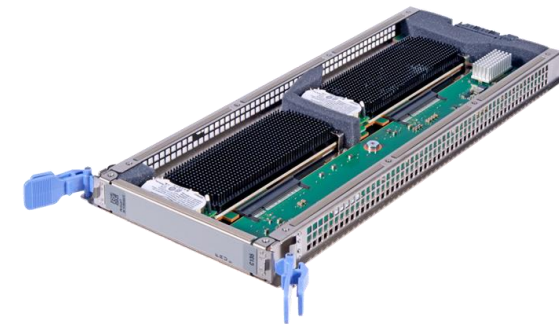
Industry first quantum-safe system protected by quantum-safe technologies through multiple layers of firmware

Helps protect IBM z16 firmware from quantum attacks through a built-in dual signature scheme with no changes required



Protect Sensitive Data

New Crypto Express card with quantum-safe APIs to modernize existing and build new applications leveraging quantum-safe cryptography along with classical cryptography



Crypto Express 8s

Maturity milestones towards quantum-safety

Are you involved in discovering crypto or mitigating issues in the crypto environment?

TODAY



Discover & Classify Data

- Classify the value of your data and identify your critical and sensitive data
- Identify locations of your data
- Understand your compliance requirements
- Create and manage your data inventory with defined ownership

Crypto Inventory

- Identify how your data is encrypted
- Create your cryptography inventory (containing certificates, encryption protocols, algorithms, key lengths, etc.)
- Manage your cryptography inventory and the lifecycle of certificates, encryption keys, etc.

Crypto Agility

- Define and implement processes to update / replace cryptography with well-defined lead-times
- Take all dimensions of crypto agility into account
- Test your crypto agility

Quantum-Safe

- Implement quantum-safe cryptography algorithms
- Understand the performance impact of quantum-safe crypto on the business

z16 tooling to aid crypto inventory

IBM Application Discovery and Delivery Intelligence (ADDI) with Crypto Discovery

- Discover where and what crypto is used in applications
- Aid in migration and modernization planning
- Capture valuable metadata and dependencies

Dynamic Crypto Usage Tracking

- Provides workload correlated crypto usage data for ICSF callers
- New workload correlated crypto usage data for CPACF callers

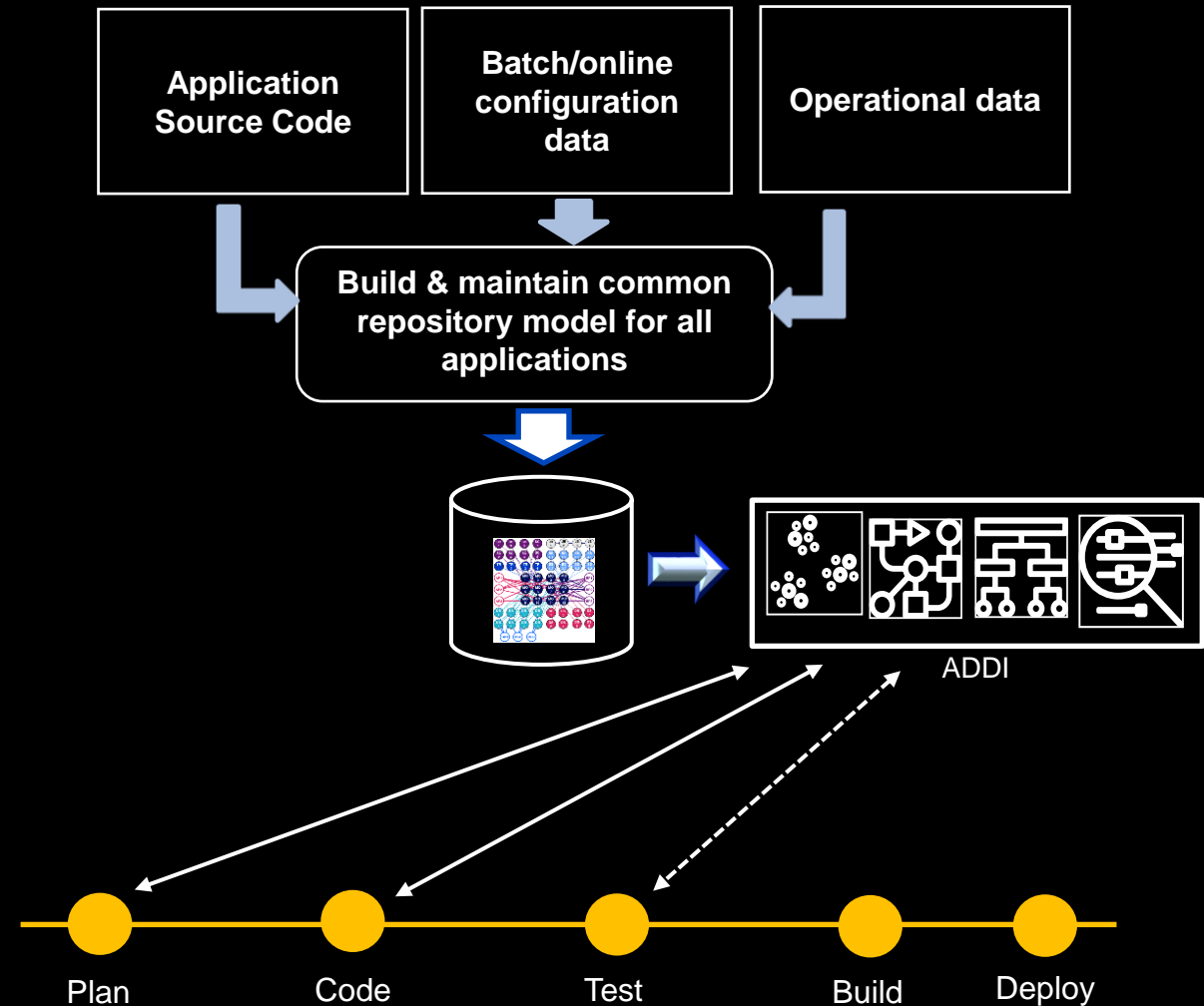
Crypto Analytics Tool

- Provides a cryptographic view with up-to-date monitoring of crypto keys and functions

z/OS Encryption Readiness Technology (zERT)

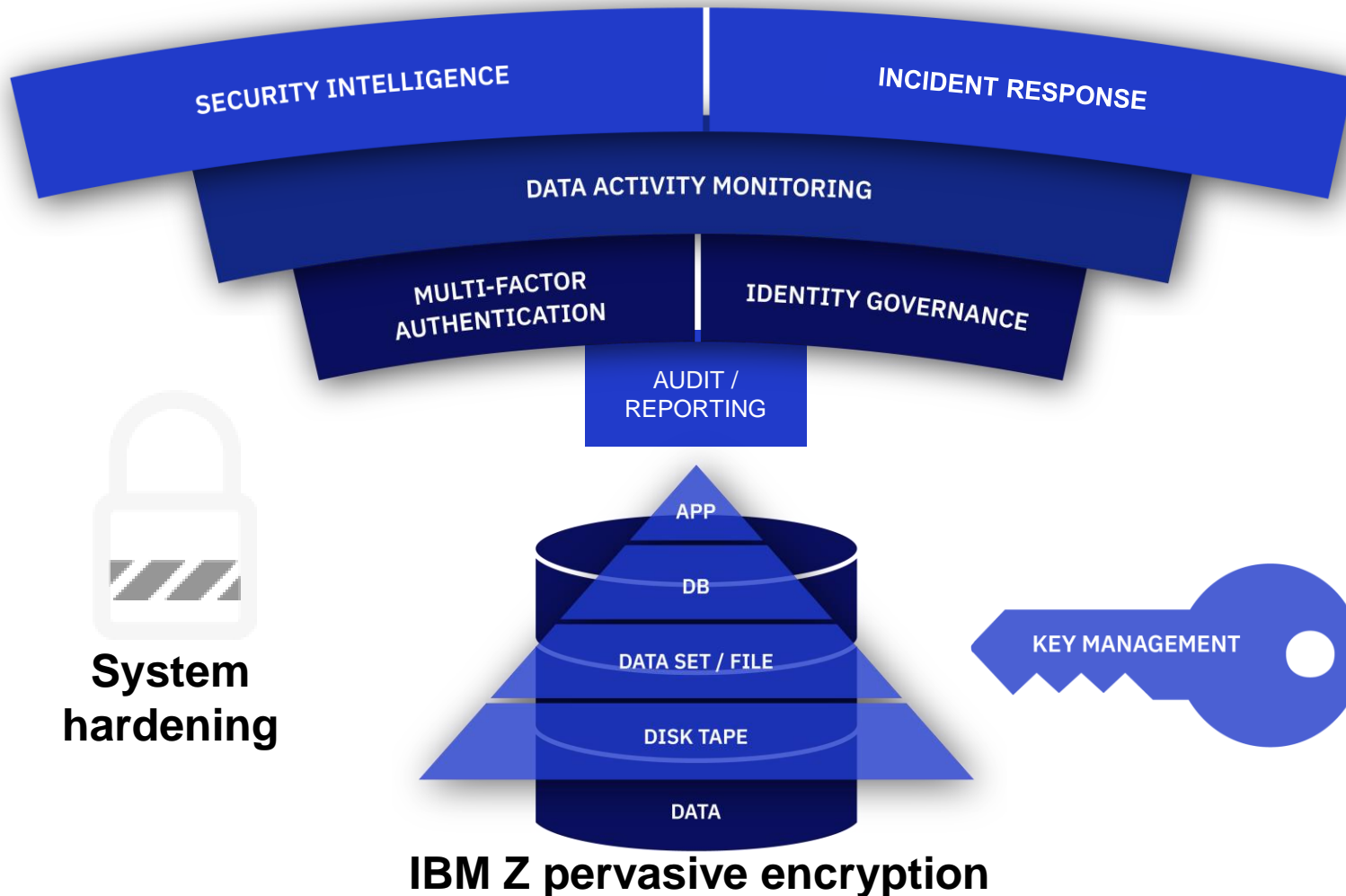
- Answers the question “Which traffic do I have and how is it protected?” – Identifies Security protocols, Crypto algorithms, Key lengths, etc.

Enable crypto discovery with IBM ADDI



ADDI: Application Discovery and Delivery Intelligence
ICSF: Integrated Cryptographic Service Facility
CI/CD: Continuous Integration / Continuous Delivery
UI: User Interface

Cybersecurity strategy requires depth



Traditional workloads and APIs:

- Db2
- IMS
- CICS / VSAM
- MQ

Relevant IBM Security Solutions:

- IBM Security zSecure Suite
- IBM Security QRadar
- IBM Security Guardium
- IBM Security Verify
- IBM Cloud Pak for Security
- IBM Multi-factor Authentication
- IBM Z pervasive encryption
- IBM EKMF Web
- IBM Z Cyber Vault

Thank you !

