IBM CyberVault for IBM Storage Scale: Create a Cyber Secure Environment and Recover in Minutes

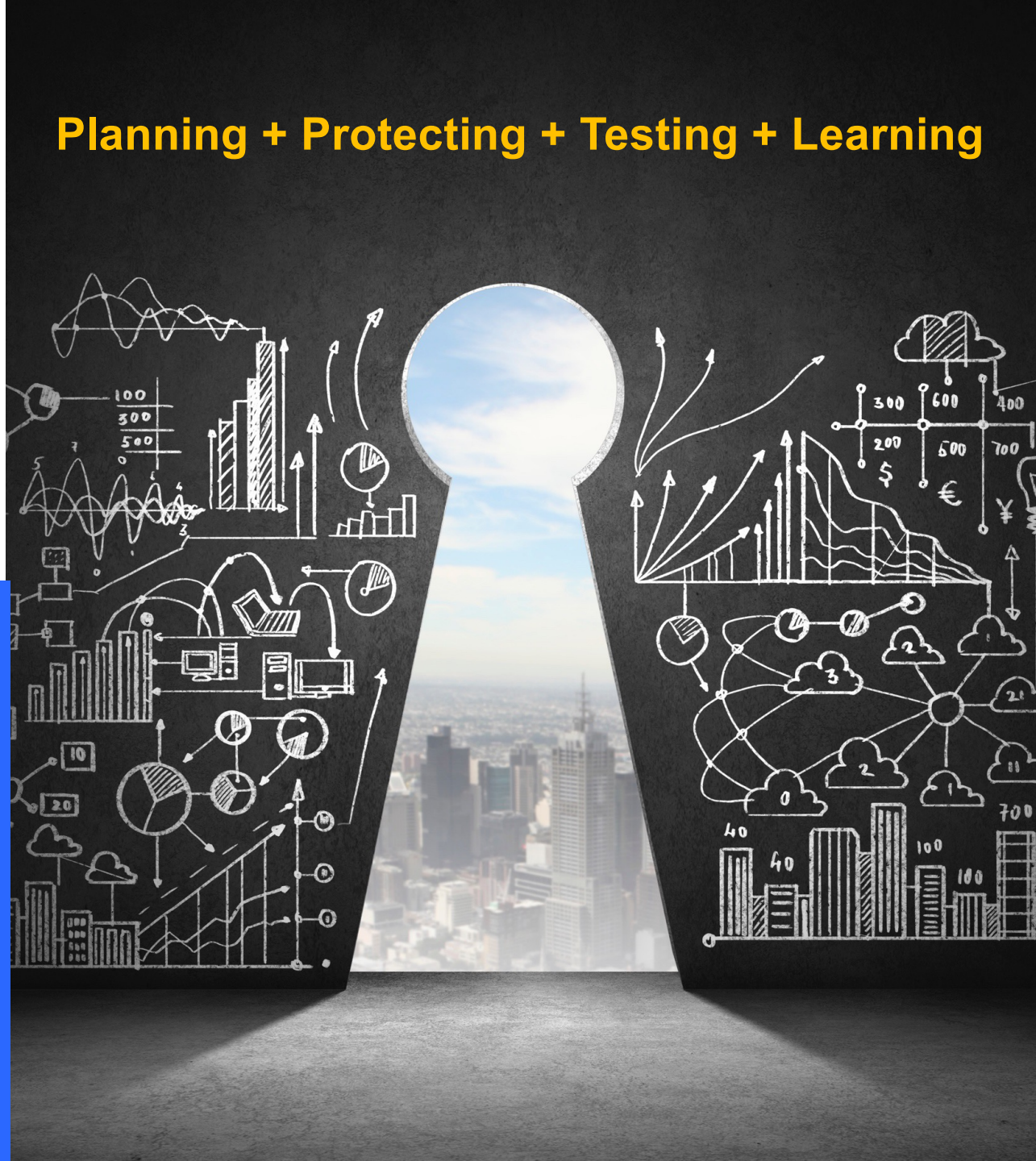
Cyber Resiliency is an Organization's **Ability to Continue** **D**elivering the Intended Outcomes Despite Adverse Cyber Incidents

83%

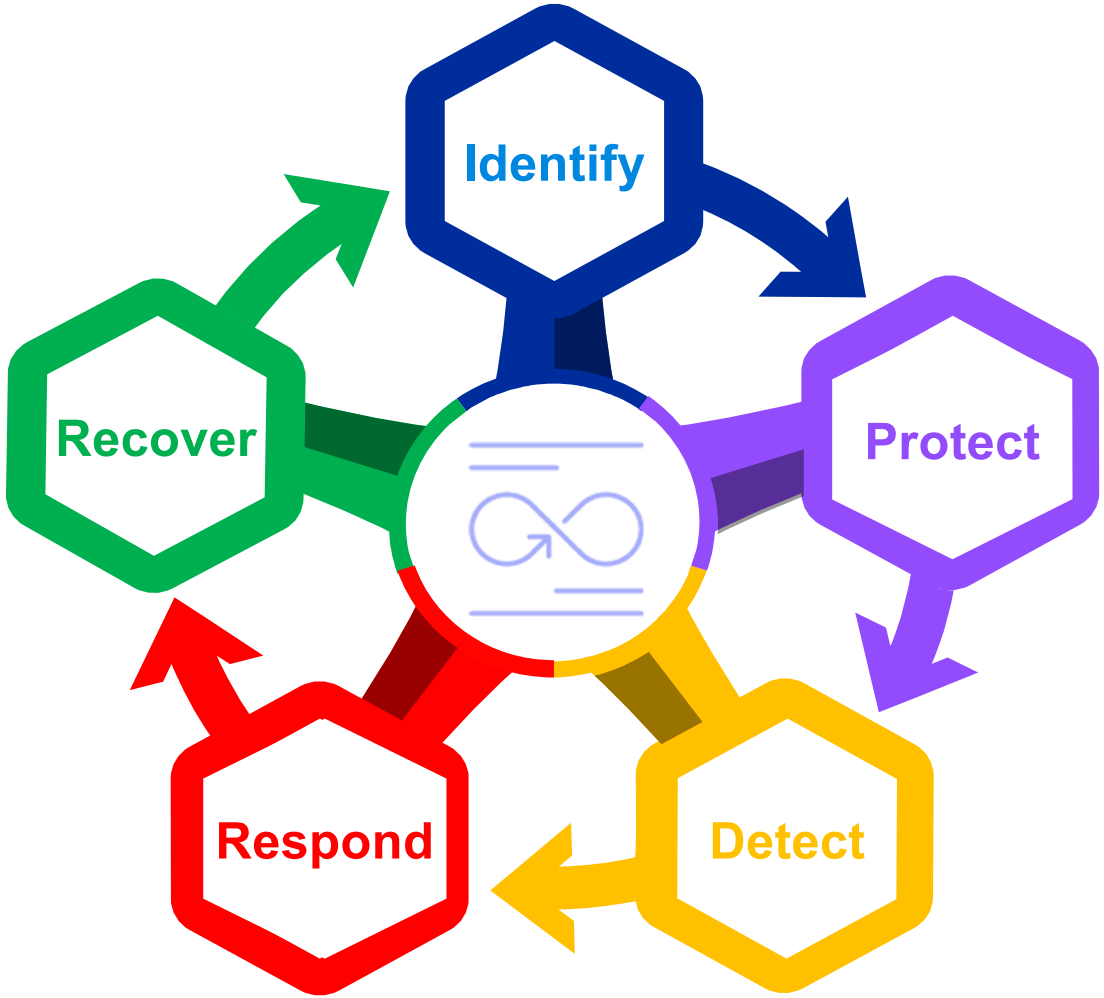
chance of experiencing a data breach

$4.45M

Global average cost of a data breech



Cyber Resilience Lifecycle



National Institute of Standards and Technology (NIST) security framework

Identify critical assets

Protect against vulnerabilities

Detect with continuous monitoring

Respond rapidly

Recover with automation

IBM is More Than a Checkmark with a Cyber Secure Framework

Identify | Protect | Detect | Respond/ Recover

Pre-Attack ← → **Peri-Attack** ← → **Post-Attack**

Attack Surface Reduction

With IBM's Cyber Resilience Assessment

Attack Defense

With Safeguarded Copy air-gapped solutions and and Data Security Services IBM provides all the tools required to protect your data

Attack Prevention

Integrations to AI enhanced IBM QRadar, Guardium, Cloud Pak for Security and other ecosystem partners

Attack Response

With near-instant recovery and one-click response of Safeguarded Copy and as a service option with IBM CyberVault

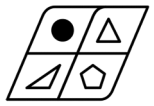
IBM Brings Business Value with a A Global Data Platform

Data Sources


Transactional


Unstructured


Semi-Structured


Mixed Media /Images /Genomics


IoT

A Unified Open Hybrid Cloud Platform

Organizational and Operational Benefits

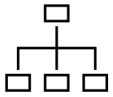

Performance and Cost Optimization


Cyber Secure Lifecyle Management


Global Data Connectivity

Data Services for Operational Agility


Access


Unify


Safeguard


Manage


Integrate

Application and Deployment Flexibility


Edge


Core

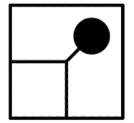

Cloud


Hybrid-Cloud

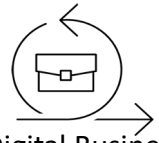
Business Value


Data Monetization


Faster Time to Market

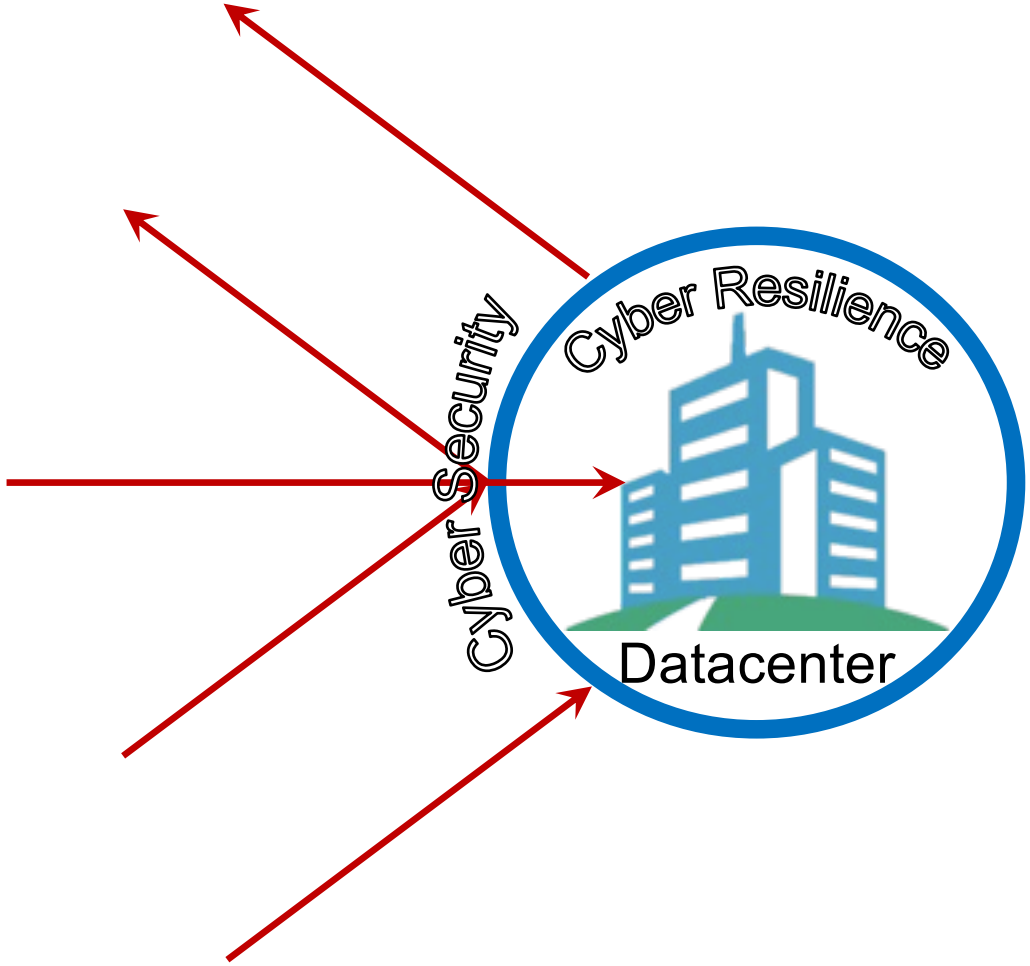

Business Decision


Optimize Resources


Digital Business

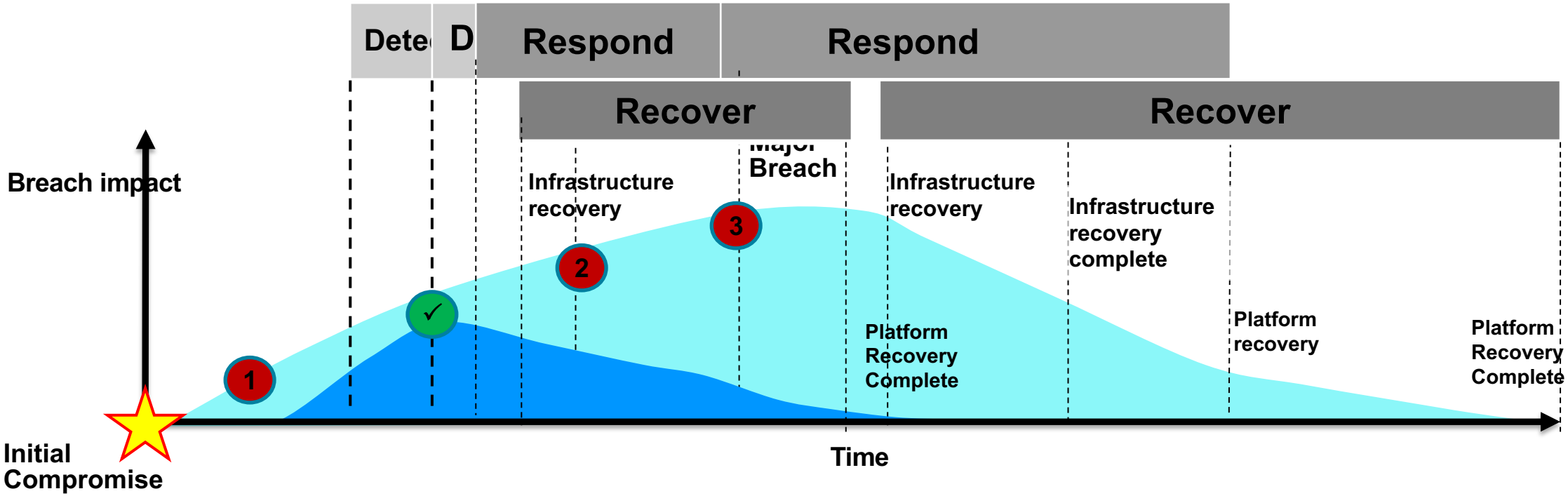
Introduction to Cyber Vault – Design Point

- **Cyber Security** is really all about keeping the bad actors out
- But when they get in, and they will…
- **Cyber Resiliency** is all about rebuilding ***after*** the event has occurred
- **Cyber Vault** adds automation to both Cyber Security and Cyber Resiliency for faster recovery



Introduction to Cyber Vault – Design Point

Cyber Incident Timeline



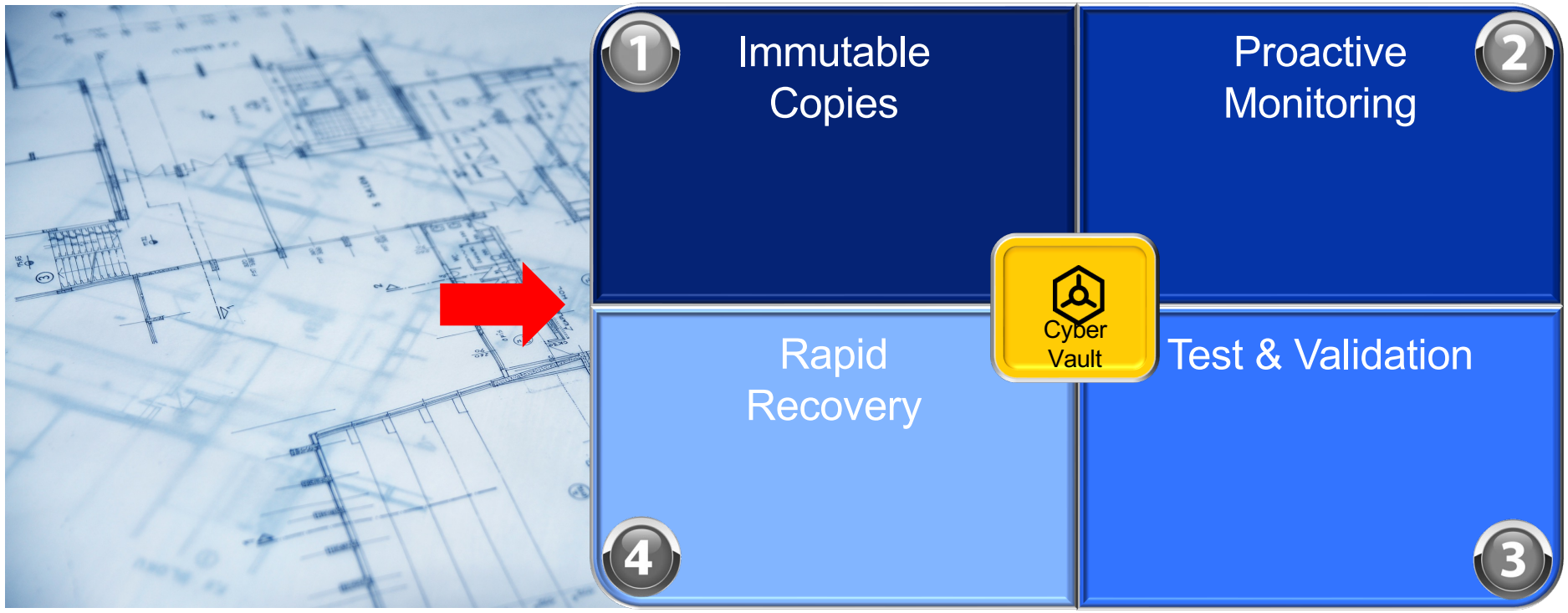
1. Corruption of data occurs - but not yet detected
2. Without the IBM Cyber Vault environment corruption is detected much later and has a greater chance to spread
3. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

IBM Cyber Vault Effect

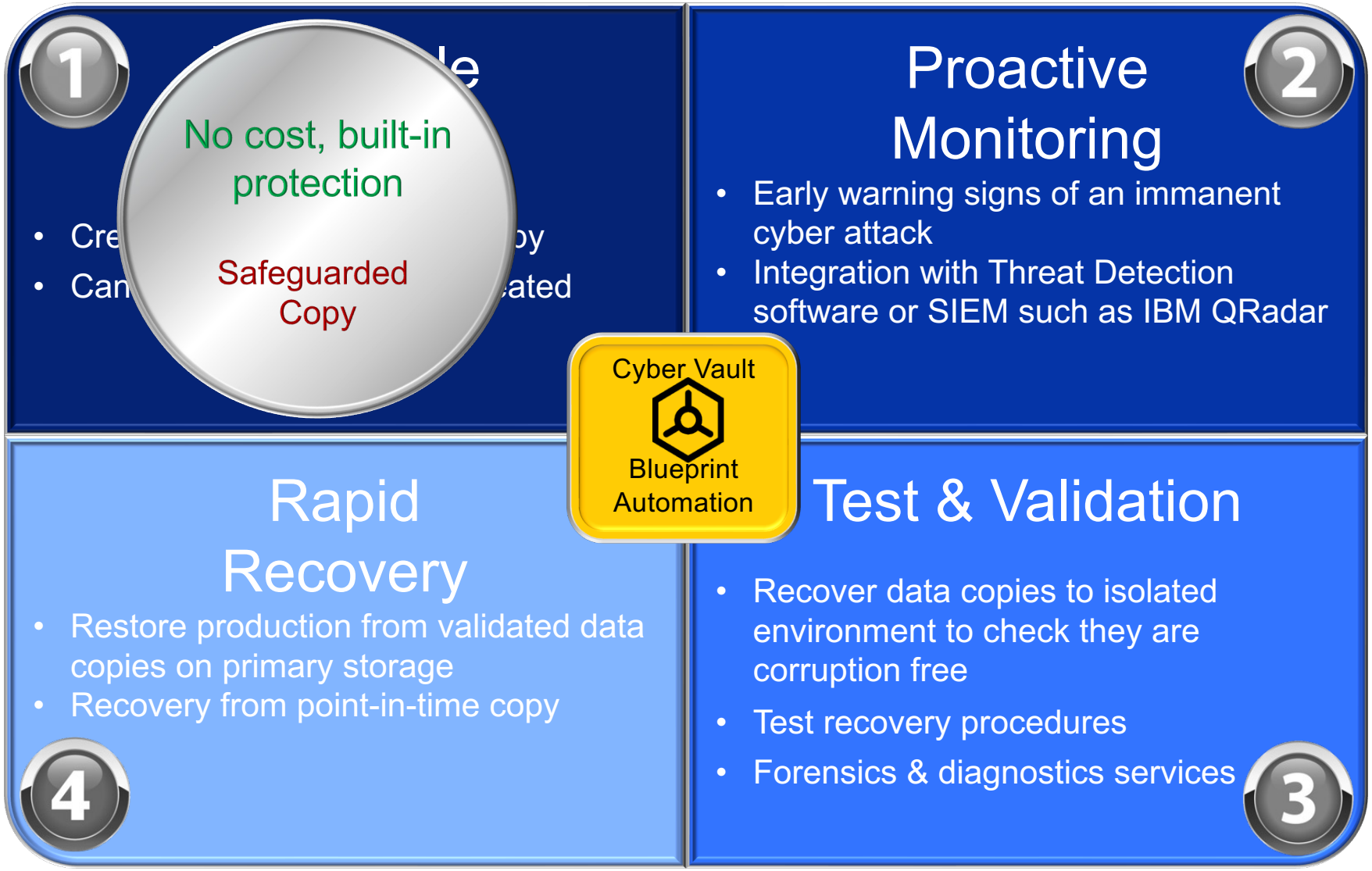
Due to the Cyber Vault environment and the use of Safeguarded Copy technology, data is continuously checked and corruption is found and corrected EARLIER and FASTER

Introduction to Cyber Vault - Blueprint

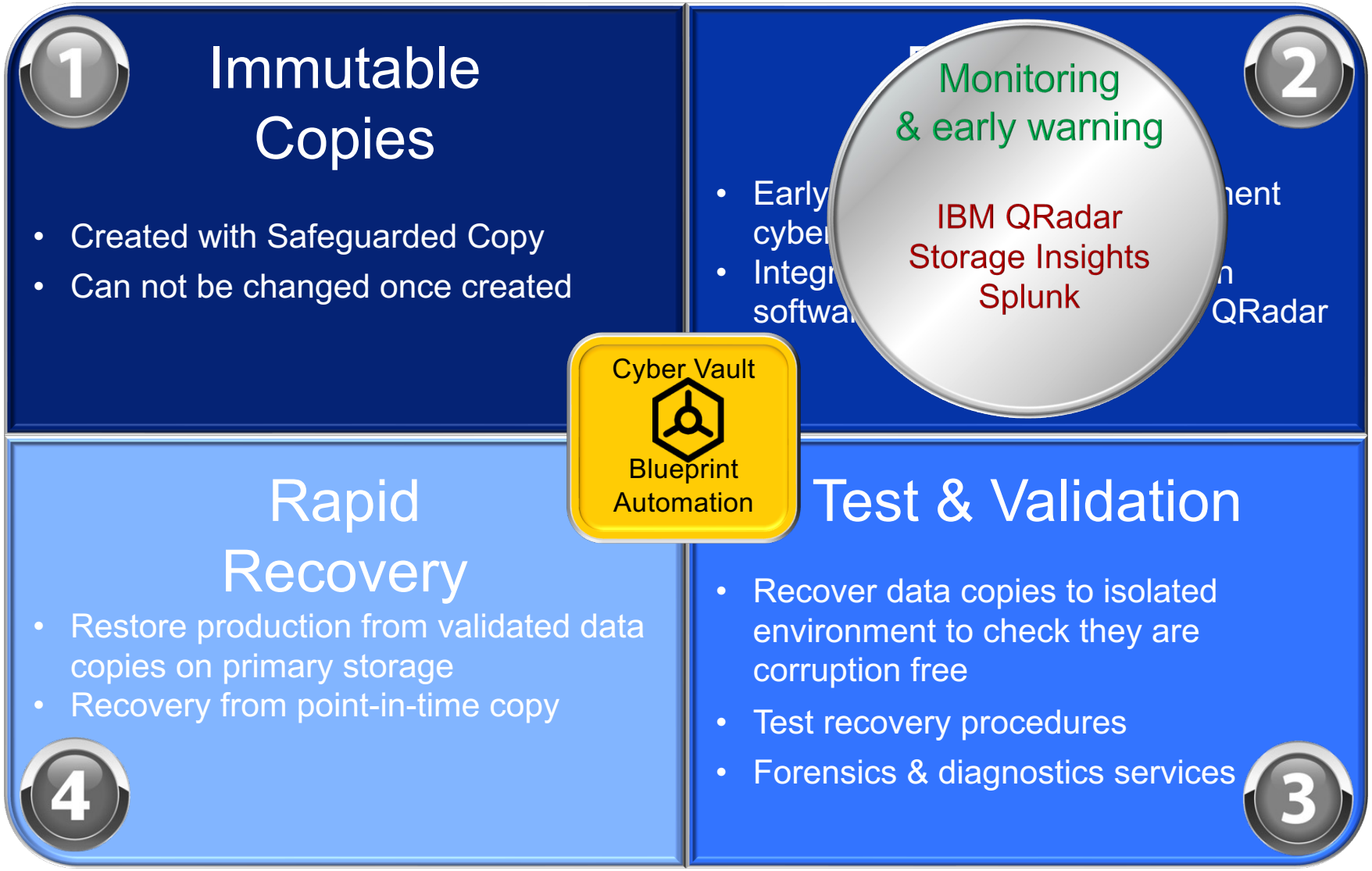
- IBM Storage Scale Cyber Vault is a “blueprint” …not a product!
- Built on storage hardware, software applications and services
- Leverages automation and intelligence to create a cyber security/cyber resiliency solution



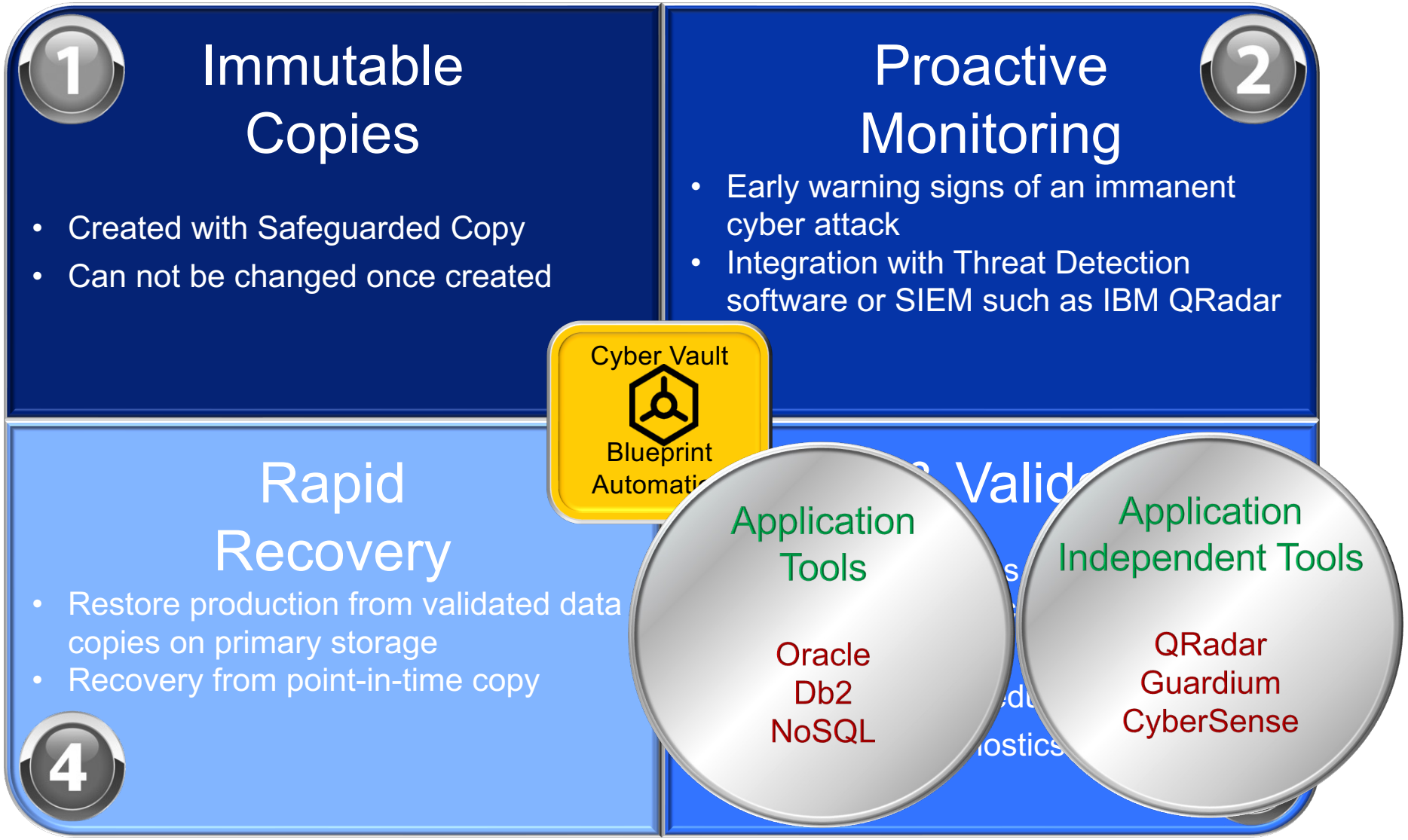
Introduction to Cyber Vault - Blueprint



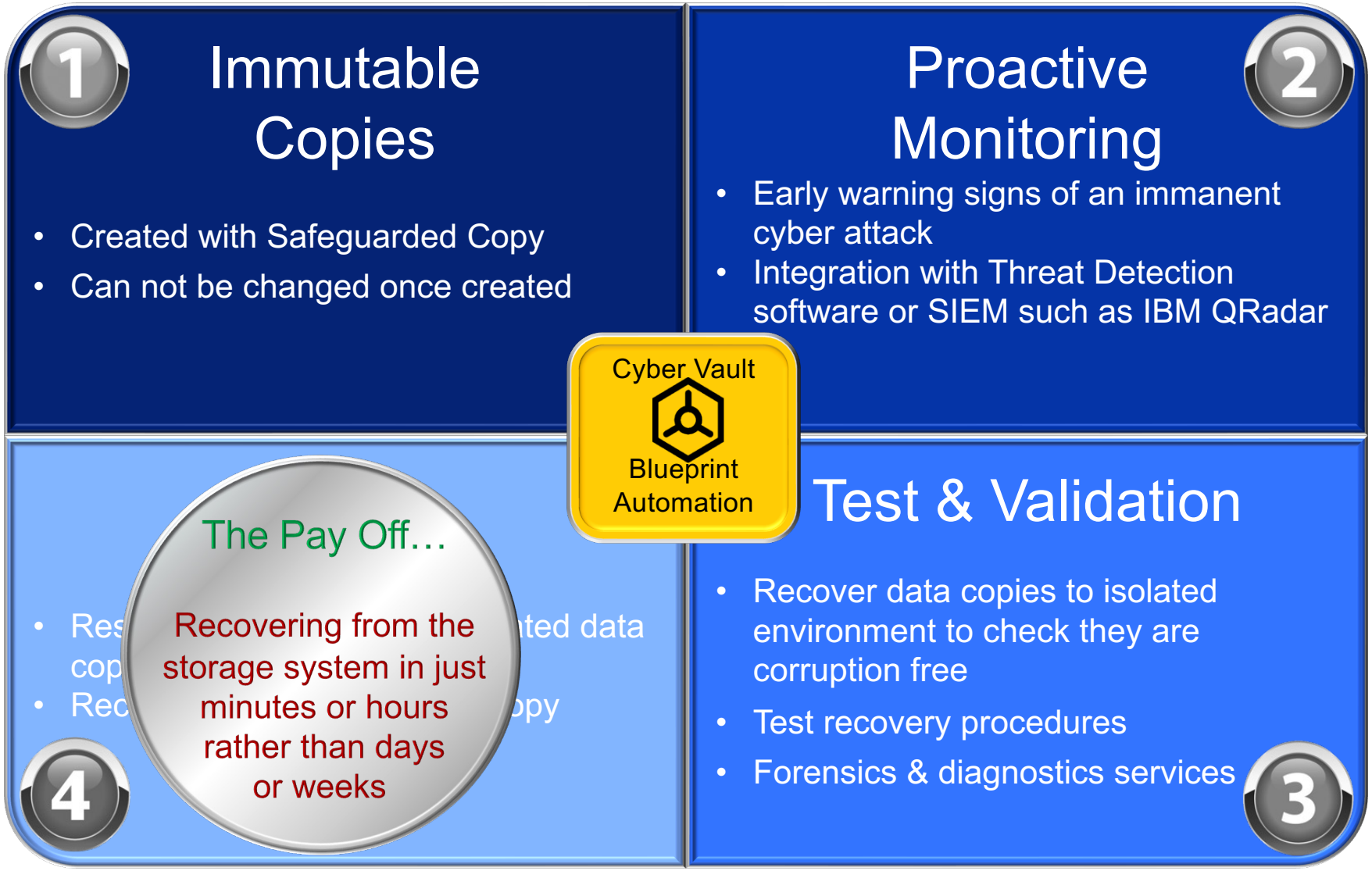
Introduction to Cyber Vault - Blueprint



Introduction to Cyber Vault - Blueprint



Introduction to Cyber Vault - Blueprint



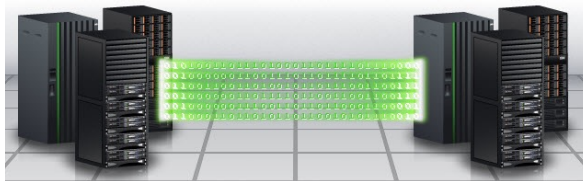
Introduction to Cyber Vault – Core Components

STORAGE

IBM Storage Scale
IBM Storage Scale System

SAFEGUARDED COPY

Immutable Copies protecting from compromised data



SIEM, SOAR & SCRIPTS

Automation, validation and recovery from cyber events

COPY SERVICES MANAGER/ SPECTRUM COPY DATA MANAGEMENT/ INTERNAL SCHEDULER

Manage replication and recovery

Note:

- Cyber Vault is designed to be flexible and modular
- Consider products mentioned here as part of a “CVVD” (Cyber Vault Validated Design)
- Most flexibility with SIEM, SOAR & Scripts
- Component interoperability depends on:
  - Ability to send and receive relevant system information (i.e. syslog data)
  - Ability to initiate activity (i.e. API calls, CLI, etc)

Safeguarded Copy - Basics

What Safeguarded Copy IS:

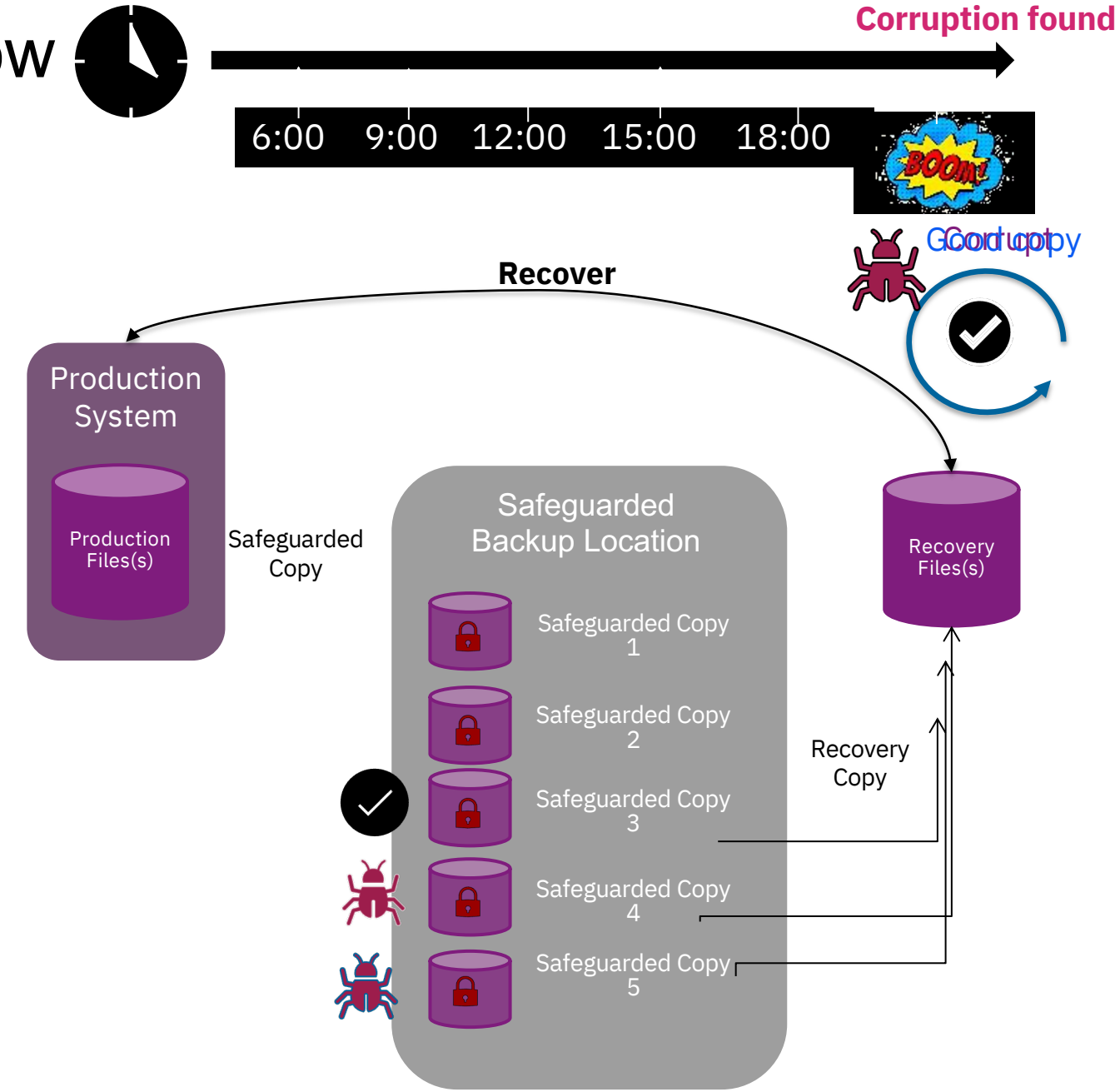
- IS a virtual airgap/isolation solution that uses snapshot functionality to provide additional protection against cyber attacks
- IS primarily used is for “Rapid Ransomware Recovery”
- IS a way to creates immutable, untouchable copies
- IS a snapshot whose data remains invisible and inaccessible to applications until such time as needed
- IS optimized for space through Thin-Provisioning
- IS policy-based and volumes will expire/ “age out” based on retention policy

What Safeguarded Copy IS NOT:

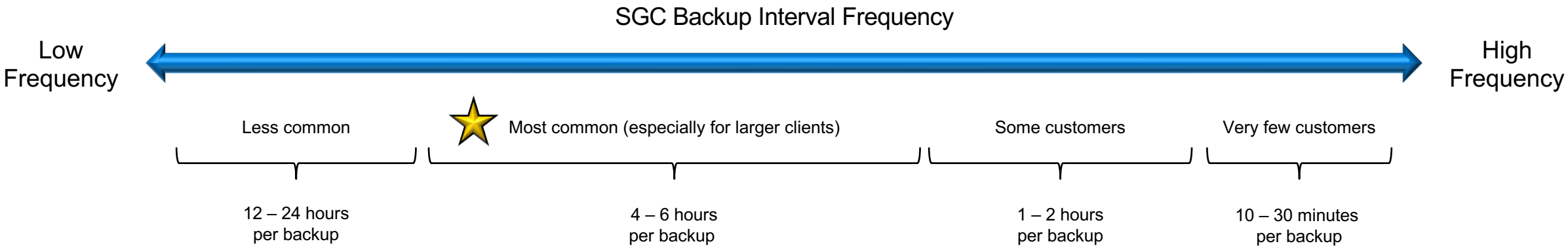
- IS NOT the same thing as Cyber Vault. Safeguard Copy is a ***capability***, Cyber Vault is a ***solution***
- IS NOT a WORM solution. It’s more accurate to say it’s “WORN (”Write Once Read NEVER”)
- IS NOT a separate product. It ***does*** require a Storage Scale DME license, though
- IS NOT a replacement for HA, D/R or Encryption. It should be used in conjunction with all those data protection schemes

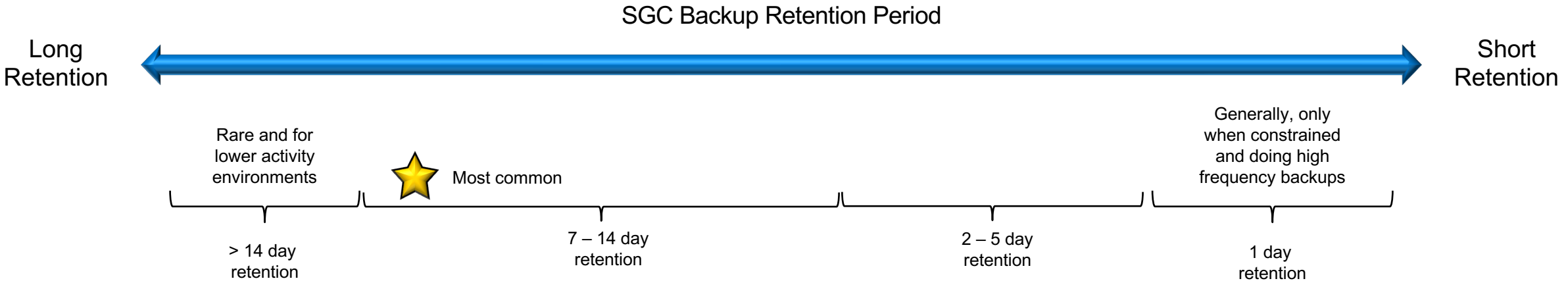
Safeguarded Copy – Workflow

- Logical Corruption Protection to prevent sensitive point in time copies of data from being modified or deleted due to errors, destruction or ransomware
- Not directly accessible to any server or application
- Data is accessible *only* after a Safeguarded copy is recovered to a separate directory.
- Recovery directories are used for:
  - Data validation
  - Forensic analysis
  - Restoration of production data

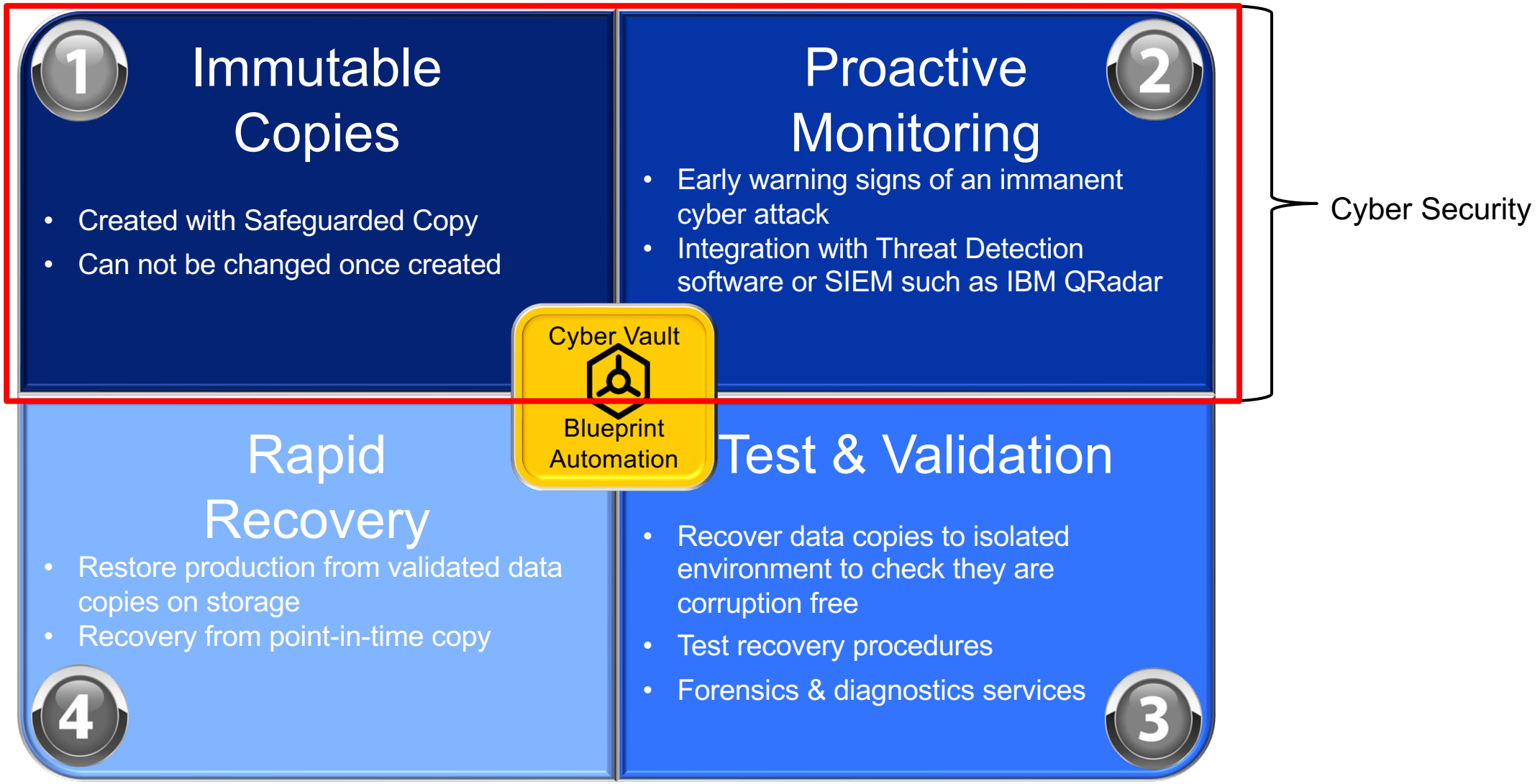


Safeguarded Copy – How Often & How Long

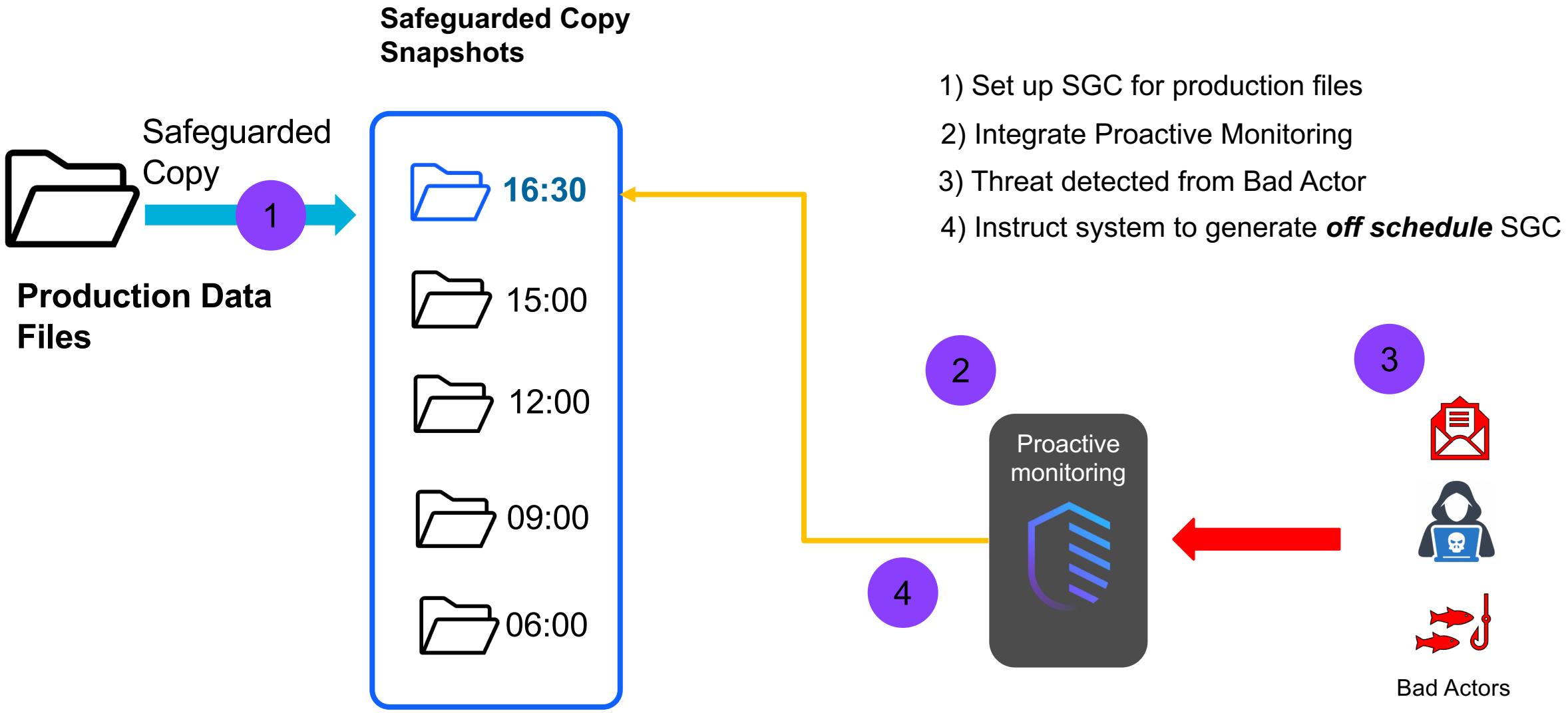




Cyber Vault Threat Detection



Cyber Vault Threat Detection – Workflow



Cyber Vault Threat Detection – SIEM

SIEM (Security Information and Event Management) is a security solution that:

- Helps organizations recognize potential security threats and vulnerabilities BEFORE they can disrupt business operations
- Detects and identifies irregular/anomalous behavior based on rules and access patterns
- Manage and maps incidents, catalogs events and initiates response

Core SIEM functionality :

- Log management
- Event Correlation and Analysis
- Incident monitoring and security alerts
- Compliance management and reporting

Cyber Vault Threat Detection – Available Tools

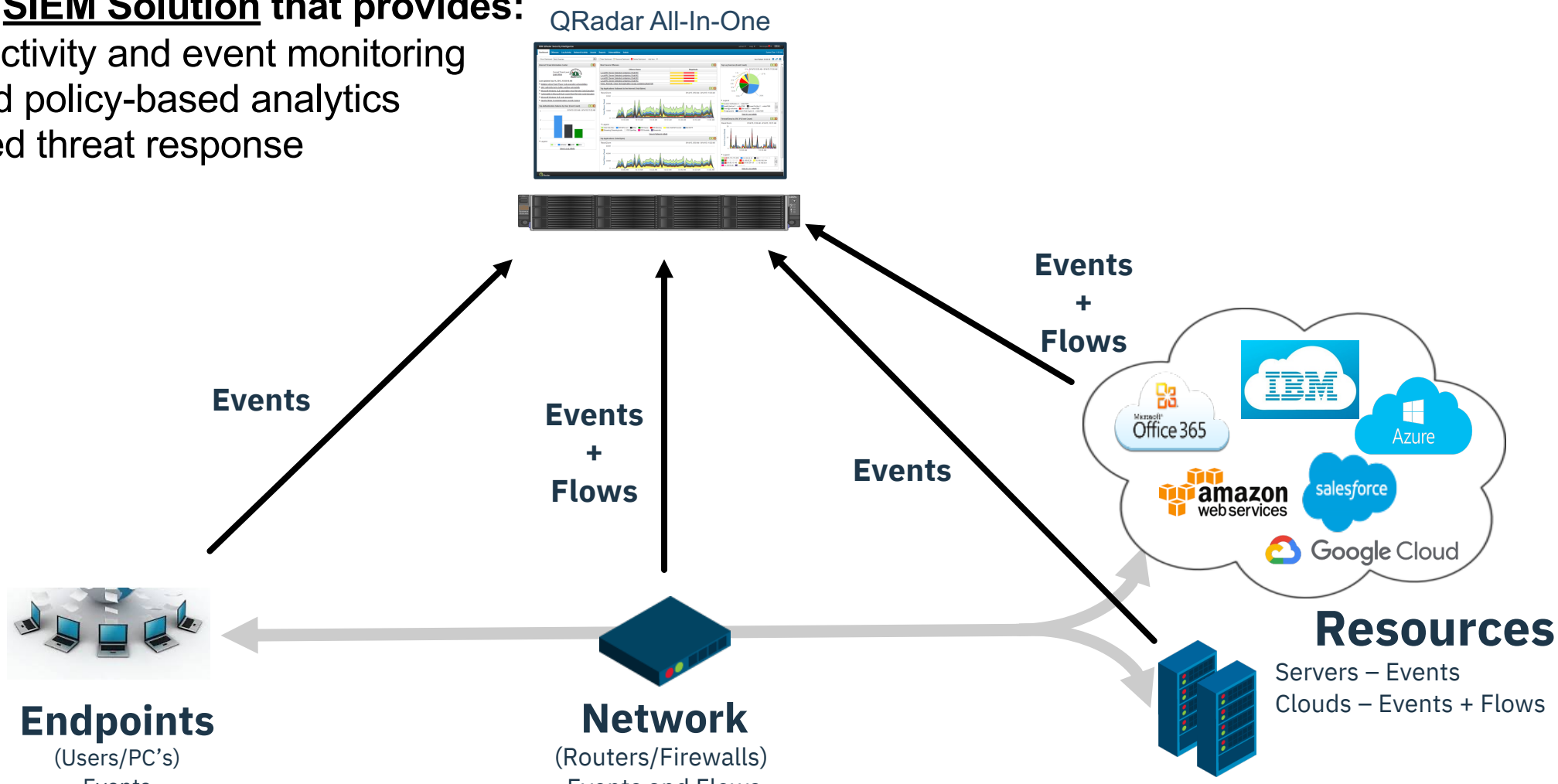
Hardware Monitoring	Application Monitoring	Event Monitoring
Storage Scale Actively monitor **alterations in storage filesystems/files** and **changes in performance** as an indicator that data is being tampered • Monitor storage activity in real time • Set up thresholds • Alerting	**Guardium** **Real-time monitoring** of data activity for **immediate response** to breaches or suspicious behavior • Classify sensitive data • Data source analytics • Centralize security management	**QRadar** Actively monitoring **user activity and syslogs**, patterns and operations (control path) • Receive syslog data • Set up rules-based alerts • Execute response based on anomalous activity

Note: These products are NOT your only choices in a Cyber Vault solution!

Cyber Vault Threat Detection – QRadar

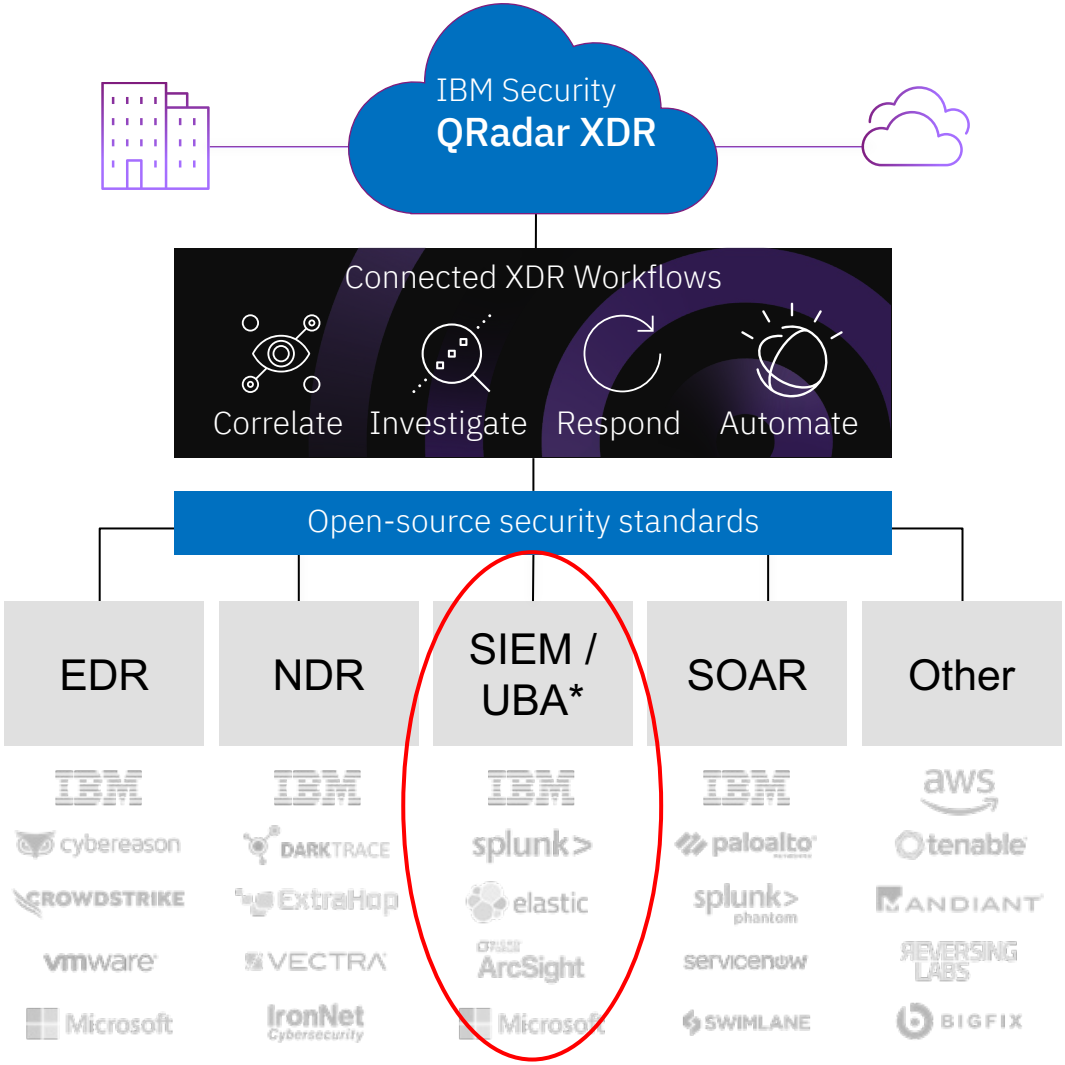
QRadar is a <u>SIEM Solution</u> that provides:

- System activity and event monitoring
- Rules and policy-based analytics
- Automated threat response



Cyber Vault Threat Detection – QRadar

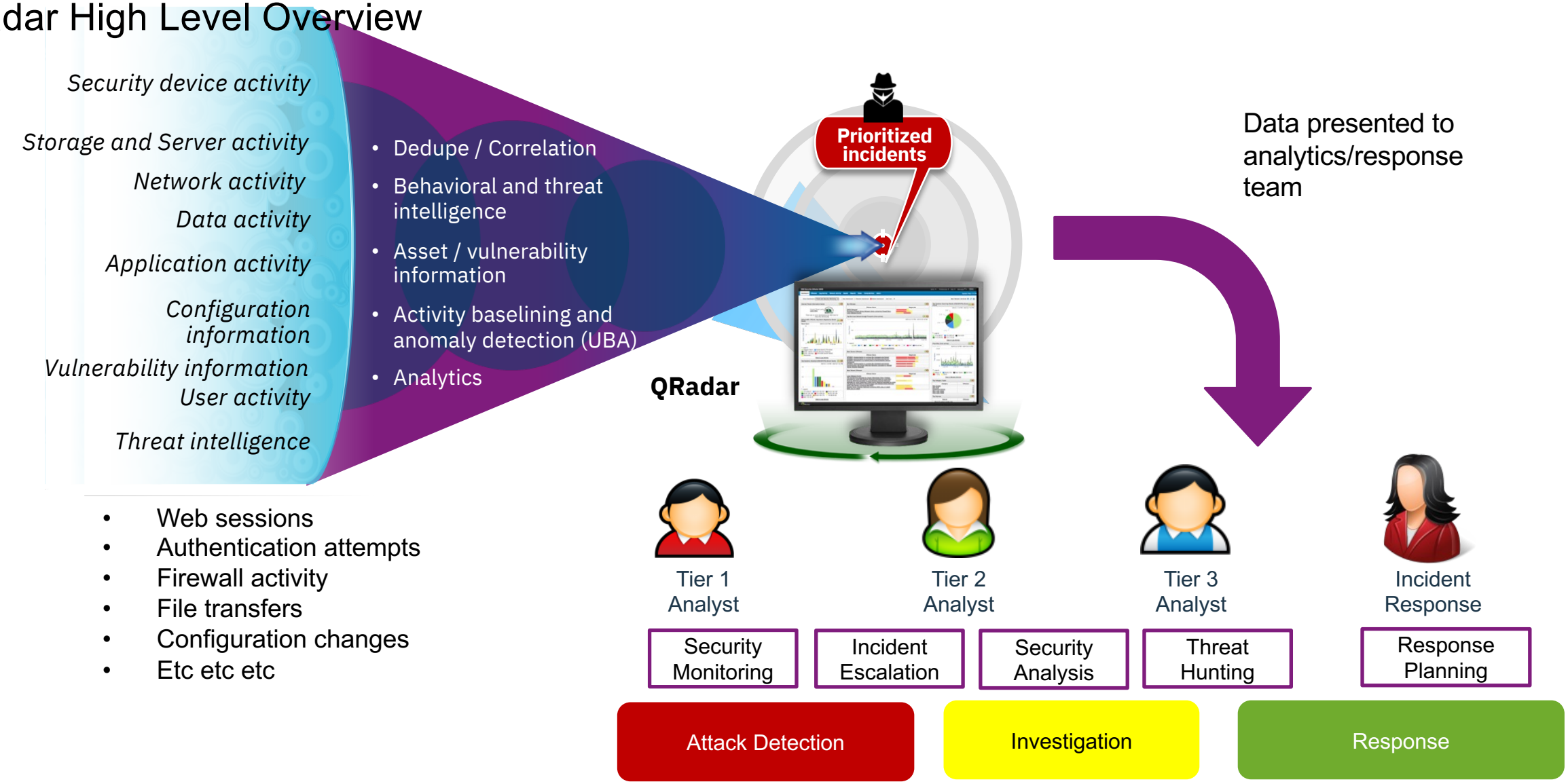
QRadar Product Suite



*User Based Analytics

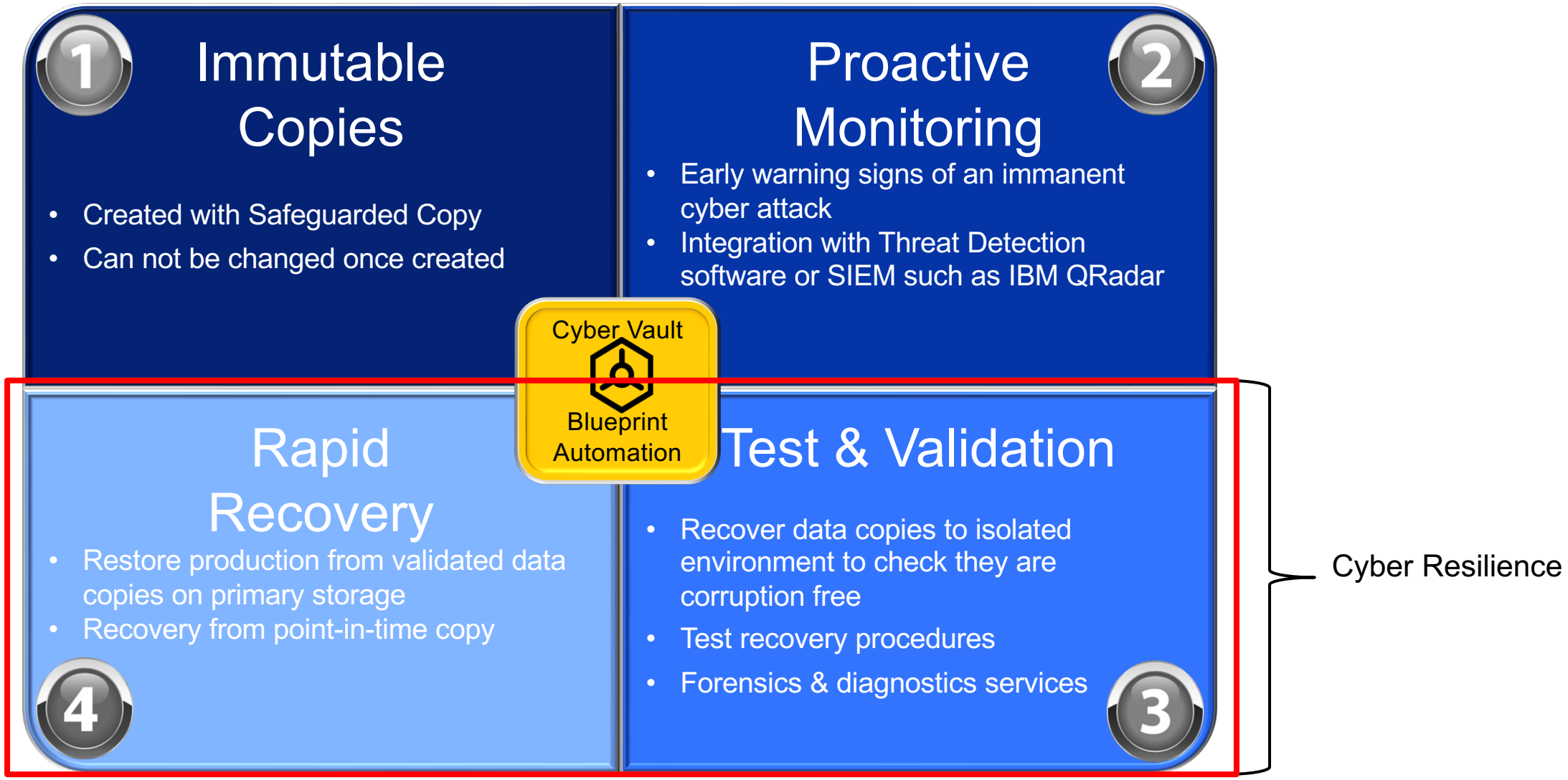
Cyber Vault Threat Detection – QRadar

QRadar High Level Overview

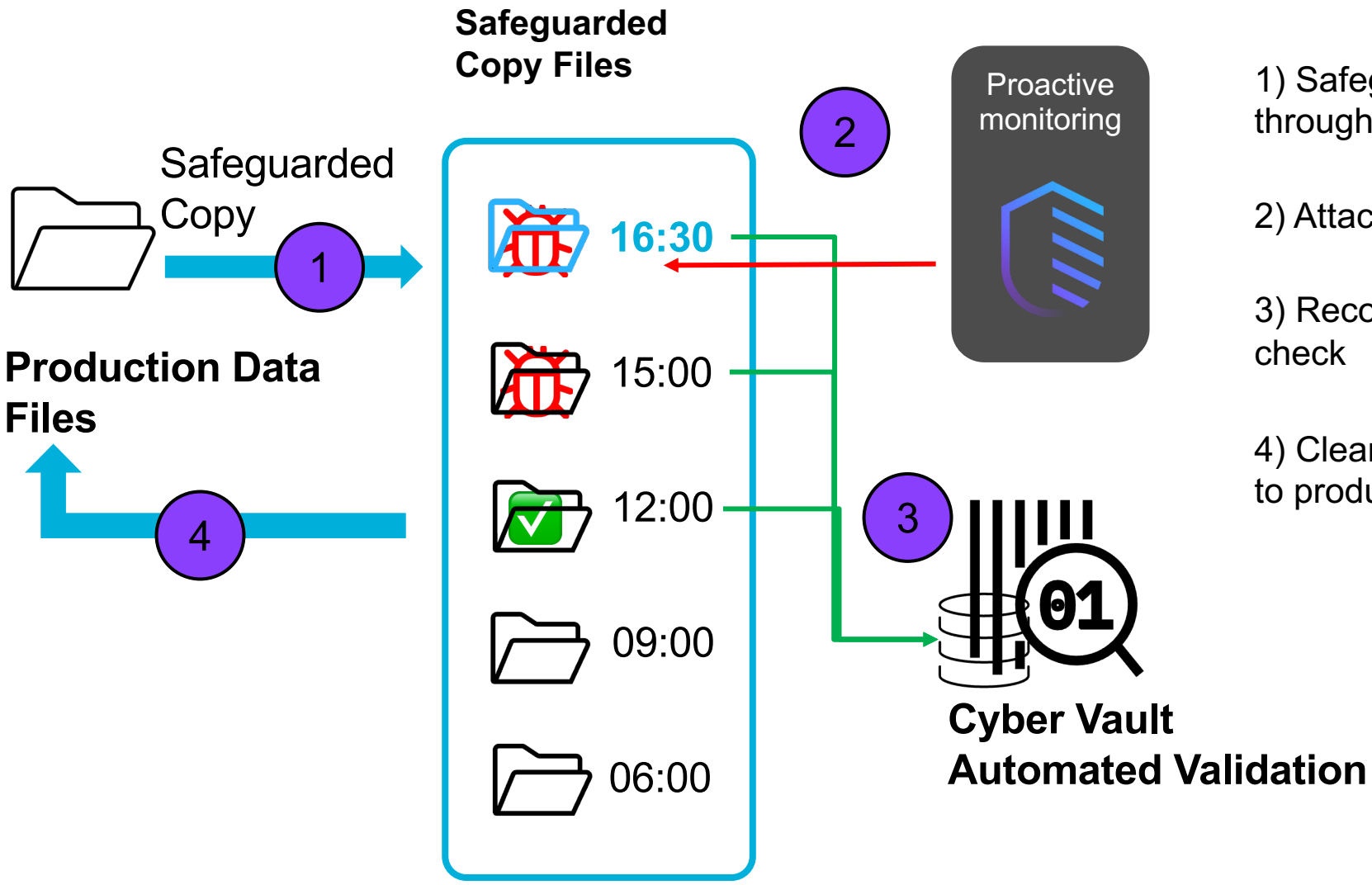


- Web sessions
- Authentication attempts
- Firewall activity
- File transfers
- Configuration changes
- Etc etc etc

Cyber Vault Data Recovery



Cyber Vault Data Recovery - Workflow



1) Safeguarded immutable copies created throughout the day

2) Attack detected by monitoring software

3) Recovery files attached to validation check

4) Clean copy quickly identified and restored to production

Cyber Vault Data Recovery - SOAR

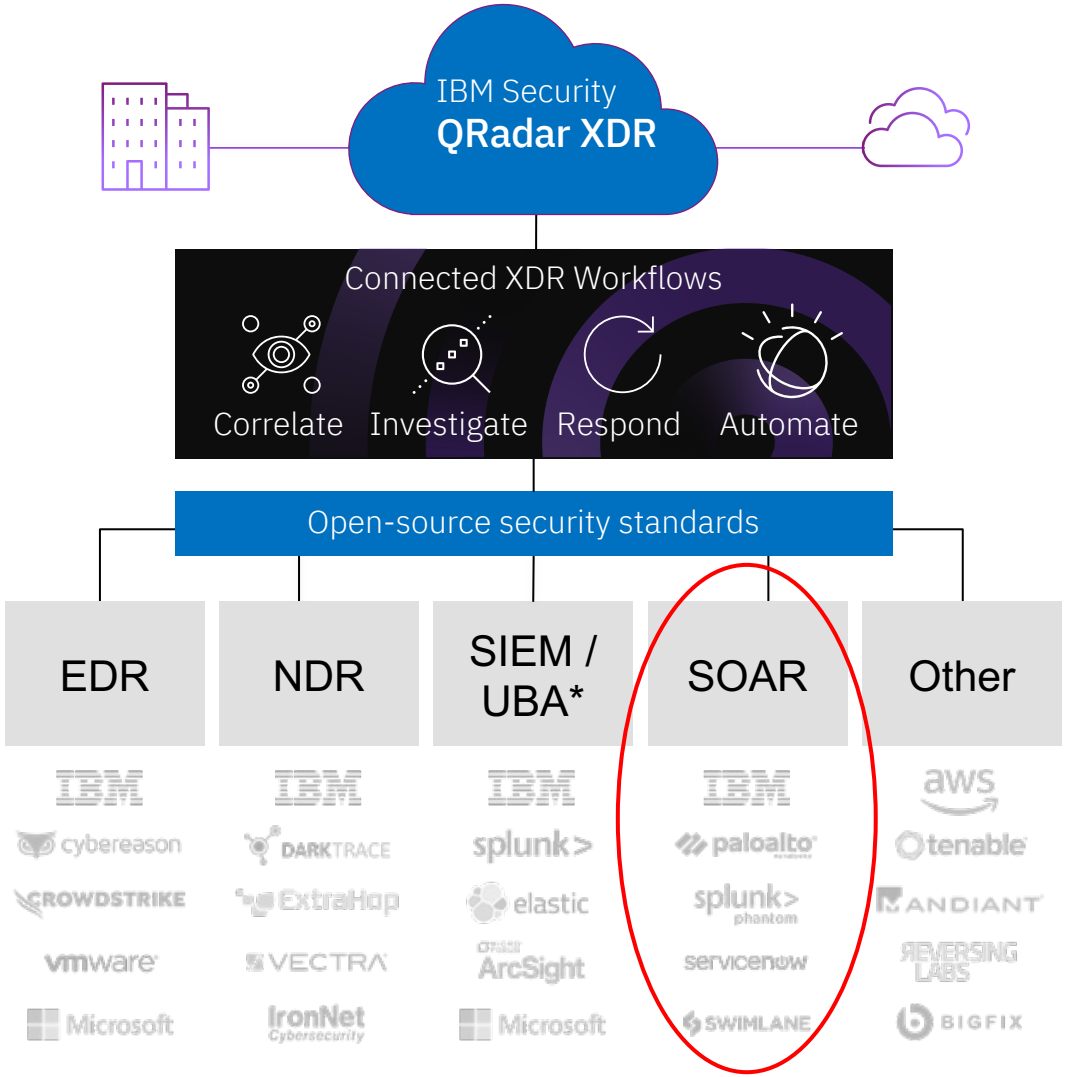
SOAR (Security Orchestration and Automated Response) is a security solution that:

- Automate manual and repetitive tasks to reduce time between threat detection and remediation
- Streamlines incident workflow process to improve the response and recovery efficiency
- Leverage analytics to provide steps to triage and contain threats

Core SOAR functionality :

- Create response workflows
- Receive SIEM data for alerts, analysis or response initiation
- Deploy packaged and/or customized playbooks
- Enable domain-level device/application integration

Cyber Vault Data Recovery – QRadar SOAR

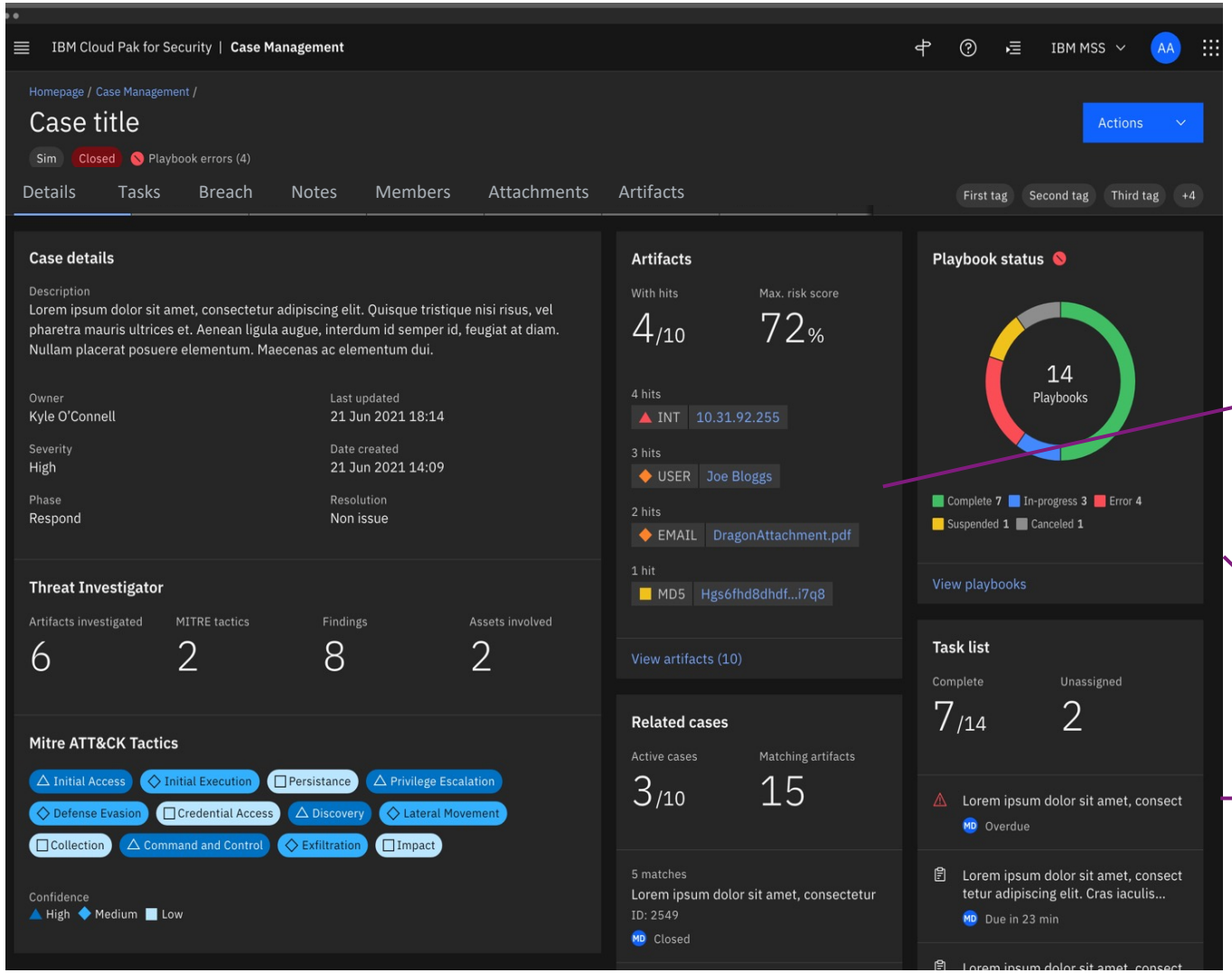


- QRadar SIEM is used primarily for event management, mapping and cataloging
- QRadar SOAR is utilized primarily for response, response management, triage and resolution
- There CAN be some overlap between the two solutions

*User Based Analytics

Data Recovery - QRadar SOAR

Information from SIEM passed to dashboard for response and remediation



What happened and how severe is this?

What are the highest priority systems involved?

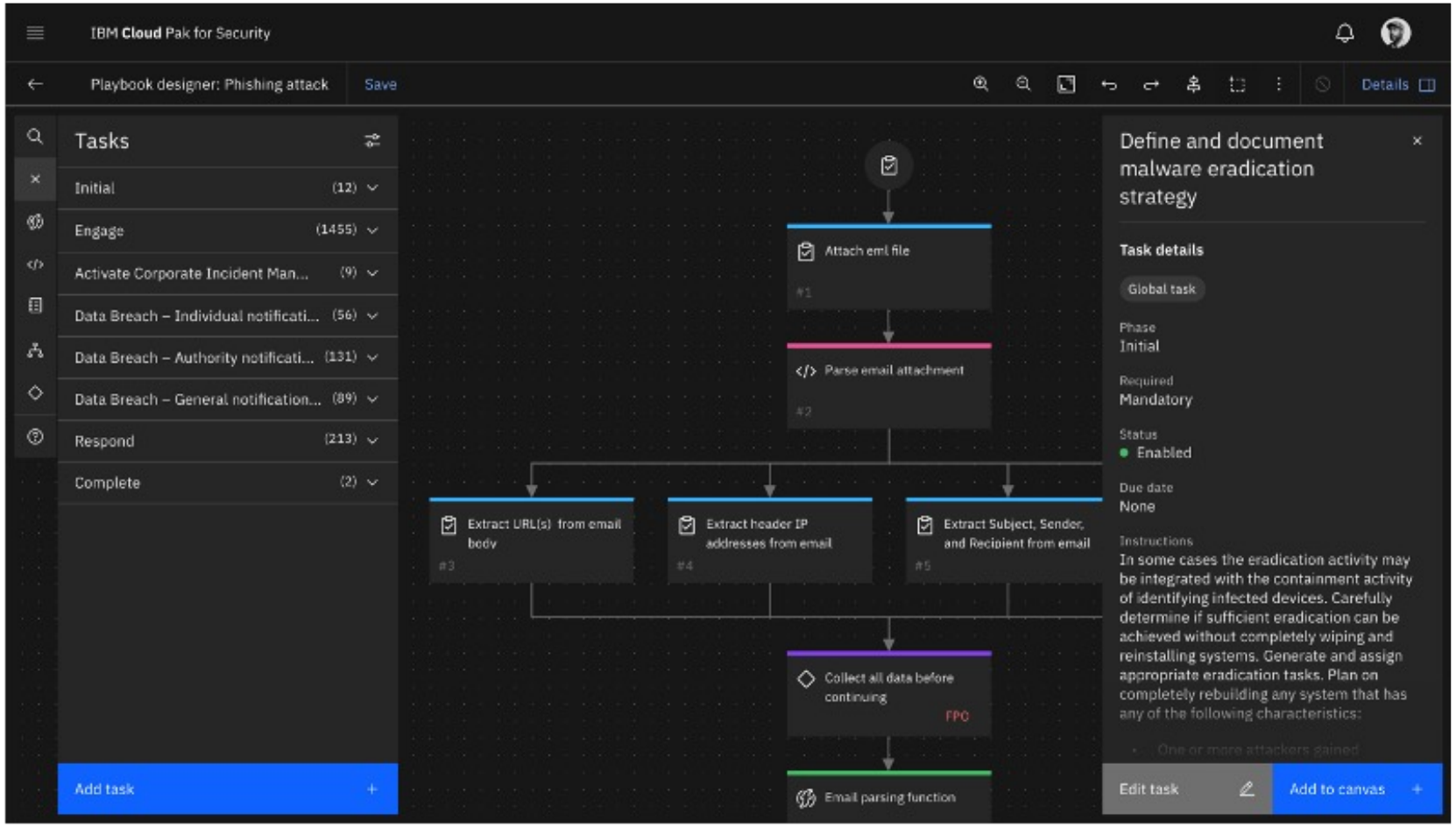
MITRE TTP framework analysis

What action has been taken and what are next steps?

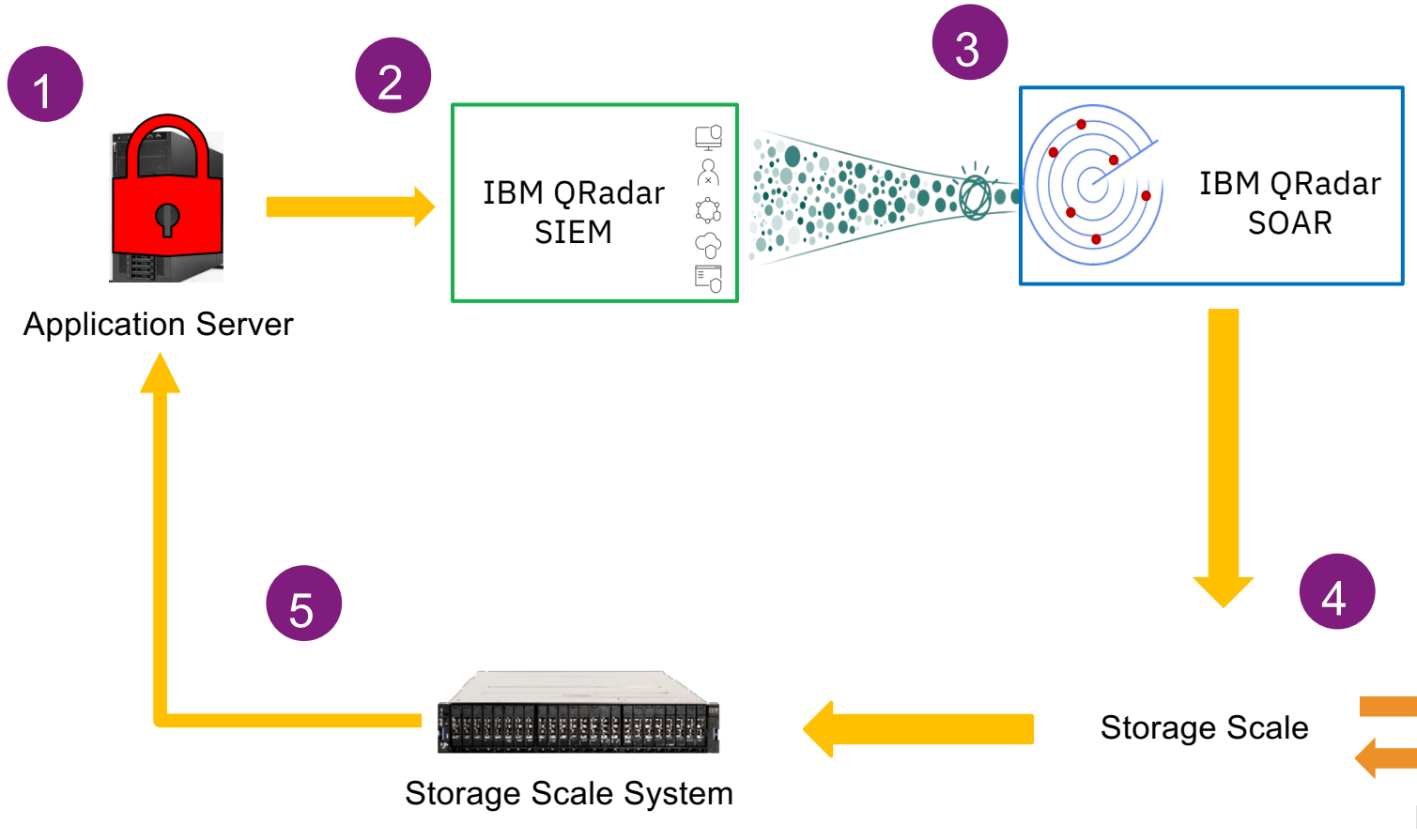
Cyber Vault Data Recovery – QRadar SOAR

Custom Playbook designer:

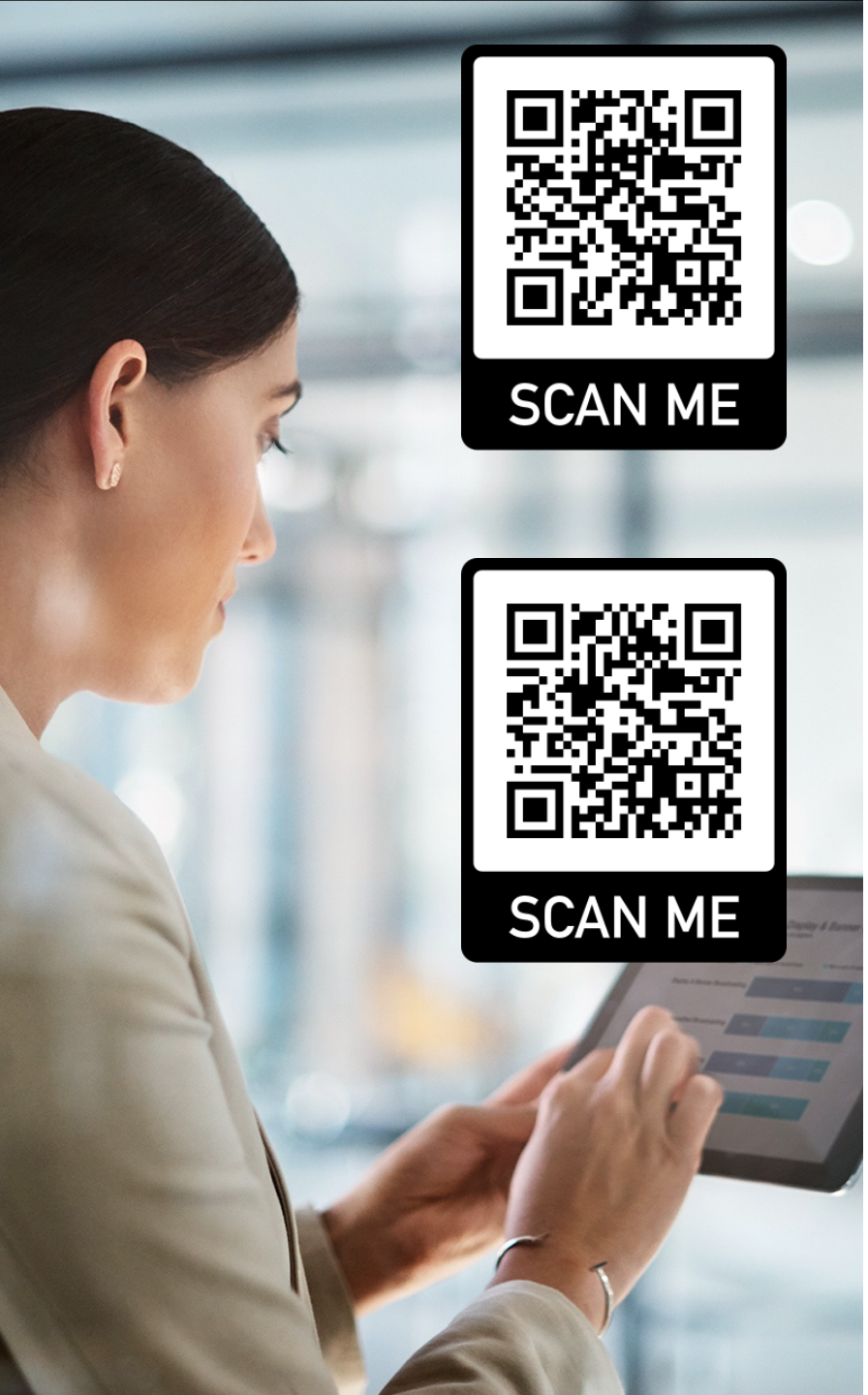
- Modern canvas to easily build and manage automations
- Dynamic playbooks with automatic or manual triggers
- Import and export playbooks between systems
- Standardize activities and accelerate development with reusable sub-playbooks



Cyber Vault Data Recovery – QRadar SOAR Example



1. Application server sends log data to QRadar SIEM
2. Ransomware alert triggered!
3. Alert sent to QRadar SOAR which executes workflow/playbooks
4. QRadar SOAR initiates CSM to recover SGC volumes from Storage Scale System to recovery server. Validate until “good copy” is found
5. Recovers good copy back to application server



Time to Stop Reacting and Create a Cyber Secure Data Strategy with a Global Data Platform

Learn more about IBM Storage for Data and AI Workloads

- IBM Storage Data and AI web page

Learn more about IBM Storage for NVIDIA

- IBM Storage and NVIDIA web page

Learn more about IBM's Global Data Platform foundation

- IBM Storage Scale System web pages
- IBM Storage Scale web page