Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025
IBM Innovation Studio Paris

IBM Power CyberVault

18 novembre

Antoine Maille
IBM France
amaille@fr.ibm.com

Mathieu Ferre
IBM France
mathieu.ferre@ibm.com

Guillaume Legmar
IBM Techzone
guillaume.legmar@fr.ibm.com

IBM

common FRANCE

La Cyber Criminalité
est déjà bien organisée … et vous ?

59% des organisations frappées par une attaque ransomware en 2024*

94% des victimes précisent que les attaquants ont d'abord ciblé **leur sauvegarde***

70% des attaques consistent au chiffrement des données*

78% Des victimes ont mis plus de 100 jours pour s'en remettre**

$4.88M Cout moyen d'une attaque**

56% Payent pour récupérer leurs données*

* Source: Sophos The State of Ransomware 2024
** Source: IBM Cost of a Data Breach 2024

Comment/Pourquoi aborder le sujet maintenant ?

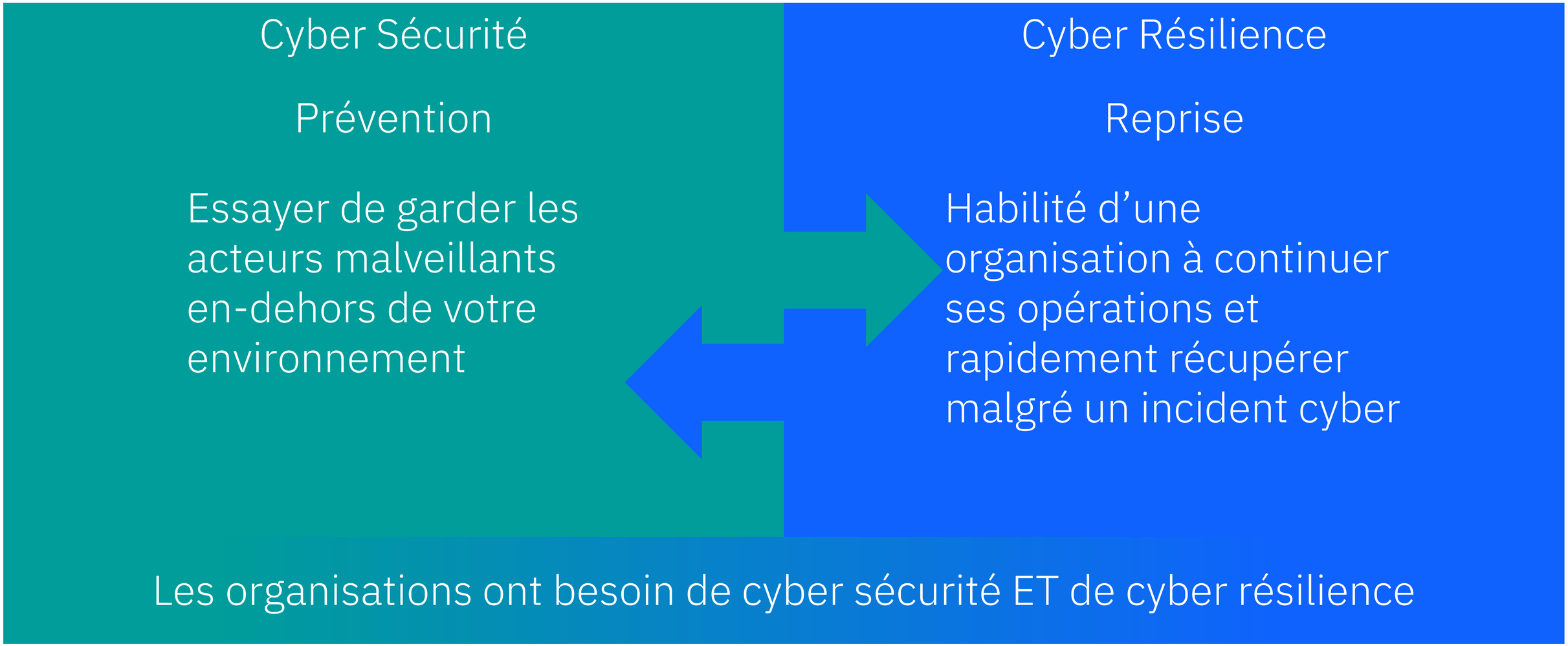
La survie de votre entreprise peut en dépendre

ANSSI :
https://cyber.gouv.fr/publications/les-regles-dor-de-la-sauvegarde
https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation

NIS-2 :
https://cyber.gouv.fr/la-directive-nis-2
https://monespacenis2.cyber.gouv.fr/simulateur

DORA : Digital Operational Resilience Act
https://www.ibm.com/topics/digital-operational-resilience-act

Cyber Sécurité and Cyber Résilience



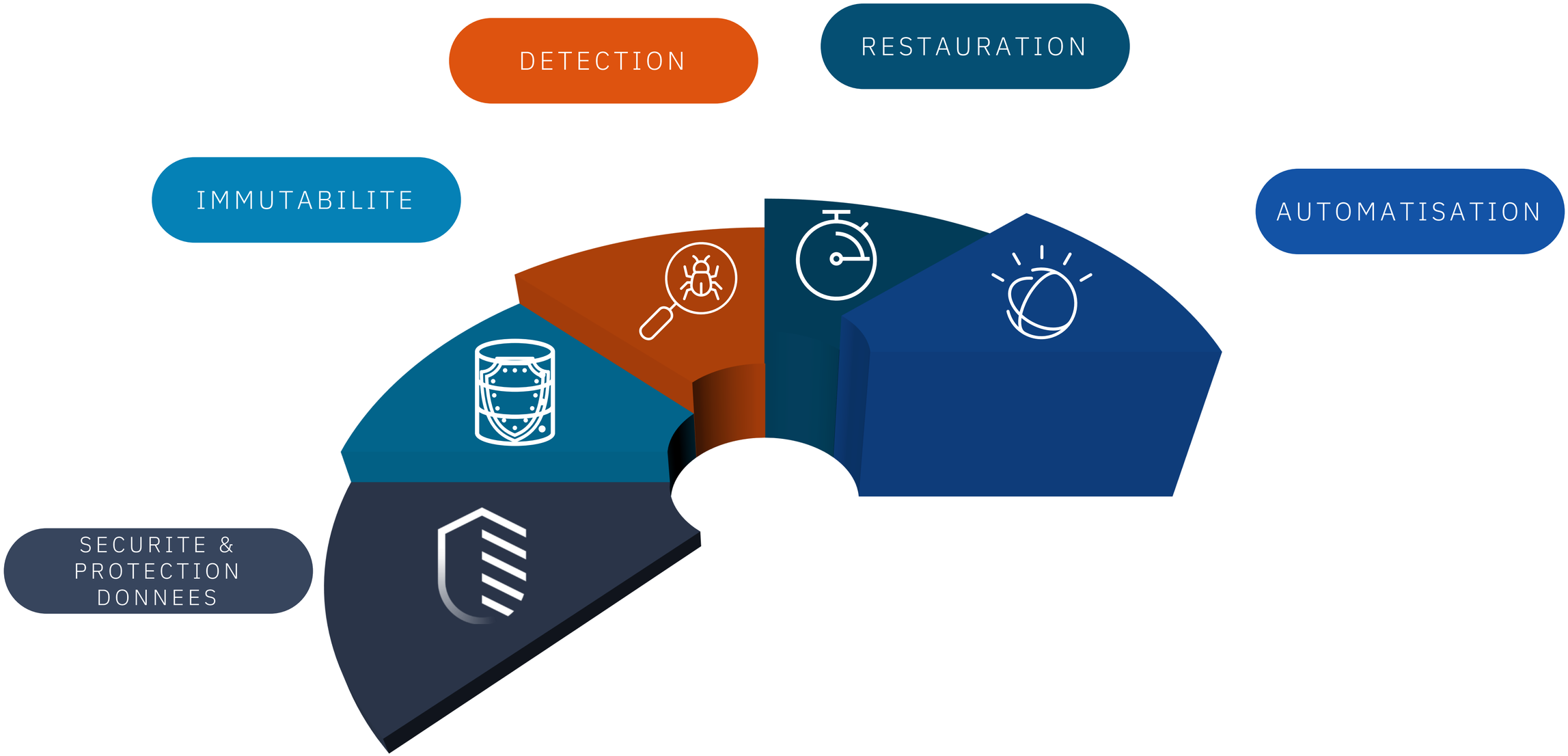
Changement de paradigme : PCA vs Cyber PCA

Categories	Traditional Recovery	Cyber Recovery
Nature de l'impact	Aléatoire Ex: catastrophe naturelle	Ciblé pensé pour faire un maximum de dégâts
Périmètre de l'impact	Local / Régional	Global Peut atteindre tous systèmes connectés
Infrastructure de Sauvegarde impactée ?	Pas spécifiquement	Une des premières cibles !
Point de restauration	Connu	Inconnu Besoin de restaurer la dernière copie "saine"
Remise en état	RPO/RTO	RPO/RTO + Restauration de données saines
Durée de la remise en état	Heures/Jours	Jours/Semaines
Probabilité d'occurrence	Faible	Elevé

Besoin de détection au plus tôt

Besoin de données saines & restaurable rapidement

Comment se preparer à la resilience des données ?



Comment se preparer à la resilience des données ?

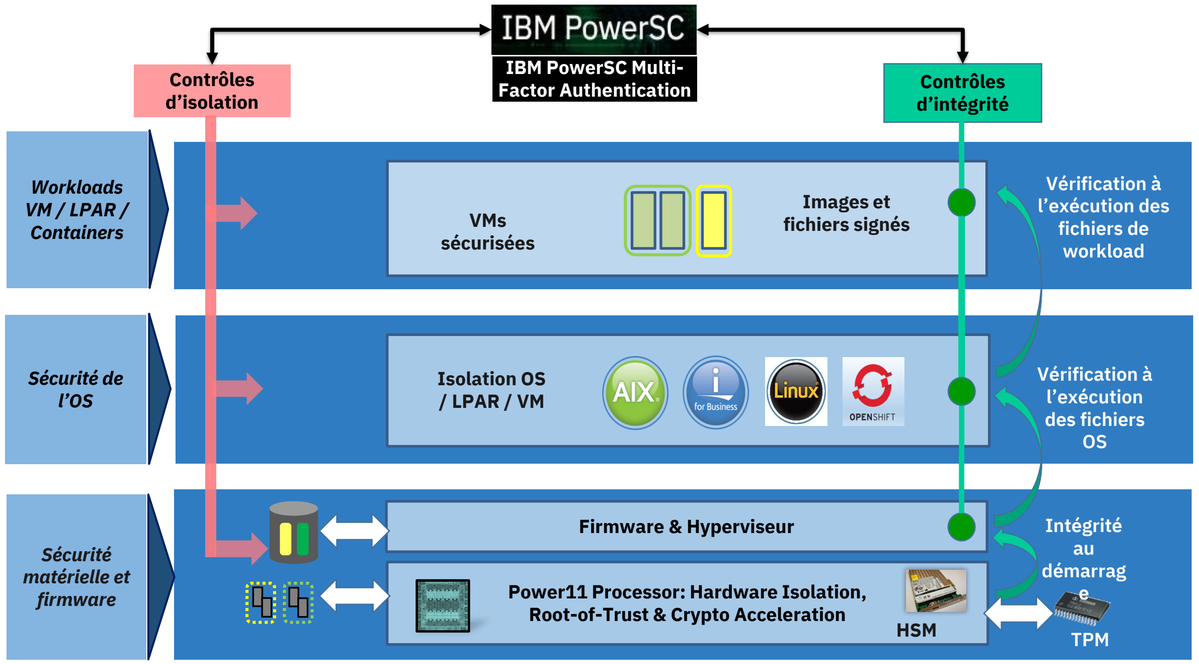
SECURITE & PROTECTION DONNEES

01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

Sécuriser les charges de travail des clients : isolement et intégrité

Environnement cloud multi-tenant le plus sécurisé avec des vulnérabilités bien inférieures que le x86



Défense renforcée contre les attaques de programmation orientée retour

- Nouvelle architecture matérielle intégrée au cœur avec une faible empreinte matérielle et une solution cryptographique basée sur des standards pour protéger l'intégrité de la pile de retour
- Sous le contrôle du Dynamic Execution Control Register (DEXCR), qui fournit un mécanisme par thread pour contrôler des fonctionnalités avec des compromis sécurité/performance ou des spéculations

Isolation accrue du processeur par rapport aux processeurs de service

Side-Channel avoidance amélioré en performance

- Gestion améliorée de l'isolation automatique des threads contre les attaques basées sur la spéculation

Algorithmes de protection quantum safe sur le LPM et le Secure Boot

- Ajout d'une méthode de protection contre les attaques quantique à venir via les fonctions ML-DSA

Power**SC** : Sécurité et Conformité des entreprises

IBM i

AIX

Red Hat Enterprise Linux

SUSE

Sécurité

Gestion des mises à jour

PowerSC

Conformité

MFA
Authentification Multifacteurs

IBM

Comment se preparer à la resilience des données ?

IMMUTABILITE

02

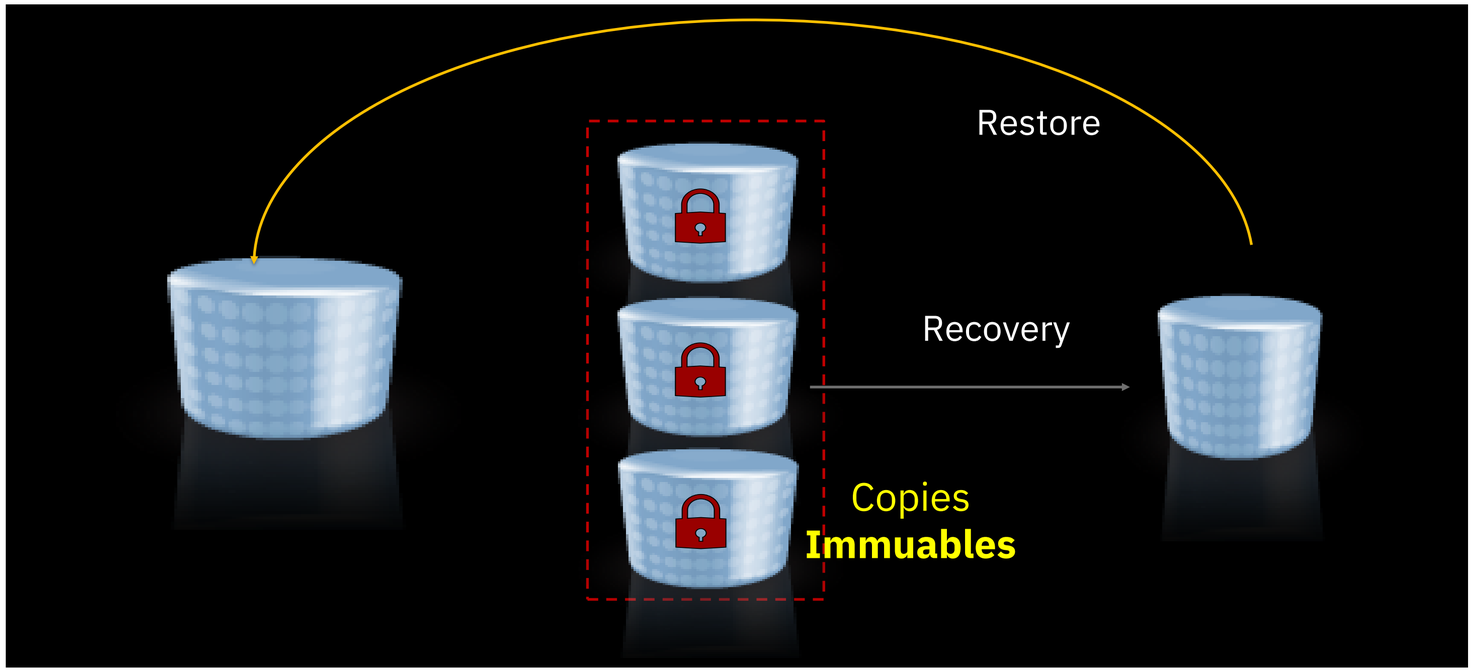
Points de données récupérables immuables, les données ne peuvent pas être supprimées

SECURITE & PROTECTION DONNEES

01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

Cyber Résilience des données avec Safeguarded Copy



Les copies sont stockées dans un **entrepôt sécurisé :**

Séparation logique avec les autres volumes
Restriction des accès

Les copies protégées ne peuvent **pas** être :

- ✓ Mappées à un host,
- ✓ Ecrites ou lues par une application,
- ✓ Supprimées par l'administrateur qui gère le stockage au quotidien.

Des **règles** sont définies pour des **groupes de volumes cohérents,** au niveau de chaque baie de stockage :

- ✓ **Fréquence** du programme de copie : en minutes, heures, jours, semaines, mois
- ✓ **Durée** de rétention définie en jour : maximum = 365 jours

Modification de la durée de rétention **non rétroactive**.

Comment se preparer à la resilience des données ?

DETECTION

03

Trouver les menaces actives
Détecter et prévenir les menaces dormantes

IMMUTABILITE

02

Points de données récupérables immuables, les données ne peuvent pas être supprimées

SECURITE & PROTECTION DONNEES

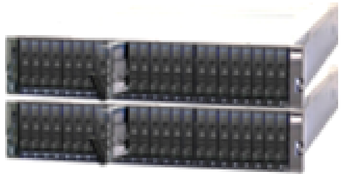
01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

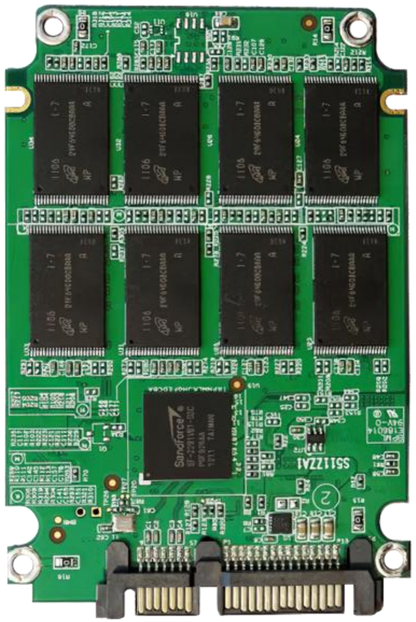
Les baies de disque IBM Flashsystem utilisent des Flash Core Modules

FlashSystem 5300

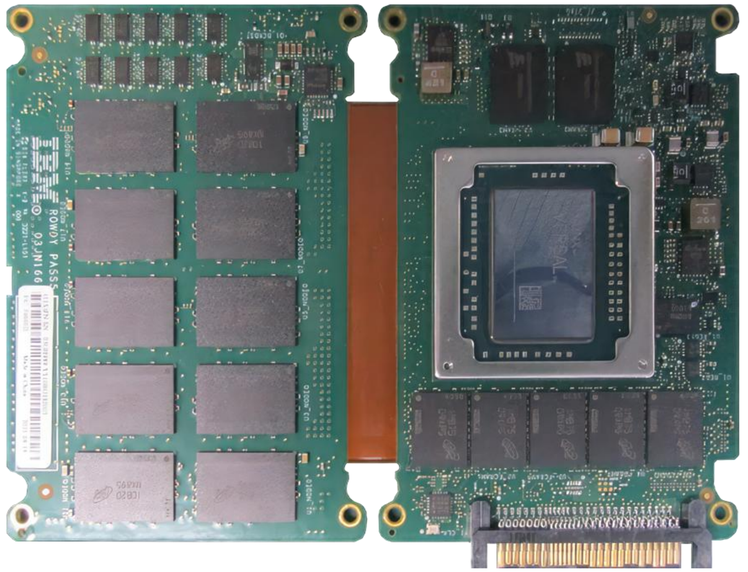
FlashSystem 7300



FlashSystem 9500



Un SSD « normal »



Un FlashCore Module

Capacités utiles (physiques) / effectives (max adressables) :

- **4.8TBu** / **22TBe** (ratio 4.5:1)
- **9.6TBu** / **29TBe** (ratio 3:1)
- **19.2TBu** / **58TBe** (ratio 3:1)
- **38.4TBu** / **116TBe** (ratio 3:1)

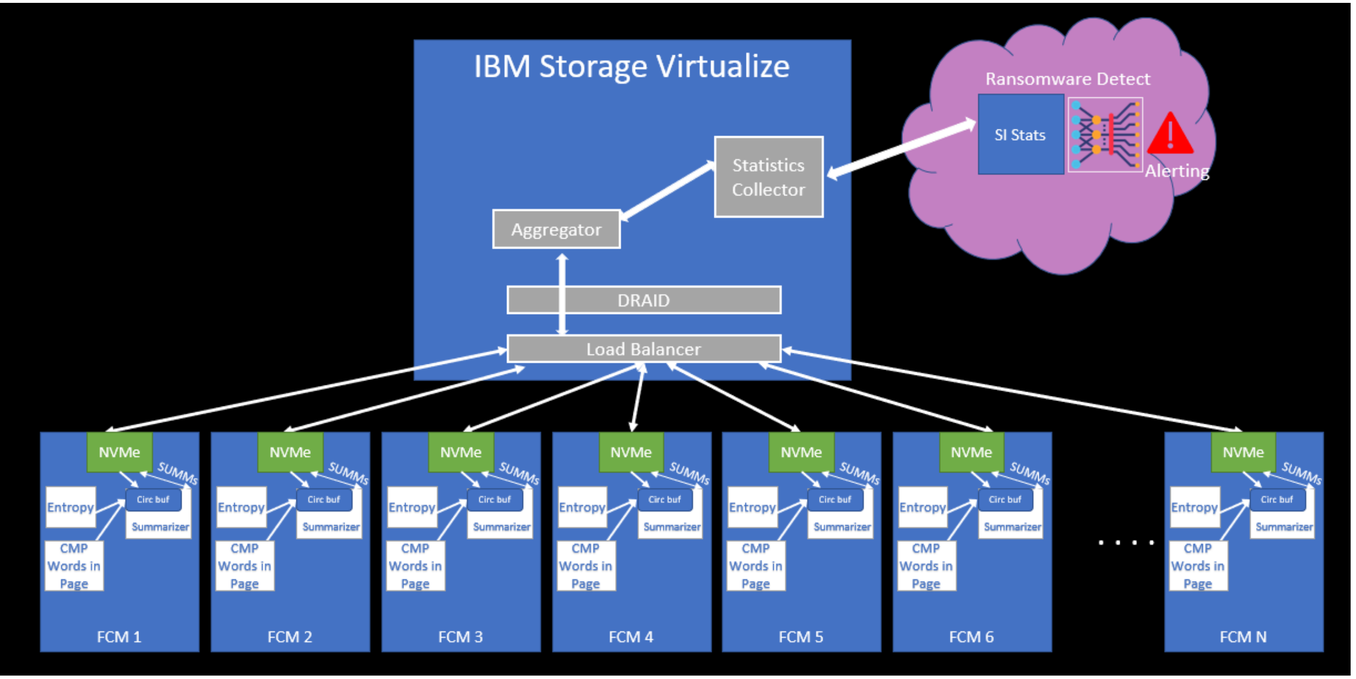
Note : valeurs en décimal (base 10)

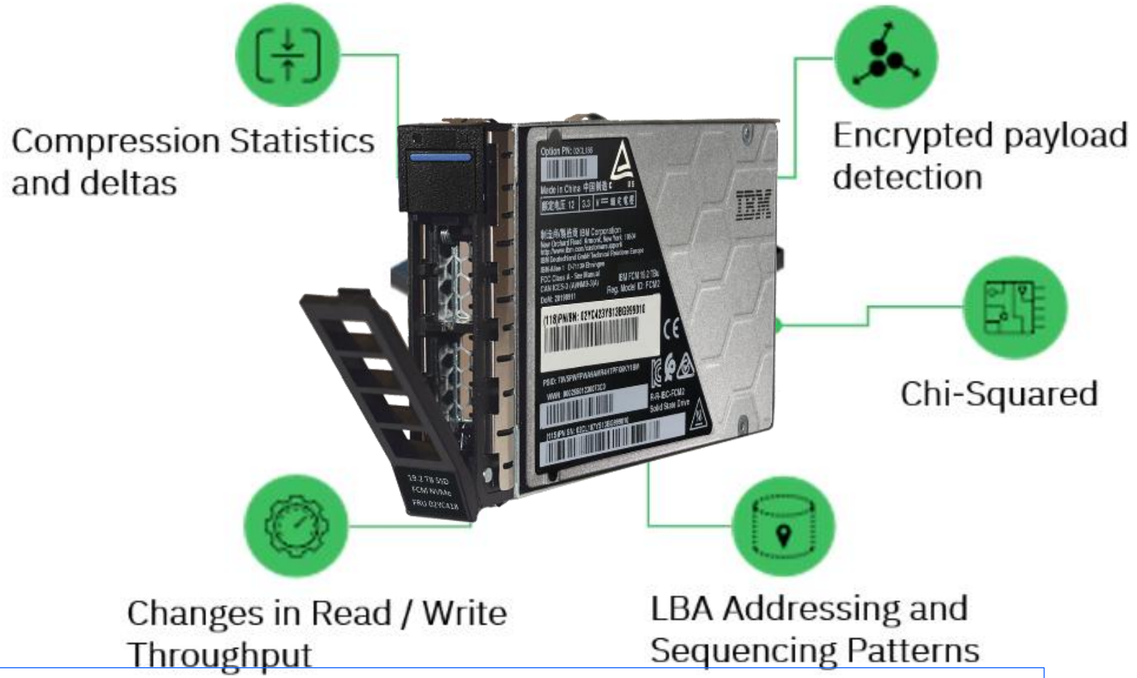
Endurance
Performance

Sécurité
Efficience

« Inline data corruption detection » avec IBM Storage **Virtualize**

Amélioration avec la génération FCM4





- Les mesures sont collectées à l'aide de FPGA installés dans les modules FlashCore Gen 4 (FCM4)
- Cette collecte est effectuée sur chaque FCM4 sans impact sur les performances.
- Les données sont transmises en temps réel à IBM Spectrum Virtualize.
- Les statistiques sont agrégées et transmises à Storage Insights PRO qui les analysera à l'aide de modèles d'apprentissage automatique (IA).
- Une alerte est transmise en cas de détection d'une anomalie ou d'une attaque RansomWare.

Comment se preparer à la resilience des données ?

DETECTION

03

Trouver les menaces actives
Détecter et prévenir les menaces dormantes

RESTAURATION

04

Récupération opérationnelle rapide en quelques secondes, minutes ou heures
Éviter le paiement de rançons

IMMUTABILITE

02

Points de données récupérables immuables, les données ne peuvent pas être supprimées

AUTOMATISATION

05

Simplification des opérations et possibilité de tester et de prouver la capacité de récupération
Intégration de la cybersécurité et de la cyber résilience

SECURITE & PROTECTION DONNEES

01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

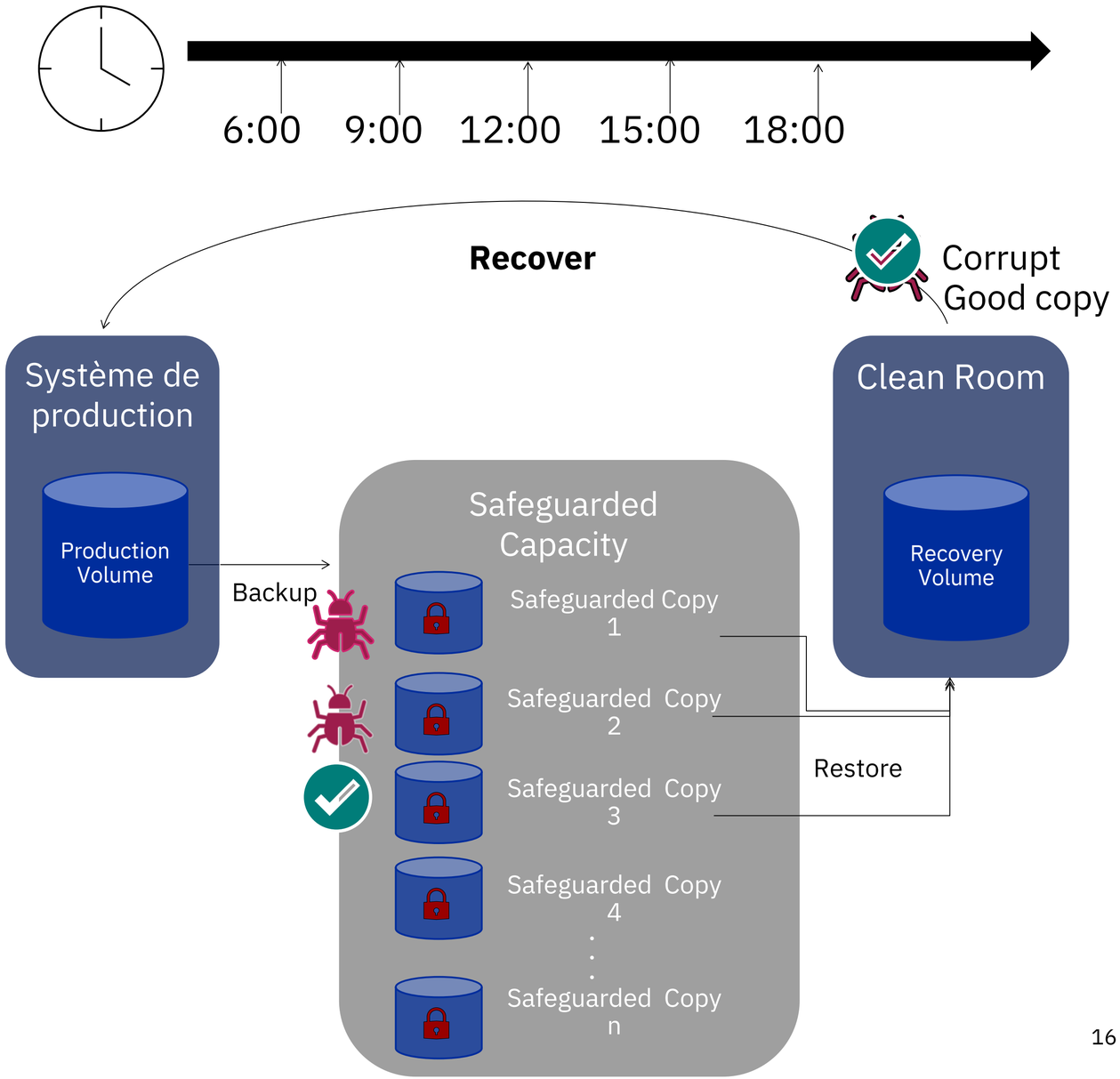
Cyber Résilience des données avec Safeguarded Copy

Les copies sont stockées dans un **entrepôt sécurisé :**
- Séparation logique avec les autres volumes
- Restriction des accès

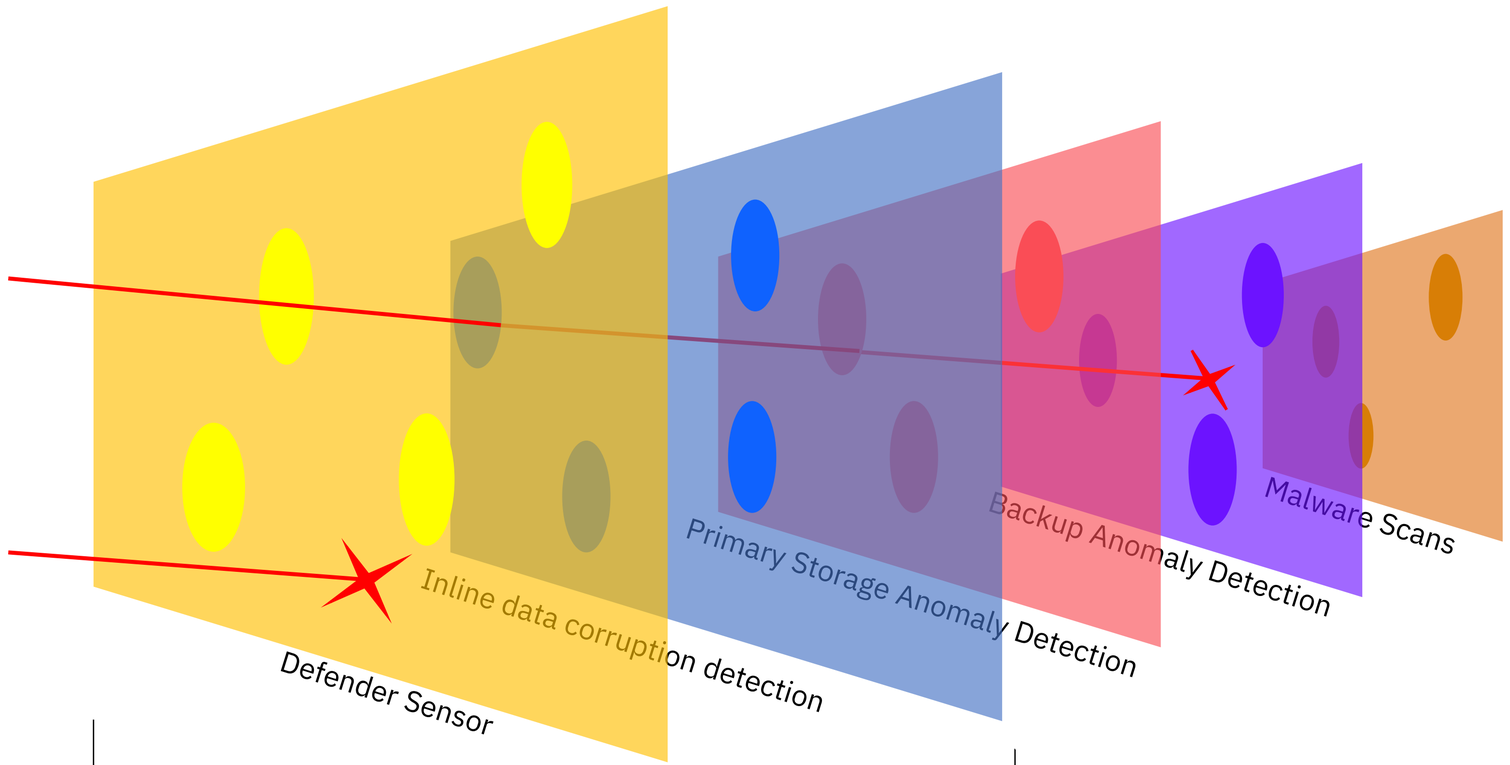
Les copies protégées ne peuvent **pas** être :
- ✓ Mappées à un host,
- ✓ Ecrites ou lues par une application,
- ✓ Supprimées par l'administrateur qui gère le stockage au quotidien.

- Pas directement accessible à un serveur ou à une application
- Les données ne sont accessibles qu'après la récupération d'une copie protégée sur un volume de récupération distinct

Les volumes de récupération sont utilisés pour :
- Validation des données sur la baie
- Analyse Post incident
- Restauration des données de production



IBM Storage: la défense multi couches !



Détection sur données actives

Détection sur les données sauvegardées

Defender Sensor
- Détecte les anomalies sur un système(prod) en analysant les schémas d'attaque par rapport aux métadonnées des fichiers et à l'analyse approfondie des fichiers.

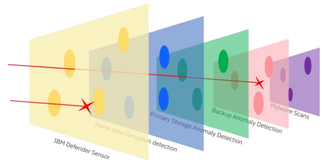
Inline Data Corruption Detection
- Détection des anomalies basée sur l'entropie
- Se produit au niveau du système de stockage par le biais de sa couche SW

Primary Storage: Anomaly Detection
- Analyse des anomalies des snapshots immuables (SGC) en fonction de l'application
- Notification des anomalies et recherche du dernier snapshot propre (dernier snapshot sans anomalie)

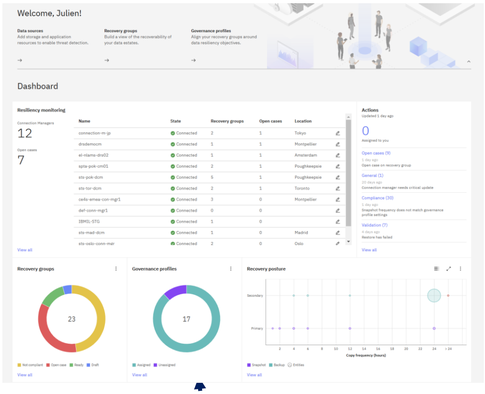
Backup Storage: Anomaly Detection
- Exploite l'IA et le ML pour identifier les anomalies dans la taille des données écrites, les taux de réduction des données (déduplication et compression).

Isolated Environment: Malware Scan
- Analyse les données de sauvegarde à la recherche de fichiers malveillants et d'exécutables connus
- Permet de nettoyer ou de mettre en quarantaine les logiciels malveillants détectés.

IBM Storage: la défense multi couches !

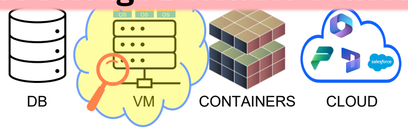


IBM Storage Defender DRS



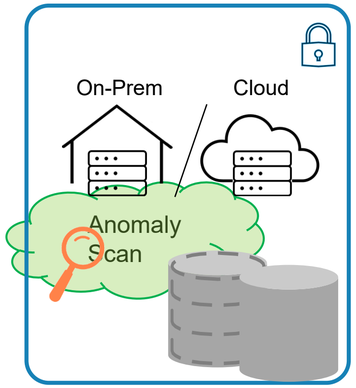
Workloads

IBM Storage Defender Sensors



View / Orchestrate

Environnement Isolé



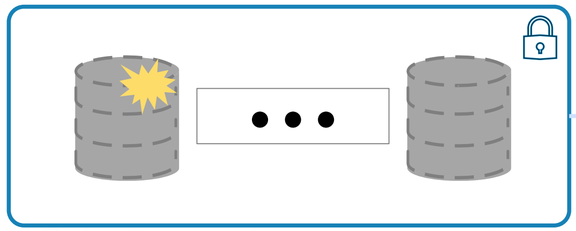
Tester / Identifier les copies

Primary storage

IBM Flashsystem

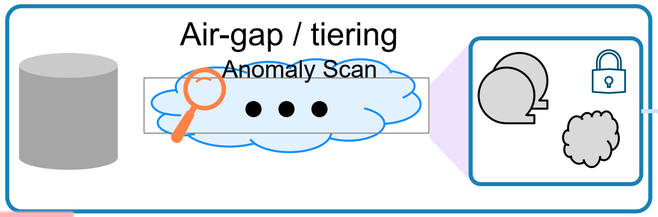
Restore

Copies Immuables



Retention courte pour recuperation rapide

IBM Storage Sentinel



Rétention longue (**sauvegardes**)

Tape, cloud, et autres medias

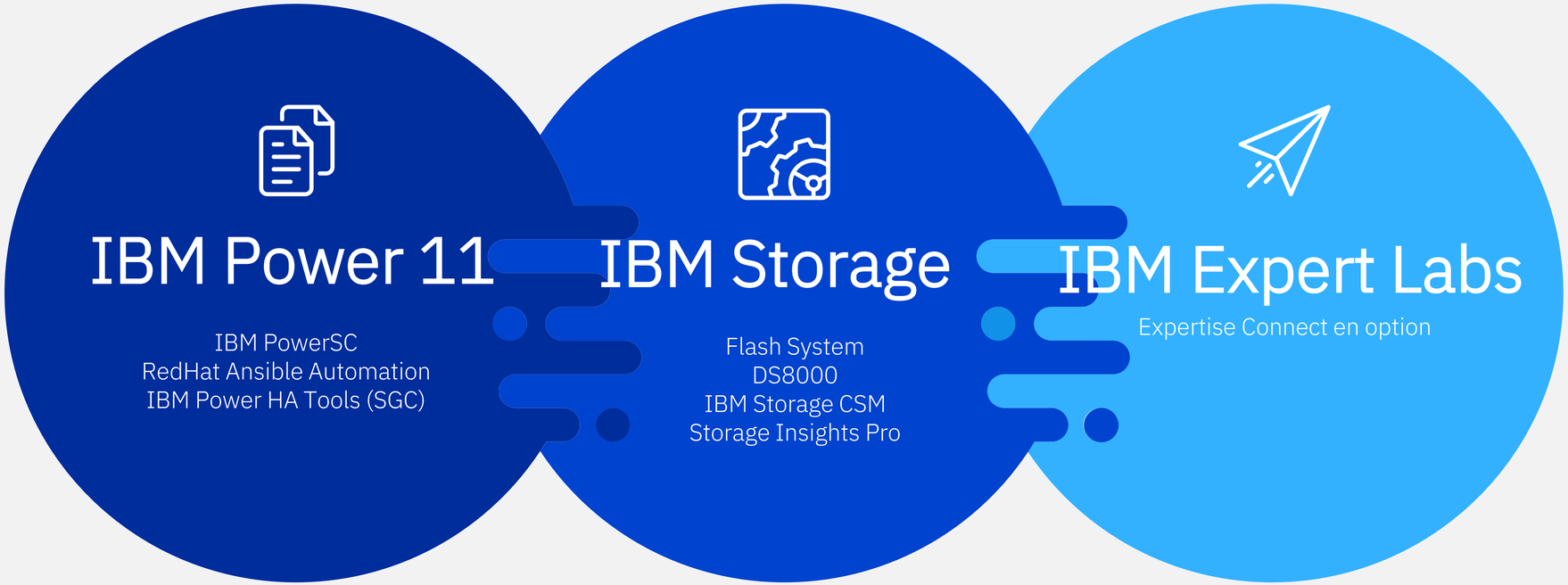
View / Orchestrate

SOC Integration

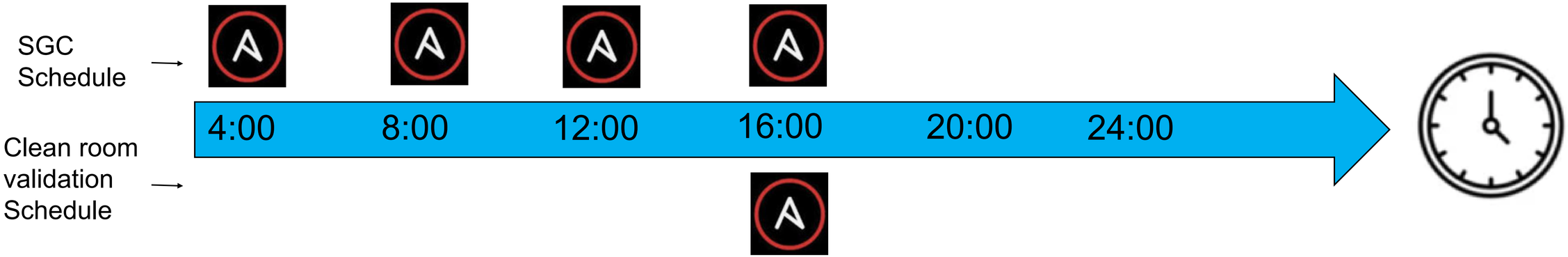
IBM Storage Data Protect
IBM Storage Protect

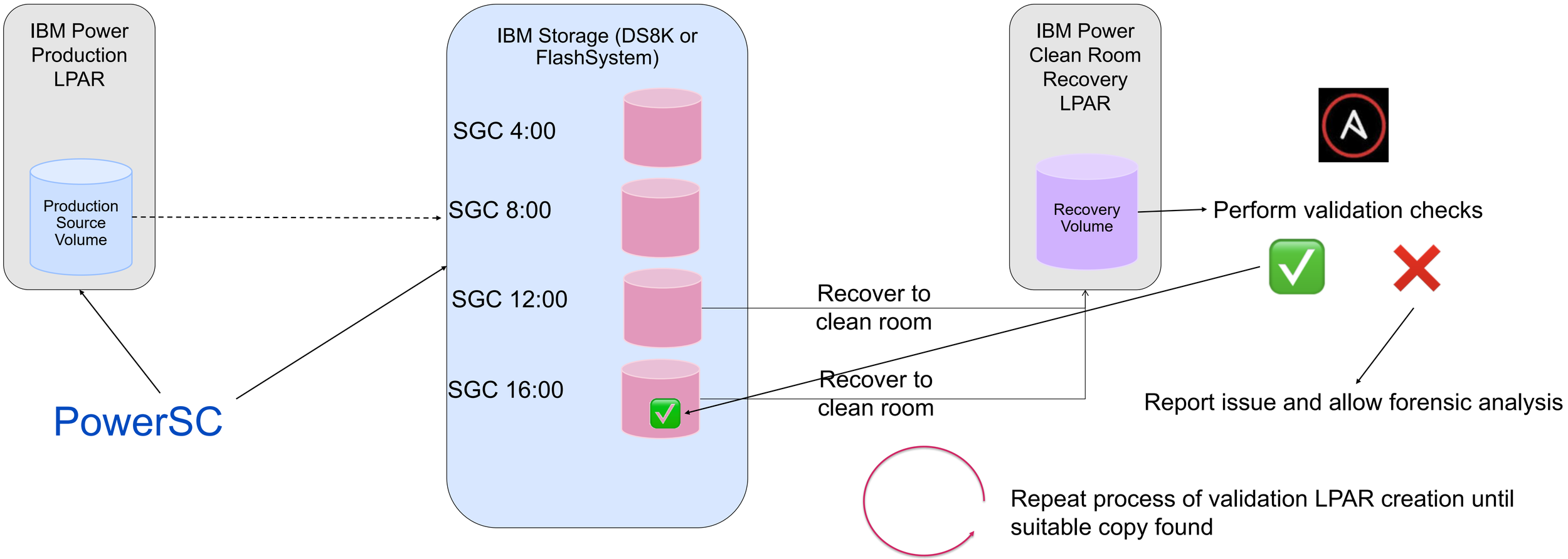
IBM Power Cyber Vault résout ce problème

Une solution de cyber-résilience entièrement intégrée avec détection des menaces en ligne, réponse automatisée et récupération rapide, conçue pour maximiser la continuité des activités et minimiser les risques et la complexité

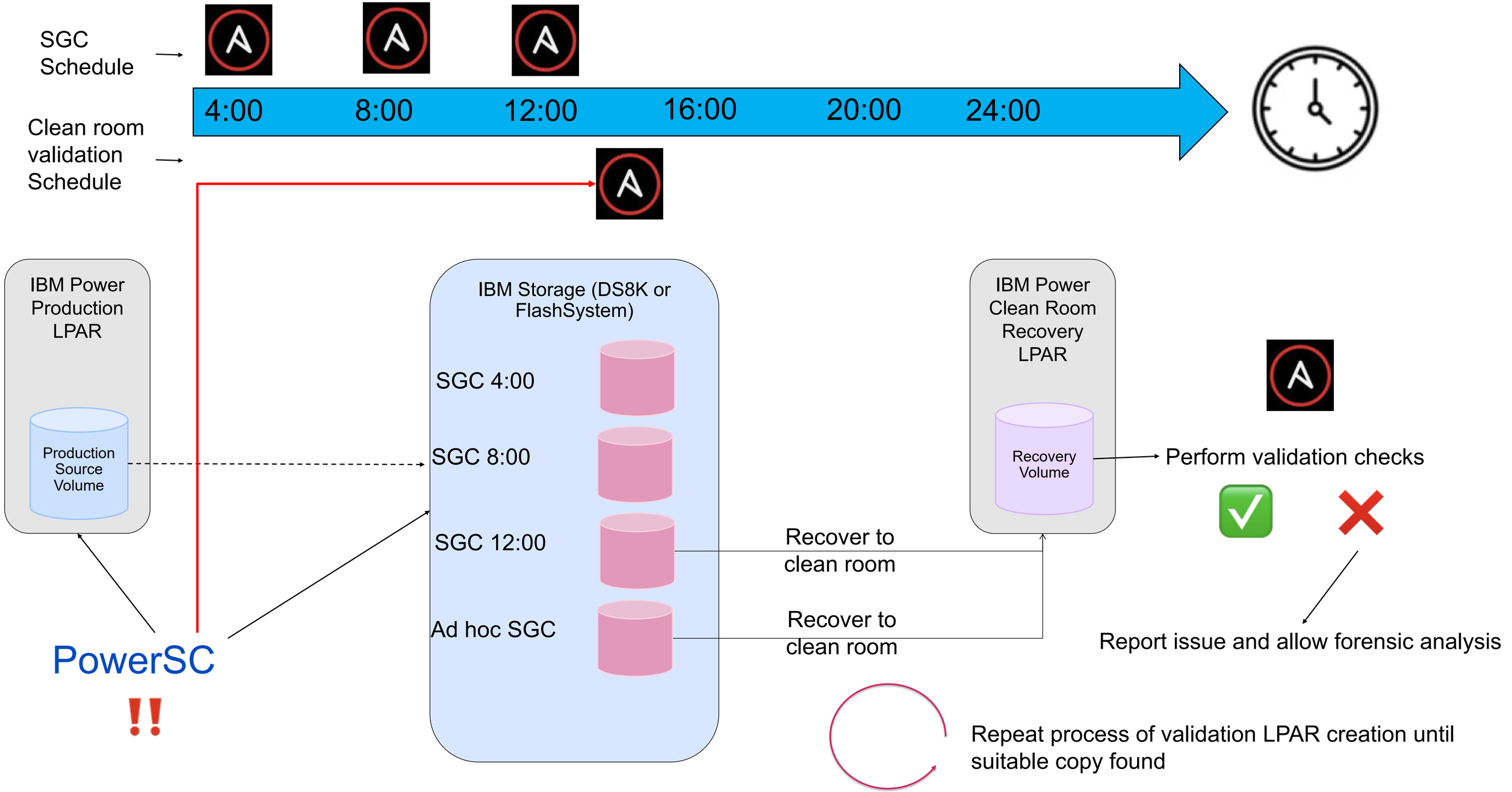


IBM Power Cyber Vault - Protect with automated SafeGuarded Copies and **proactive** validation



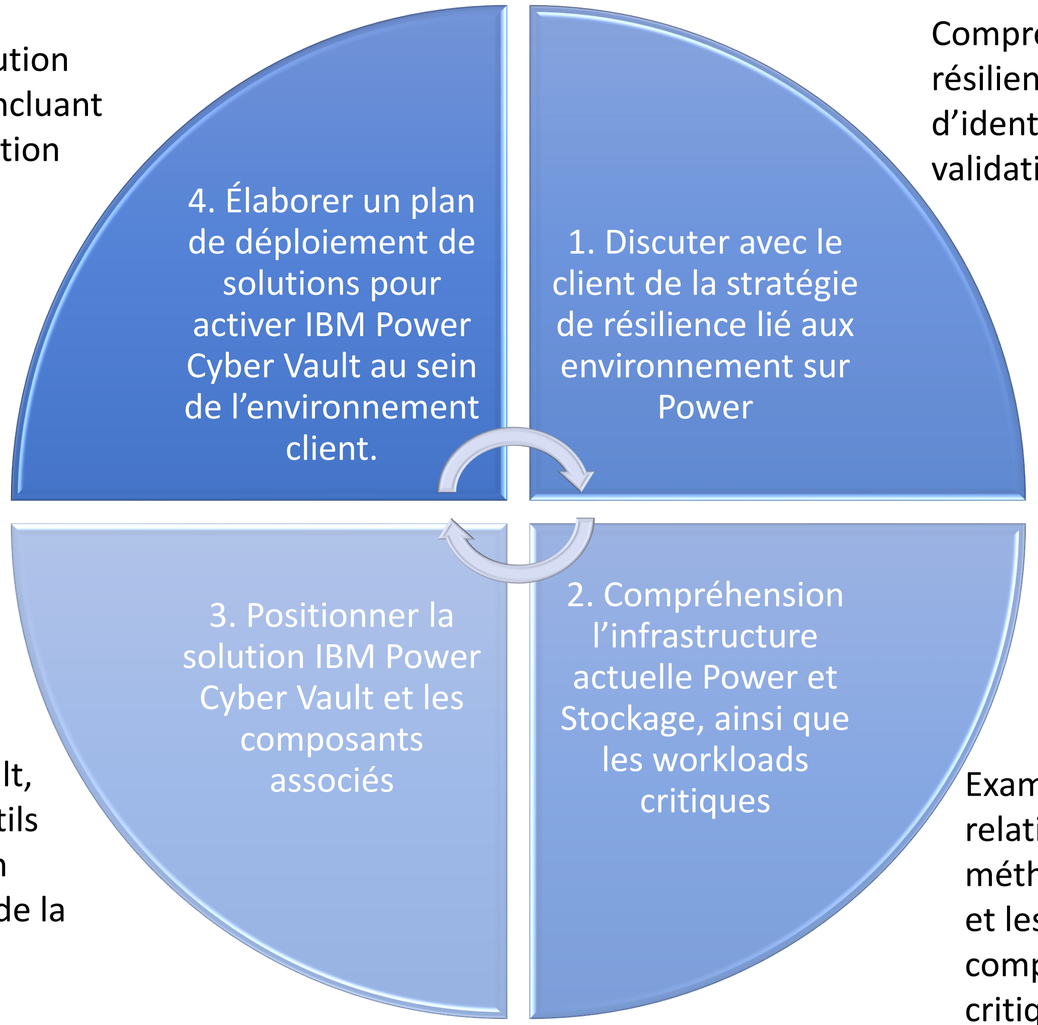


IBM Power Cyber Vault - Protect with automated SafeGuarded Copies and **reactive** validation



IBM Power Cyber Vault Workshop

Travailler avec le client pour créer une solution basée sur l'offre IBM Power Cyber Vault, incluant l'analyse des gaps et le plan d'implémentation du projet.



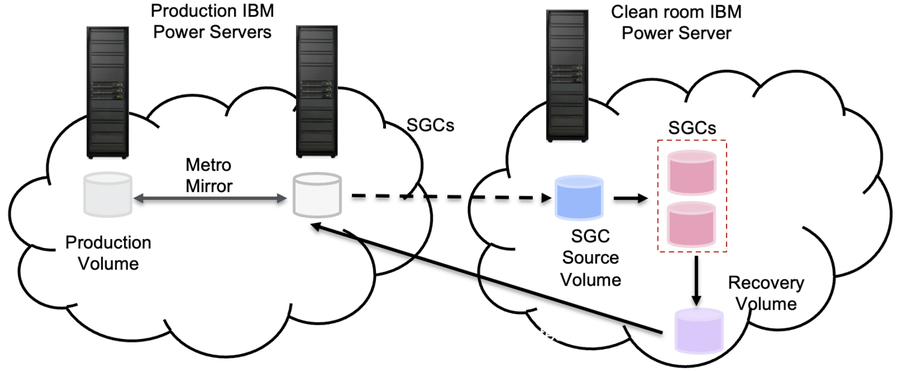
Comprendre la stratégie actuelle de cyber résilience Power des clients en termes d'identification, de protection, de détection, de validation et de récupération.

Aperçu de la solution IBM Power Cyber Vault, incluant l'architecture, les prérequis, les outils utilisés et les livrables. Comment la solution peut-elle répondre aux besoins des clients de la stratégie de cyber résilience Power ?

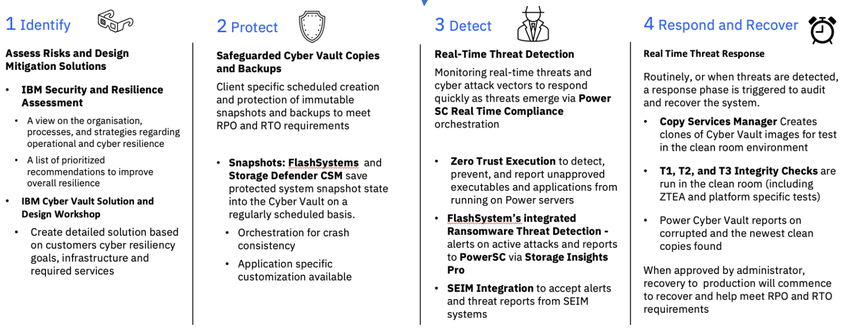
Examen de l'infrastructure Power et Stockage en relation avec l'environnement de production, les méthodes de réplication, les technologies de HA et les ressources en clean room. Une compréhension haut niveau des workloads critiques à protéger dans le cadre de la solution IBM Power Cyber Vault.

IBM Power Cyber Vault Workshop – Le rendu

- Rapport final sur IBM Power Cyber Vault, incluant :
  - Architecture de solution proposée
  - Prérequis et actions associées
  - Vue générale des charges de travail critiques et des besoins de récupération
  - Champ et calendrier de déploiement et de test



Components	Status
Red Hat Ansible Automation Platform	Installed
IBM PowerSC	Required
IBM CSM (Copy Services Manager)	Required
IBM Storage (DS8K or FlashSystems)	FS9Ks Installed
Storage Insights Pro for FCM4 alerting	Required
IBM ZTEA (Zero trust execution for AIX) – optional	Not required



1 Identify

Assess Risks and Design Mitigation Solutions

- **IBM Security and Resilience Assessment**
  - A view on the organisation, processes, and strategies regarding operational and cyber resilience
  - A list of prioritized recommendations to improve overall resilience
- **IBM Cyber Vault Solution and Design Workshop**
  - Create detailed solution based on customers cyber resiliency goals, infrastructure and required services

2 Protect

Safeguarded Cyber Vault Copies and Backups

Client specific scheduled creation and protection of immutable snapshots and backups to meet RPO and RTO requirements

- **Snapshots: FlashSystems** and **Storage Defender CSM** save protected system snapshot state into the Cyber Vault on a regularly scheduled basis.
  - Orchestration for crash consistency
  - Application specific customization available

3 Detect

Real-Time Threat Detection

Monitoring real-time threats and cyber attack vectors to respond quickly as threats emerge via **Power SC Real Time Compliance** orchestration

- **Zero Trust Execution** to detect, prevent, and report unapproved executables and applications from running on Power servers
- **FlashSystem's integrated Ransomware Threat Detection -** alerts on active attacks and reports to **PowerSC** via **Storage Insights Pro**
- **SEIM Integration** to accept alerts and threat reports from SEIM systems

4 Respond and Recover

Real Time Threat Response

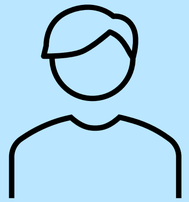
Routinely, or when threats are detected, a response phase is triggered to audit and recover the system.

- **Copy Services Manager** Creates clones of Cyber Vault images for test in the clean room environment
- **T1, T2, and T3 Integrity Checks** are run in the clean room (including ZTEA and platform specific tests)
- Power Cyber Vault reports on corrupted and the newest clean copies found

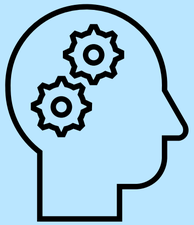
When approved by administrator, recovery to production will commence to recover and help meet RPO and RTO requirements

Current on-premise environment			
IBM Power LPARs			
General Info	**Model**	**Data Centre**	**Environment**
	OracleLPAR1	DC1	Production
Resources	**CPU**	**Memory**	**SSP**
	2.5	80GB	Default
S/W	**OS version**	**Function**	**Application version**
	AIX 7.1	DB	Oracle 12c
Storage (Primary)	**Size**	**Primary storage**	**Replication method**
	500GB	FlashStorage_FS9K_1	Metro Mirror/Sync
Storage (Secondary)	**Size**	**Primary storage**	**Replication method**
	500GB	FlashStorage_FS9K_2	Metro Mirror/Sync
HA/DR solution	**HA solution**	**DR primary strategy**	**DR backup strategy**
	IBM PowerHA EE	IBM PowerHA EE	Offline backup
Business Recovery SLAs	**RTO**	**RPO**	
	< 30 mins	< 2mins	
Current cyber resiliency	**Protect**	**Detect**	**Respond**
	Only backups	PowerSC agent	none
Cyber Resiliency Schedule	**SGC Interval**	**Retention**	**Long Term Retention**
	4 hours	14 days	6 months

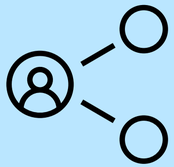
IBM Power Cyber Vault Expertise Connect



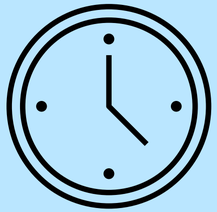
IBM assigne un spécialiste IBM Power Cyber Vault comme contact technique primaire



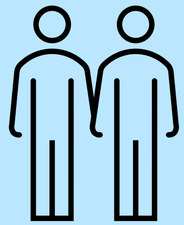
Le spécialiste possède l’expertise sur la solution Power Cyber Vault et les besoins du client



Le spécialiste peut être dédié à 100% ou partagé avec un nombre limité d’autres clients, selon les besoins



Disponible dans les jours ouvrés



Les leaders sélectionnés par le staff IT du client sont autorisés de servir comme « contact désigné » pour travailler avec IBM

Le contact désigné priorisera et filtrera les requêtes pour le spécialiste

Pour aller plus loin:

Evaluation autonome

En 30 minutes, déterminez le degré de préparation de votre entreprise aux cyberattaques et assurez la conformité avec un maillage complexe de réglementations telles que DORA UE (Digital Operational Resilience Act), GLBA (Gramm-Leach-Bliley Act), FISMA (Federal Information Security Modernization Act), DPDP (Digital Personal Data Protection Act), NIS-2, ainsi que des cadres réglementaires similaires dans différentes régions du monde

IBM Cyber-resilience Assesment

Atelier immersif

En l’espace de quelques heures vous profiterez d’une évaluation personnalisée, des conseils et des démonstrations de nos experts, vous participerez à une session d’idéation et repartirez avec un plan d’action adapté à votre situation.

Atelier immersif

Merci pour votre attention

#pw2025

IBM

common
FRANCE

IBM Power
Quick Reference Guide

Build IBM Power Cyber Vault

Overview

it takes time to recover from a cyber incident. That's typically because traditional backup and HA/DR practices were simply not designed for the nature of today's cyber attacks by outside actors. Based on the NIST Cybersecurity Framework model, the build IBM Power Cyber Vault service is designed to help your organization identify, protect, detect, respond and more rapidly recover from a cyber-attack.

This service is a comprehensive cyber resiliency solution, creating automated processes for data protection and recovery within an isolated clean room IBM Power Cyber Vault environment.

Custom SOW
AIX/Linux/IBM i
Implement

IBM Technology Expert Labs

Target Audience

- CIOs or IT Operations managers that have the charter to protect their business against cyber attacks.

Why Use This Service?

- Do you want to improve detection, recover more quickly, and minimize the potential financial impact of cyber attacks?
- Are you facing challenges with forensic logical data corruption detection and fear attacks may get replicated across your HA/DR environment?

Benefits

- This service will help you implement a modern Cyber resilience protection plan, including how to continue operations and rapidly recover despite suffering a cyber-incident.
- Regularly capturing and then validating trusted copies of your production environment to a Cyber Vault is the base for faster detection and recovery.

Activities

- Conduct a design workshop to **identify** current cyber resiliency gaps and define an isolated Cyber Vault architecture with agreed data retention policies and recovery time objectives
- Using the agreed reference architecture, build a clean room Cyber Vault solution to **protect** critical data including automated management of regular immutable backup copies.
- Implement appropriate zero trust and other selected tools to **detect** logical data corruption and / or validate trusted immutable copies in the Cyber Vault.
- Define, plan and test automated **respond** policies to be triggered on detection of cyber events and designed to help accelerate isolation and recovery time.
- Plan and test how to **recover** from trusted immutable copies in the Cyber Vault to meet return to business objectives and operational requirements.
- Provide ongoing advice and mentoring during a 6-month period after implementation.

Deliverables

- Provide reference architecture and design for a Cyber Vault solution.
- Provide Ansible automation workbooks (AIX/Linux) or PowerHA Tools for IBM i automation scripts for management of immutable copies.
- Provide operational and testing runbooks for logical corruption detection in saved copies.
- Provide ongoing guidance on best practices for respond and recover policies and procedures.

Scope

- Implementation phase: 6–12 weeks (dependent on scope and environment complexity)
- Expertise Connect: 6 months after successful deployment

Contacts

- Contact us at systems-expert-labs@ibm.com or your local Technology Expert Labs team

IBM

IBM Power
Quick Reference Guide

Build Red Hat Ansible Automation for IBM Power

Overview

The Automate Operations with Red Hat Ansible on Power service is designed to help you get started with automated operations, leveraging customized playbooks.

Standard Offering
AIX/Linux/IBM i
Implement

IBM Technology Expert Labs

Target Audience

- Clients using Power that are considering automation for their AIX, IBM i or SAP HANA workloads

Why Use This Service?

- Are you using or considering automation to reduce expense and optimize system management?
- Are you considering modernizing or migrating existing AIX or IBM i management scripts to include Ansible?

Benefits

- The service will help you get started successfully with Ansible automation on Power
- It will help you gain experience with creating custom Ansible playbooks
- It will help you quantify the benefits of using Ansible for automating your IT environment

Activities

- Implement and configure Ansible on Power for AIX, IBM i or SAP HANA
- Advise on using Ansible ad-hoc commands and existing modules
- Advise on building Ansible playbooks and roles
- Advise on use of Ansible collections for Power, targeted at AIX and IBM i operations
- Advise on integrating Ansible with PowerVC via REST APIs
- Advise on using Ansible playbooks for automation of common tasks such as:
  - Configuring systems
  - Deploying software
  - Implementing patches
  - Updating security settings

Deliverables

- Implementation of Ansible and creation of sample playbooks for automated operations
- Recommendations for potential use cases of Ansible for configuration, software and security management
- Recommendations on additional capabilities such as Red Hat Ansible Automation Platform (formerly Tower)
- Skills enablement and guidance on best practices for managing automated operations with Ansible

Scope

- Limited to implementing one Ansible environment and creating up to 3 custom playbooks
- Duration: ~1 week
- Offering number: 6911-37J

Contacts

- Contact us at systems-expert-labs@ibm.com or your local Technology Expert Labs team

IBM

IBM Power
Quick Reference Guide

Build IBM PowerSC

Overview

This service provides a deployment of the PowerSC Graphical User Interface Server and Agents in your environment and provides centralized management of numerous security and compliance-related safeguards designed to mitigate the security risk of your AIX and Linux systems running on Power.

Standard Offering
AIX/Linux/IBM i
Implement

IBM Technology
Expert Labs

Target Audience

- Clients interested in deploying or evaluating PowerSC to secure AIX or Linux running on Power
  and Linux running on Intel.

Why Use This Service?

- Are you looking to deploy a solution that is designed to mitigate security risk on AIX and Linux?
- Would you like to better detect, prevent or respond to security intrusion occurring on AIX or Linux?

Benefits

- Reduce security risk by deploying PowerSC's diverse set of security safeguards designed to protect AIX or Linux
- Continually monitor and respond to cyberthreats using PowerSC's Endpoint Detection and Response (EDR) capabilities
- Mitigate the risk of ransomware and malware leveraging PowerSC's extensive feature set

Activities

- Advise on the numerous security and compliance capabilities provided by PowerSC
- Advise on PowerSC's support for automation via REST API
- Analyze the security objectives of the client
- Identify the subset of PowerSC functionality needed by the client
- Plan and implement a proof-of-concept deployment of PowerSC corresponding to the client's requirements using the client's environment
- Test the proof-of-concept deployment using the functions most important to the client
- Document implementation details that will be needed by the client

Deliverables

- Recommendation of PowerSC integration
- Install and configuration user guide provides step-by-step guidance on deploying PowerSC Graphical User Interface Server and Agents
- Proposal for additional services that were identified during the engagement

Scope

- Limited to assistance with 1 PowerSC UI Server instance and 2 PowerSC UI Agent instances
- Duration: ~1 week
- Offering number: 6911-37G

Contacts

- Contact us at systems-expert-labs@ibm.com or your local Technology Expert Labs team

IBM

IBM Power
Quick Reference Guide

Build IBM Zero Trust Execution for AIX

Overview

IBM Zero Trust Execution for AIX (ZTEA) provides a malware defense for AIX that uses a Zero Trust approach. ZTEA is designed to detect, and optionally prevent, the execution of all types of software-based malware including ransomware, zero-day malware, next-generation malware, hacking tools, viruses, root kits, worms, and trojans.

Custom SOW
AIX
Implement

IBM Technology Expert Labs

Target Audience

- Clients looking to detect or prevent malware on AIX or VIOS

Why Use This Service?

- Do you need to comply with compliance requirements for anti-virus, malware prevention, or allowlisting?
- Do you want to mitigate the risk of malware, including ransomware attack?

Benefits

- Decrease the cost of a security breach by detecting an attacker as soon as unauthorized hacking tools are executed
- Decrease the cost of security breach by detecting or preventing malware in real-time
- Deploy malware defense using ZTEA's three risk mitigation levels to implement a malware risk mitigation plan that best fits the unique security goals and resources of your organization

Activities

- Deploy using PowerSC or Red Hat Ansible, which provide centralized monitoring and management of ZTEA
- Deploy components
  - ClamAV
  - AIX Trusted Execution
  - Cross-Reference Hash Database files
- Develop scripted, consistent and efficient processes for provisioning on AIX
- Deploy Secure malware risk mitigation on high security mission critical AIX instances
- Deploy Trusted malware risk mitigation on medium security AIX instances
- Deploy Standard malware risk mitigation on your standard AIX instances

Deliverables

- Implementation assistance with ZTEA using client AIX instances
- Client is provided with a licensed copy of ZTEA ksh93 scripts for the duration of the contract
- An electronic copy of all ZTEA documentation
- An electronic copy of all presentation slides
- Guidance on best practices for ZTEA deployment

Contacts

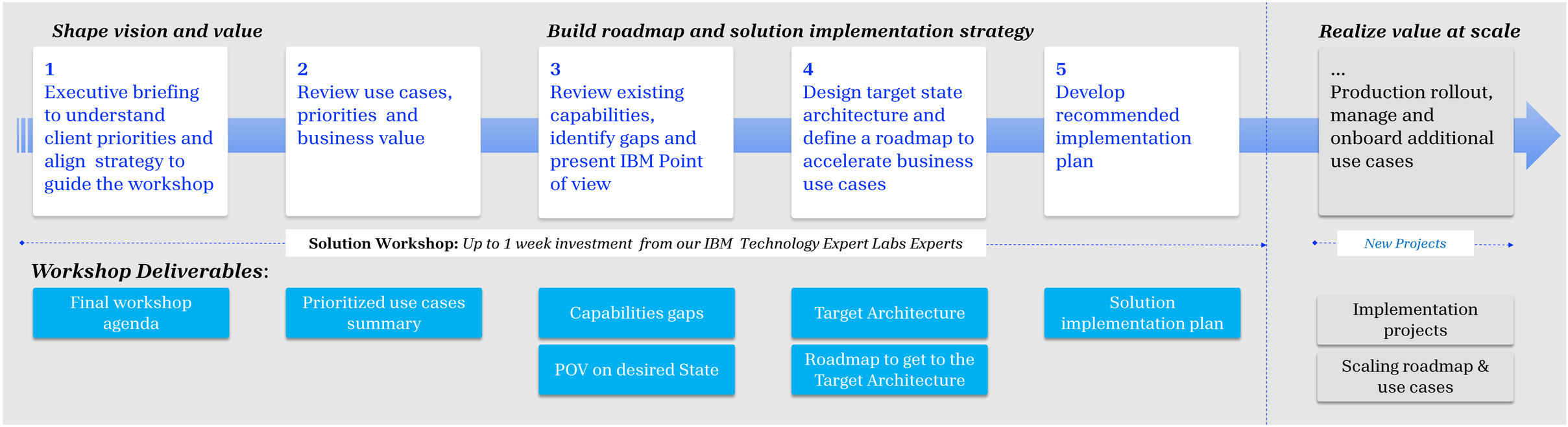
- Contact us at systems-expert-labs@ibm.com or your local Technology Expert Labs team
- For more information https://ibm.biz/ibm_ztea

IBM

Client Facing

Solution Workshops

An IBM investment to help our clients to maximize the value of IBM Technology and accelerate the journey to realize value at scale



Workshop Objectives

- Understand current and future use cases, strategic direction and goals
- Assess technical capabilities, challenges, gaps and opportunities for improvement and define a future state architecture and roadmap
- Generate new insights to help accelerate business outcomes

Workshop Outcomes

- Target architecture and recommended capabilities
- Roadmap to get to the target architecture and implementation plan to accelerate business outcomes

Client Benefits: Leverage IBM experts to help you shape a future state architecture to accelerate the journey to business outcomes