Varautuminen kyberhyökkäyksiin

Varaudu ajoissa ja yhdessä !

DataEnter

Juha Ekström
Tietotyöläinen
Juha.ekstrom@fi.ibm.com

IBM

Panostukset kyberhyökkäyksiin

Tuottoa

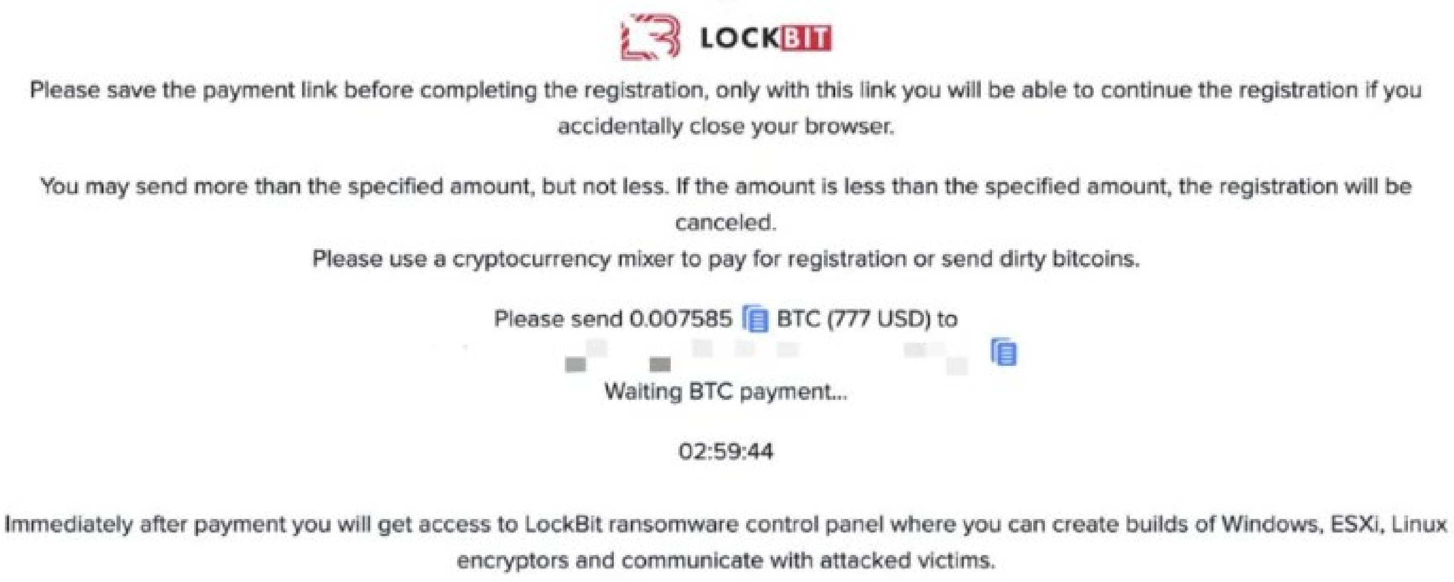
Kyberrikollisuus

Kannattavaa liiketoimintaa – tuotekehitykseen panostus kasvaa kokoajan

RaaS (Ransomware as a Service)

Ransomware viipymisaika (DWELL time)

101 d	21 d	10 d	24 h	4 h
2018	2020/21	2022	2023	2025


LOCKBIT

Please save the payment link before completing the registration, only with this link you will be able to continue the registration if you accidentally close your browser.

You may send more than the specified amount, but not less. If the amount is less than the specified amount, the registration will be canceled.

Please use a cryptocurrency mixer to pay for registration or send dirty bitcoins.

Please send 0.007585 BTC (777 USD) to

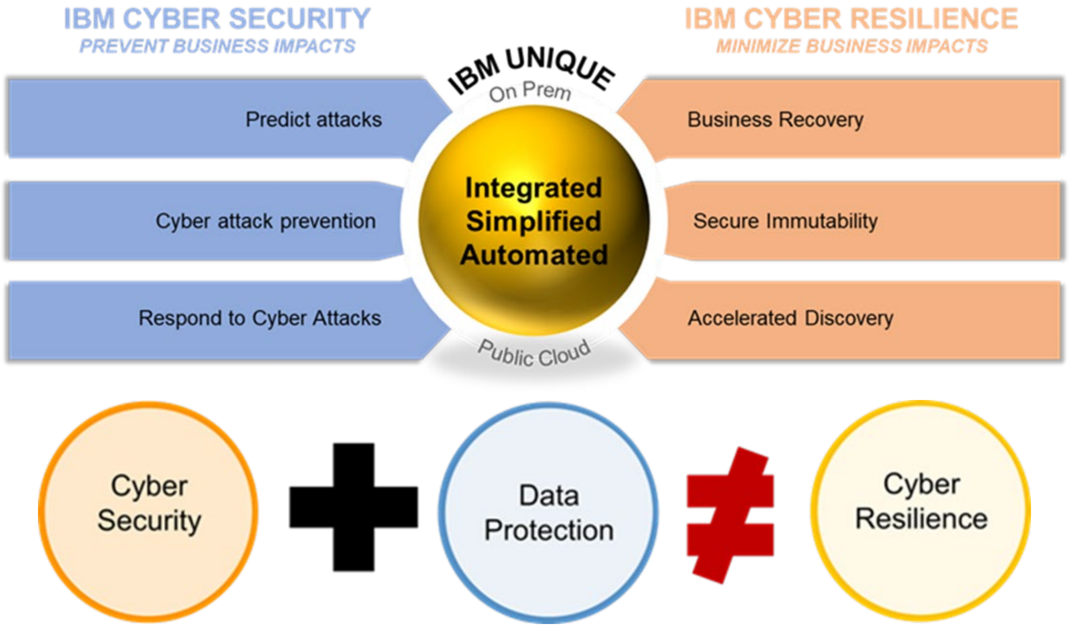
Waiting BTC payment...

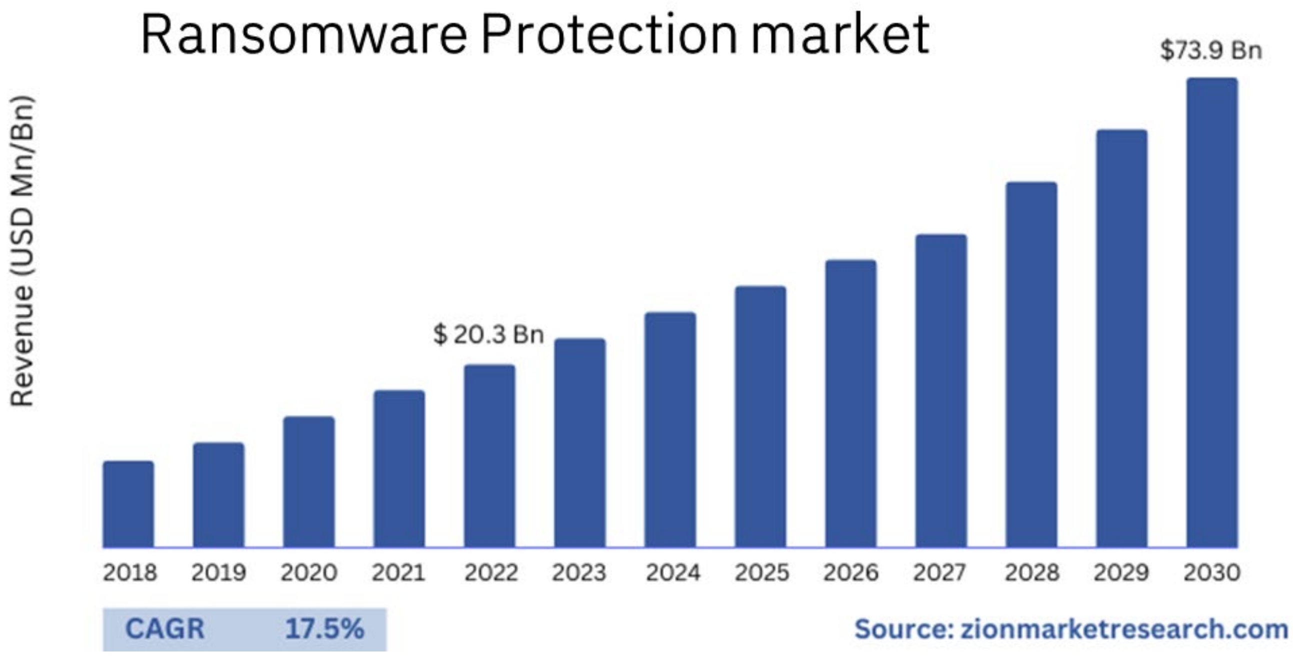
02:59:44

Immediately after payment you will get access to LockBit ransomware control panel where you can create builds of Windows, ESXi, Linux encryptors and communicate with attacked victims.

Source: [December 2024 Ransomware: FunkSec's Rise and RaaS Expansion]

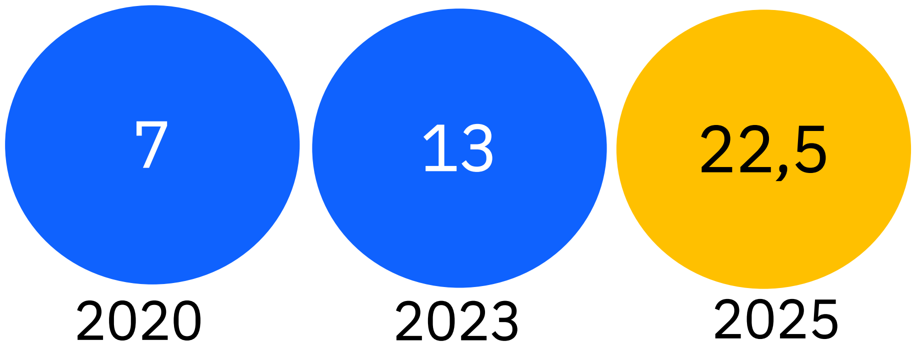
Panostukset kyberhyökkäyksiin





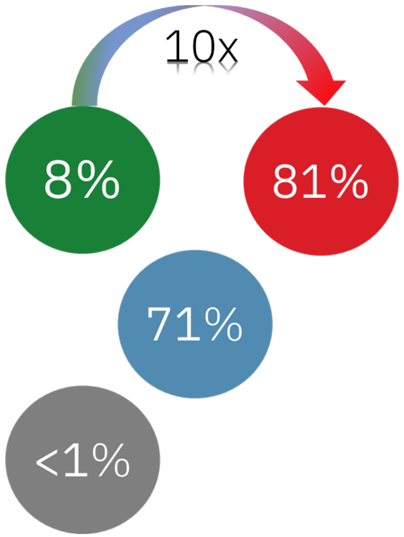
Jaettu vastuu – selkeät roolit & suunnitelmat reagointiin

Cyber Insurance market (USD Bn)



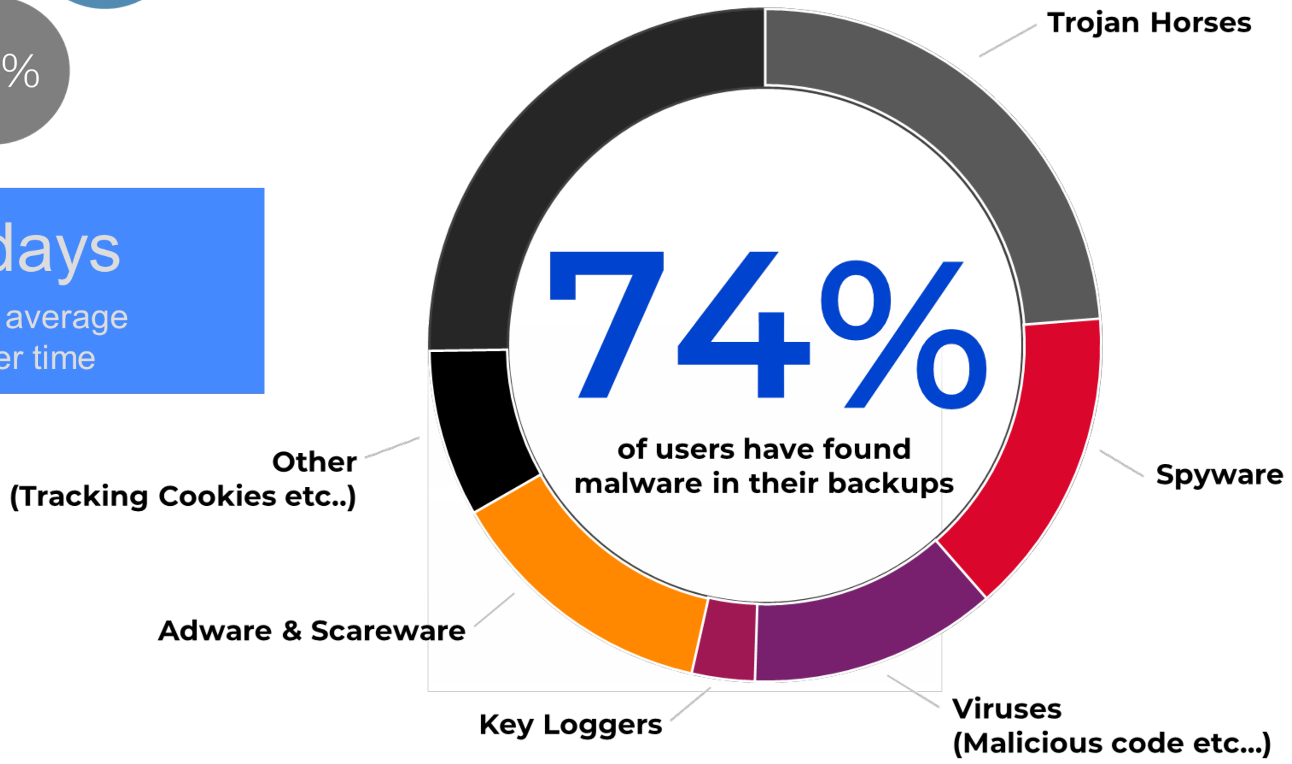
https://www.security.org/insurance/cyber/statistics/

Onko kaikki kunnossa ?



23 days
industry average
recover time

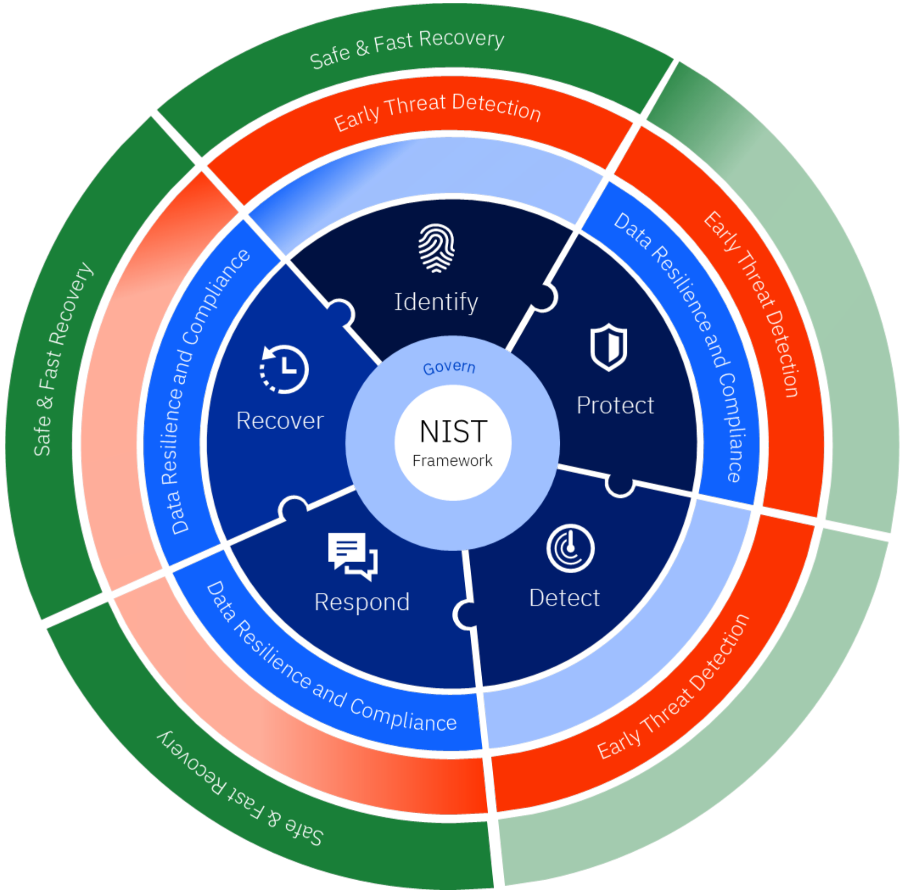
Haittaohjelmat ympäristössä, riippumatta nykyisistä SOC – kerroksen suojausta



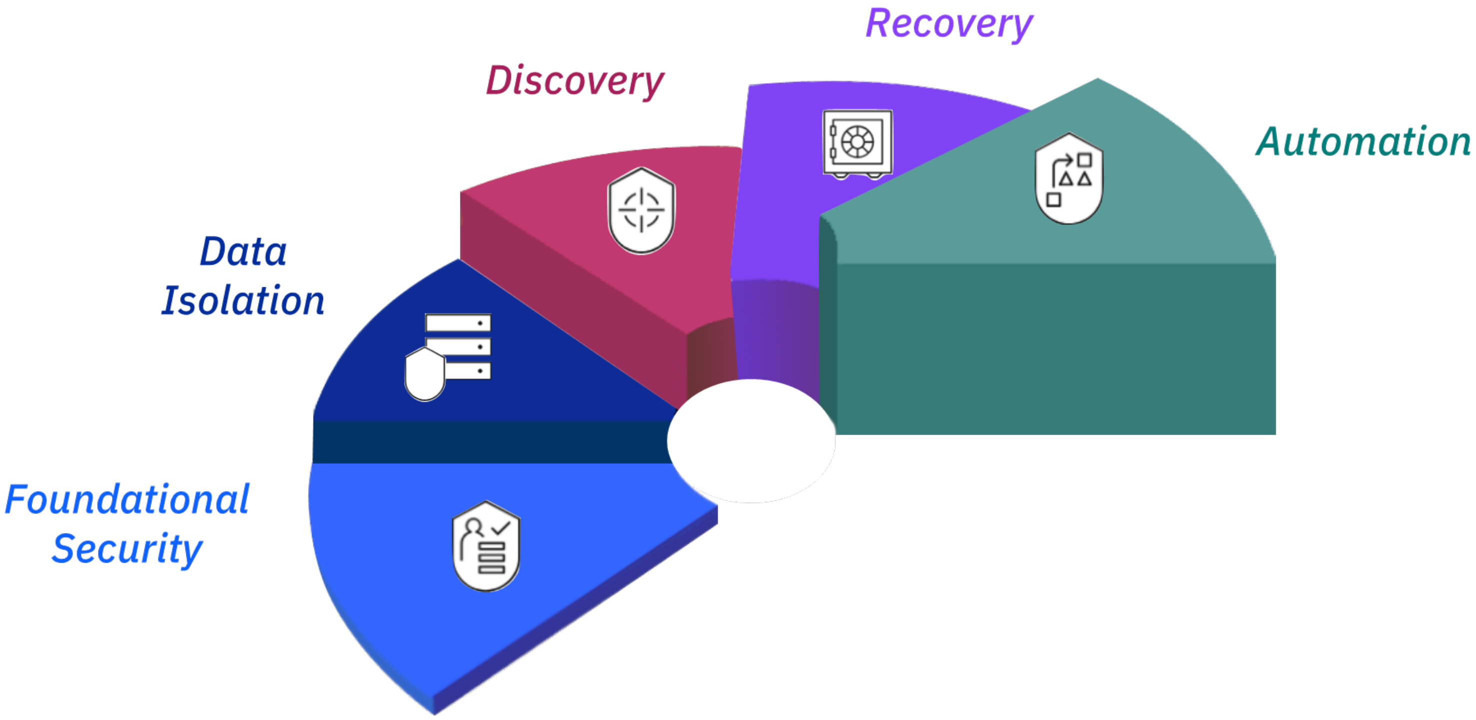
ransomware-trends_wpp.pdf, Veeam insight, 2025 Ransomware Trends and proactive Strategies

Varautuminen – Kuinka edetä

NIST –viitekehys teknologiariippumaton lähestymistapa



IBM näkemys perustuen NIST –viitekehykseen



Toiminnallisuus eri kerroksissa

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

IBM PoV: Operatiivinen jatkuvuustikas

1. Foundational Security

CYBER SECURITY
Security Operations Centre (SOC) **Integration**

User Credentials - Zero Trust Principals

End-point Security

Network Security - Firewalls etc

DATA CLASSIFICATION - Compliance, Criticality, Risk

DATA PROTECTION - Copies, Backups, DR, HA

IBM PoV: Operatiivinen jatkuvuustikas

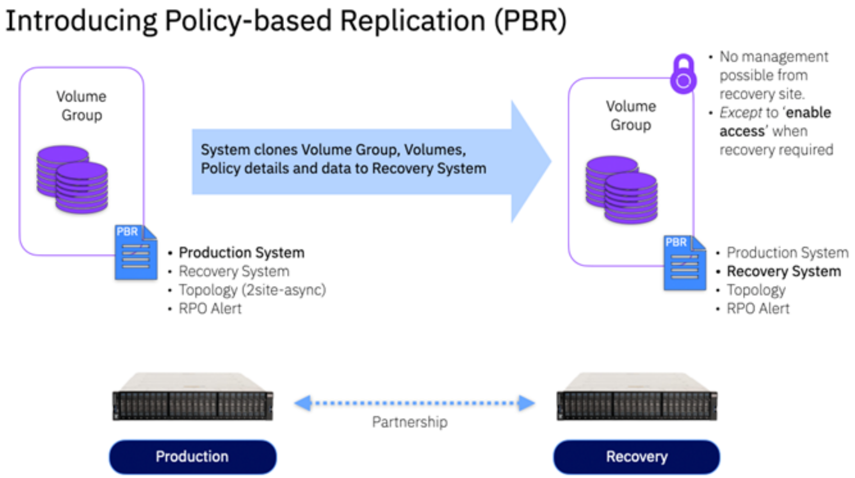
1. Foundational Security

IBM Storage

IBM Storage Virtualize, IBM Storage FlashSystem, and IBM SAN Volume Controller Security Feature Checklist

Updated for IBM Storage Virtualize Version 8.5.3

IBM



Back up from Storage Snapshots.
Lower the additional impact from backup activities on the environment by retrieving virtual machine (VM) data from Storage Snapshots.

On-Demand Sandbox.
Use Storage Snapshots to create completely isolated copies of your production environment in just a few clicks for fast and easy developing, testing and troubleshooting.

Quickly and easily recover.
Individual items or entire VMs with Veeam Explorer™ *for Storage Snapshots.*

Snapshot orchestration at the primary storage.
In addition to a backup chain, a Veeam backup job can save snapshots and manage their retention separately.

Suojauksen 4. ulottovuus

Cyber hyökkäyksistä palautuminen eroaa totutusta palautumisesta

Category	Traditional Recovery	Cyber Recovery
Nature of impact	Random e.g. natural disasters	Targeted engineered for maximum impact
Scope of impact	Local / Regional	Global can affect any connected systems
Backup repository affected	Not typical	Possible
Recovery point	Known	Unknown need most recent **uninfected** copy
Mitigation objective	RPO/RTO	RPO/RTO + **Safe Recovery**
Duration of impact	Hours to Days	Days to Weeks
Relative probability of occurrence	Low	High

Need Early Detection

Need Fast & Safe Recovery

IBM PoV: Operatiivinen jatkuvuustikas

2. Data Isolation

DATA ISOLATION

Air Gapping

Logical Isolation

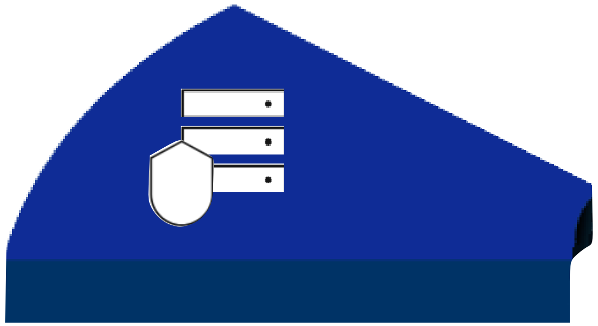
Physical Isolation

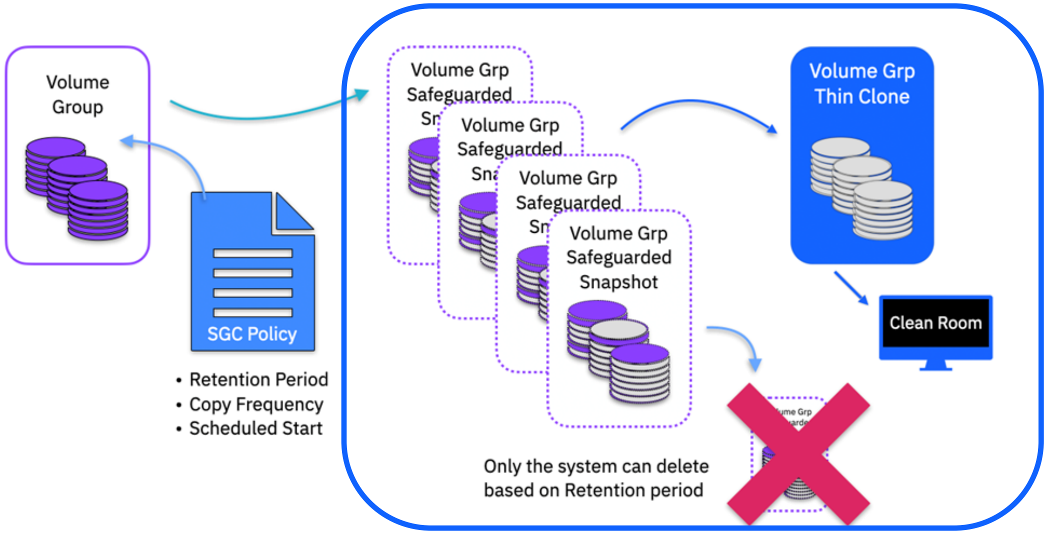
Least Privileged Access Principals

DATA IMMUTABILITY

IBM PoV: Operatiivinen jatkuvuustikas

2. Data Isolation



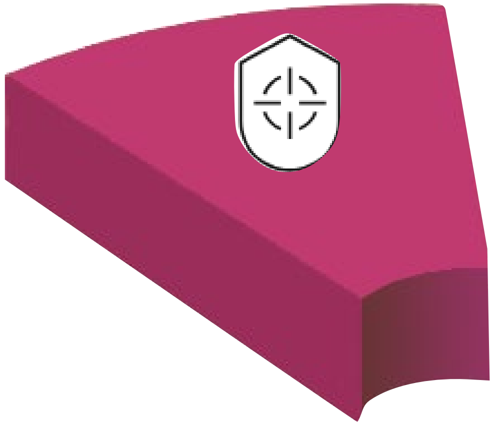


Physical tape is truly off-line

- Secure air gap
- Regulatory compliant WORM media
- Encryption at-rest
- Cost efficient multi-copy

IBM PoV: Operatiivinen jatkuvuustikas

3. Discovery



DISCOVERY/DETECT

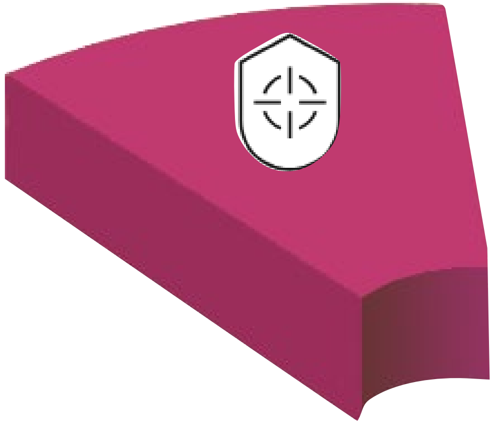
Data Integrity - Malware Scanning
Machine Learning - Inferencing

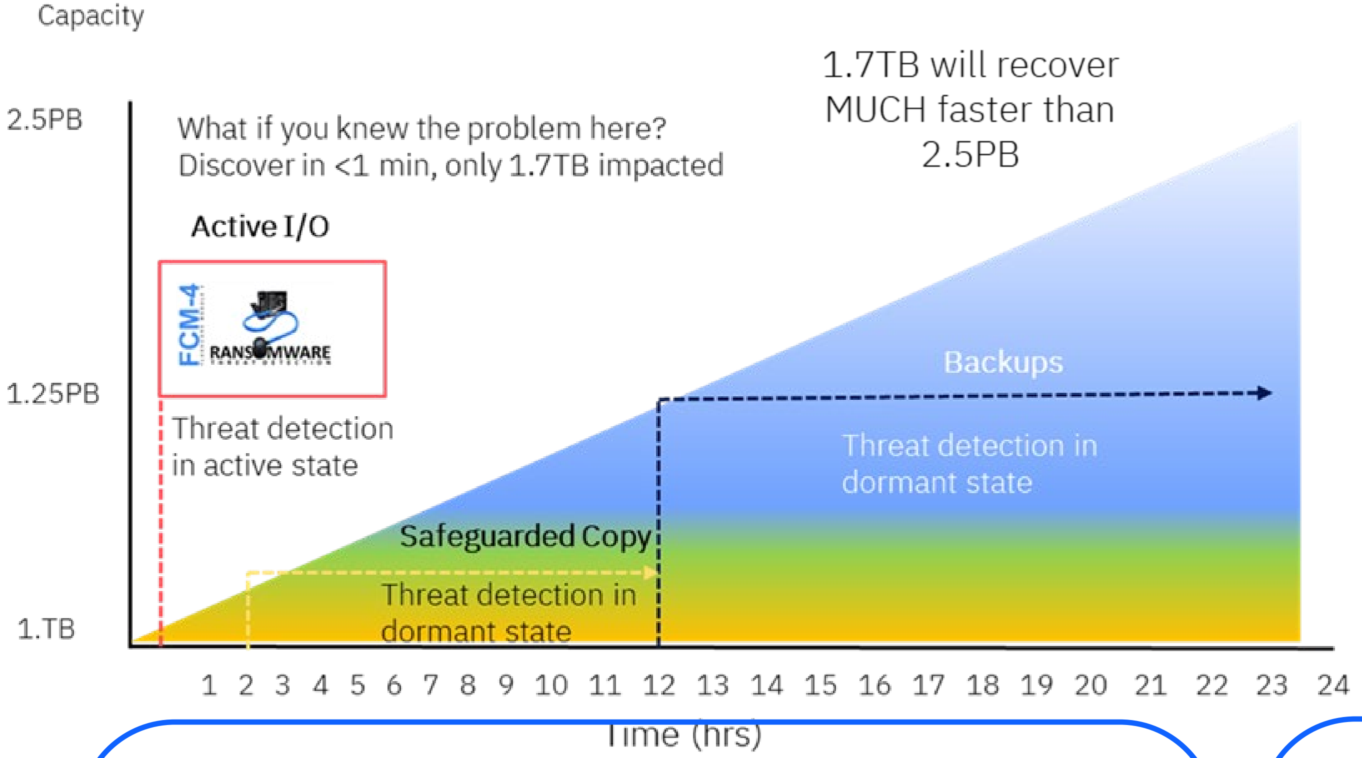
Primary Data (Snapshots)	Secondary Data (Backups)

ANOMALY DETECTION
Near real-time with Machine Learning & Inferencing

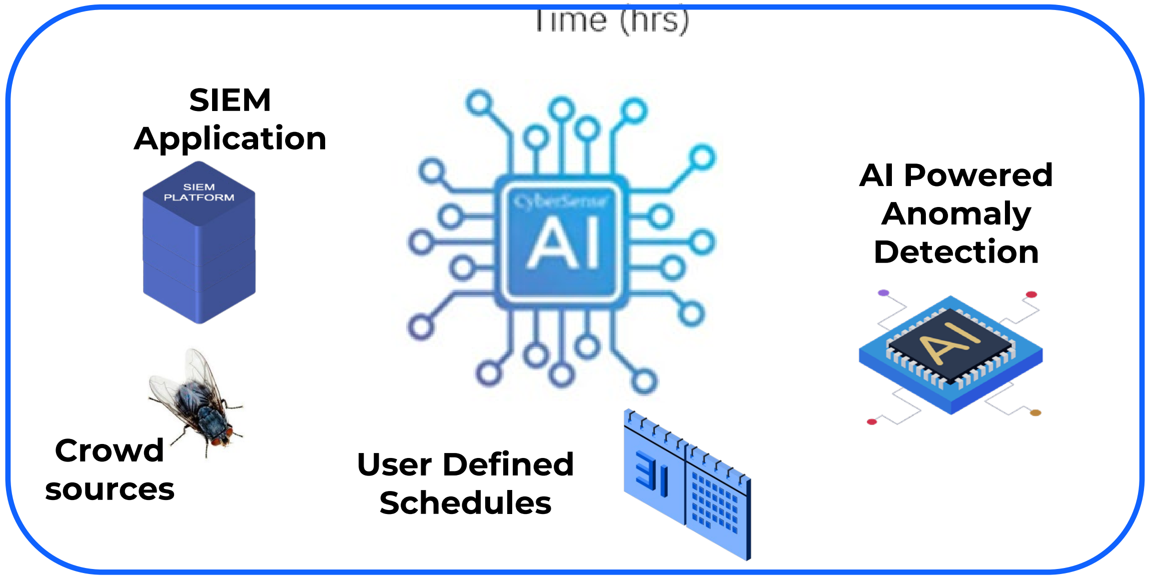
IBM PoV: Operatiivinen jatkuvuustikas

3. Discovery



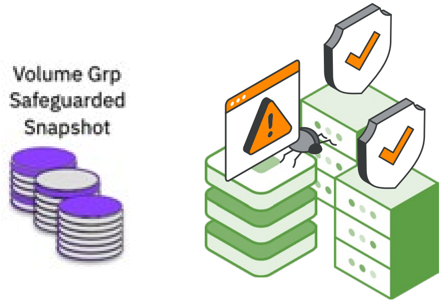


- Isolated & secure
- Software defined
- Designed for always-on automation



CleanRoom

Recovery testing & malware scanning



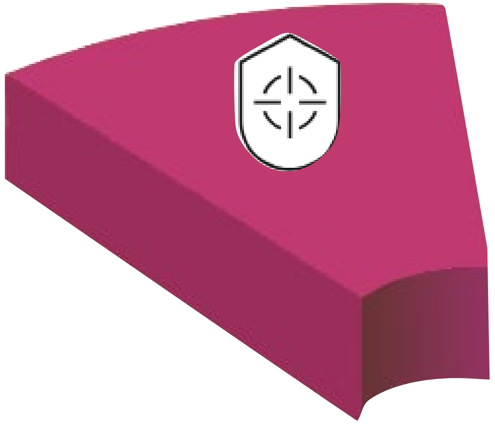
IBM PoV: Operatiivinen jatkuvuustikas

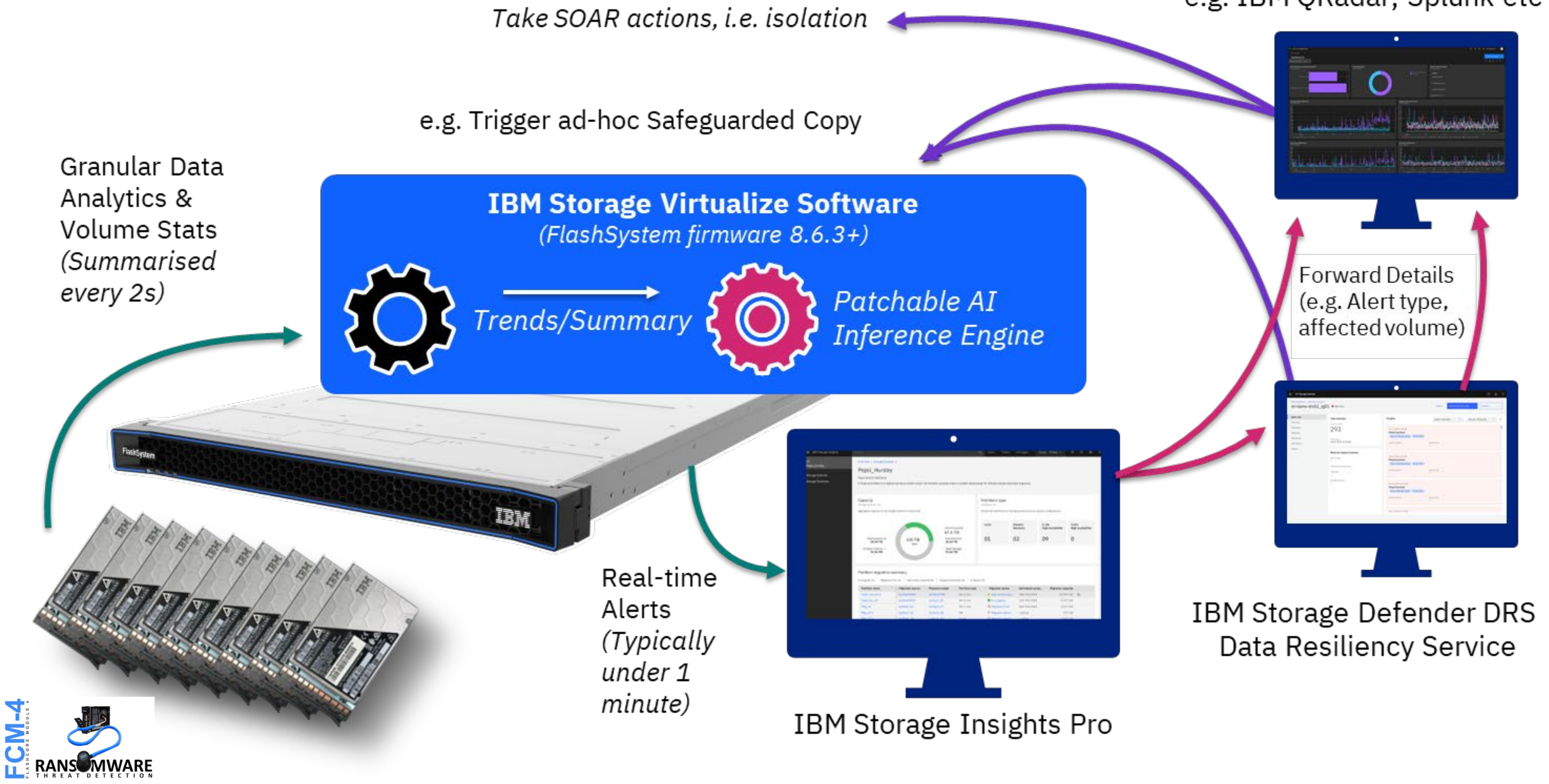
SNIA
Advancing storage & information technology

Computational Storage Architecture and Programming Model

Version 1.0

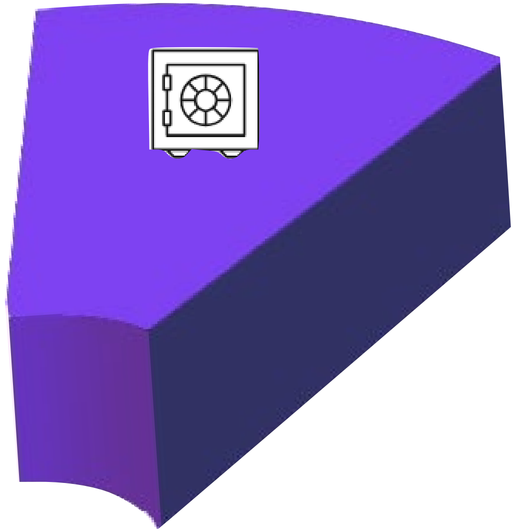
3. Discovery





IBM PoV: Operatiivinen jatkuvuustikas

4. Recovery



FAST & SAFE RECOVERY

Clean Room, Cyber Vaulting

Modern Recovery
(Instant Mass Restore)

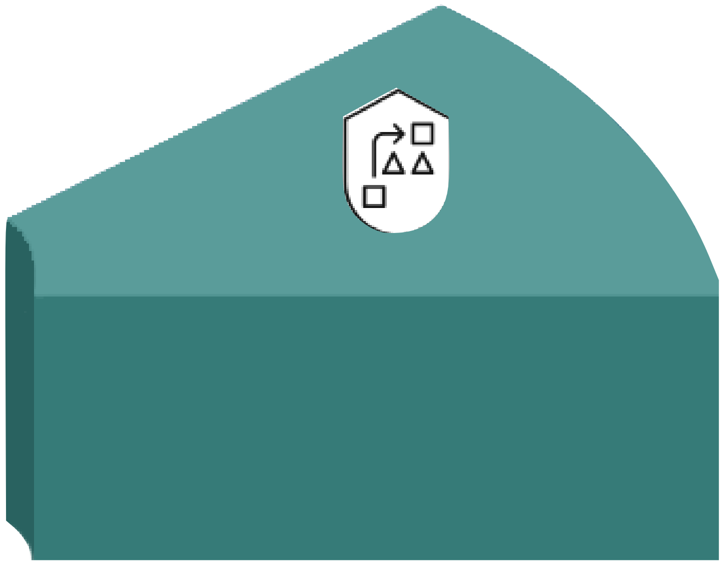
Known Recovery Stance
(Clean Copies)

MINIMUM VIABLE COMPANY
Understanding from Classification - on-array instant restoration

FULL COMPANY
Understanding from Classification - secondary restoration tasks

IBM PoV: Operatiivinen jatkuvuustikas

5. Automation



AUTOMATION & ORCHESTRATION

Integration with SIEM/SOAR

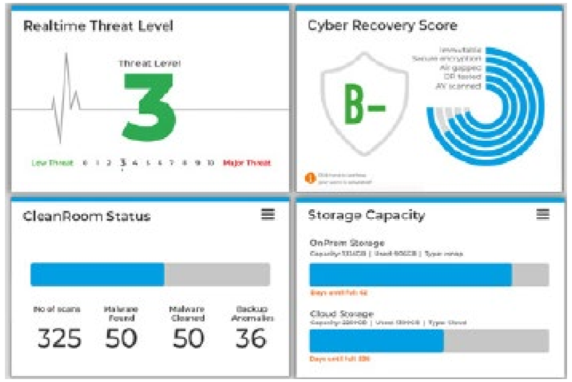
Automated Isolation

Automated Recovery

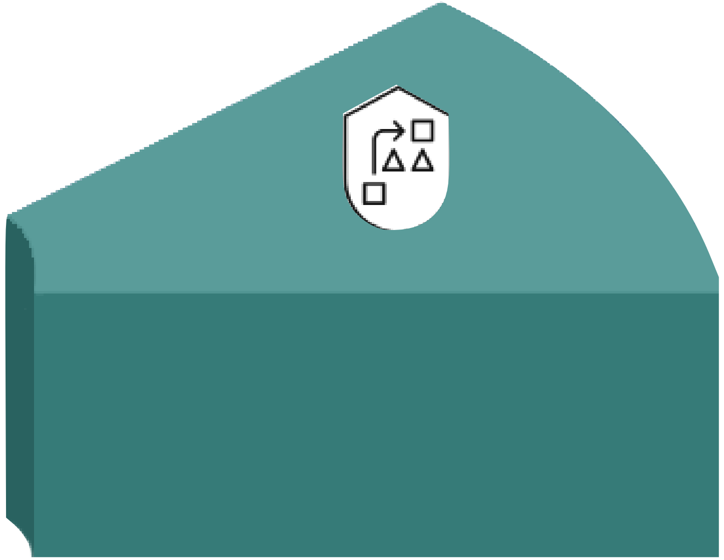
STORAGE RESILIENCY

Alerting, Orchestrated Recovery Groups, Playbooks

IBM PoV: Operatiivinen jatkuvuustikas



5. Automation

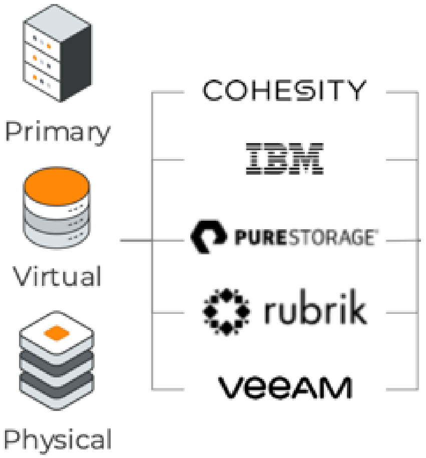


Customer Security Tools

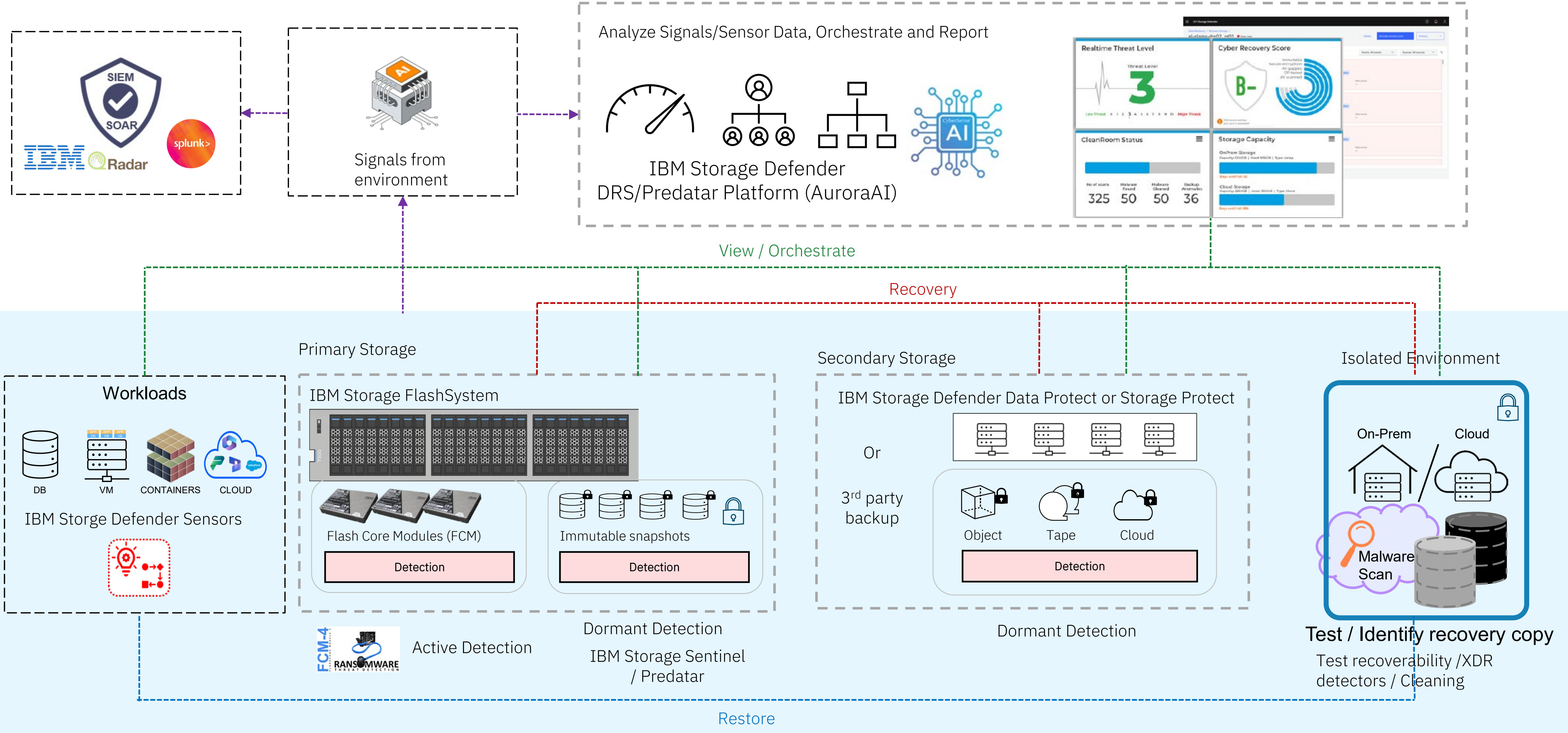
Microsoft Sentinel · Radar · splunk>

Customer Communication

freshdesk · slack · servicenow · Microsoft Teams



Datan saatavuus on tiimityötä




KIITOS