# Data Resiliency for Ransomware & Cyber Warfare

Peter D. Bille – Storage Solution Specialist
Pdbille@ibm.com


IBM

# Data Resilience

# Why Act Now?

**2X**
Cyber Attacks YTY

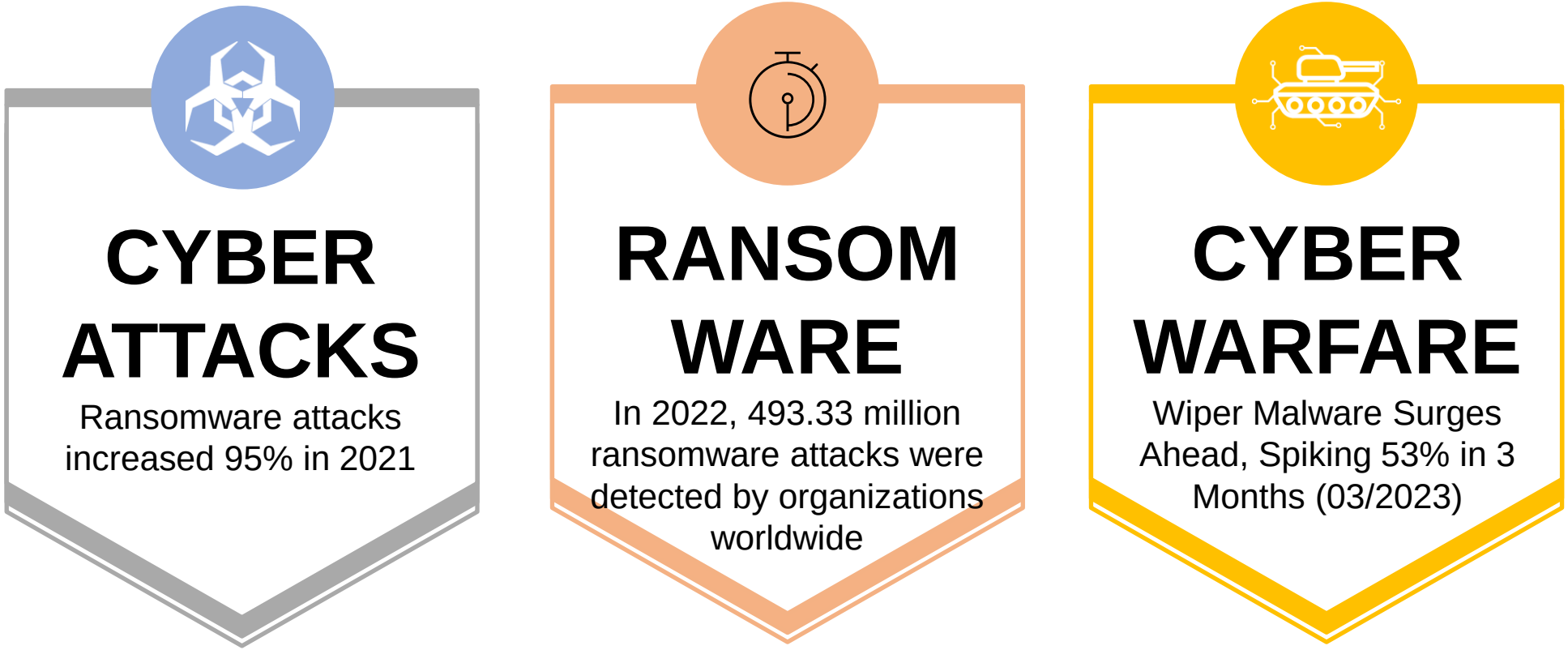
**53%**
Wiper Malware Surges Ahead
first 3 months of 2023

**21%**
dormant threats, up from 5% YTY
(270 days to detection)

**23**
days, average recovery
after an attack

**93%**
93% explicitly target backups

# The Trend


CYBER ATTACKS
Ransomware attacks increased 95% in 2021
RANSOM WARE
In 2022, 493.33 million ransomware attacks were detected by organizations worldwide
CYBER WARFARE
Wiper Malware Surges Ahead, Spiking 53% in 3 Months (03/2023)
INCREASING THREATS

# What is Cyber Resiliency?

**According to NIST:**

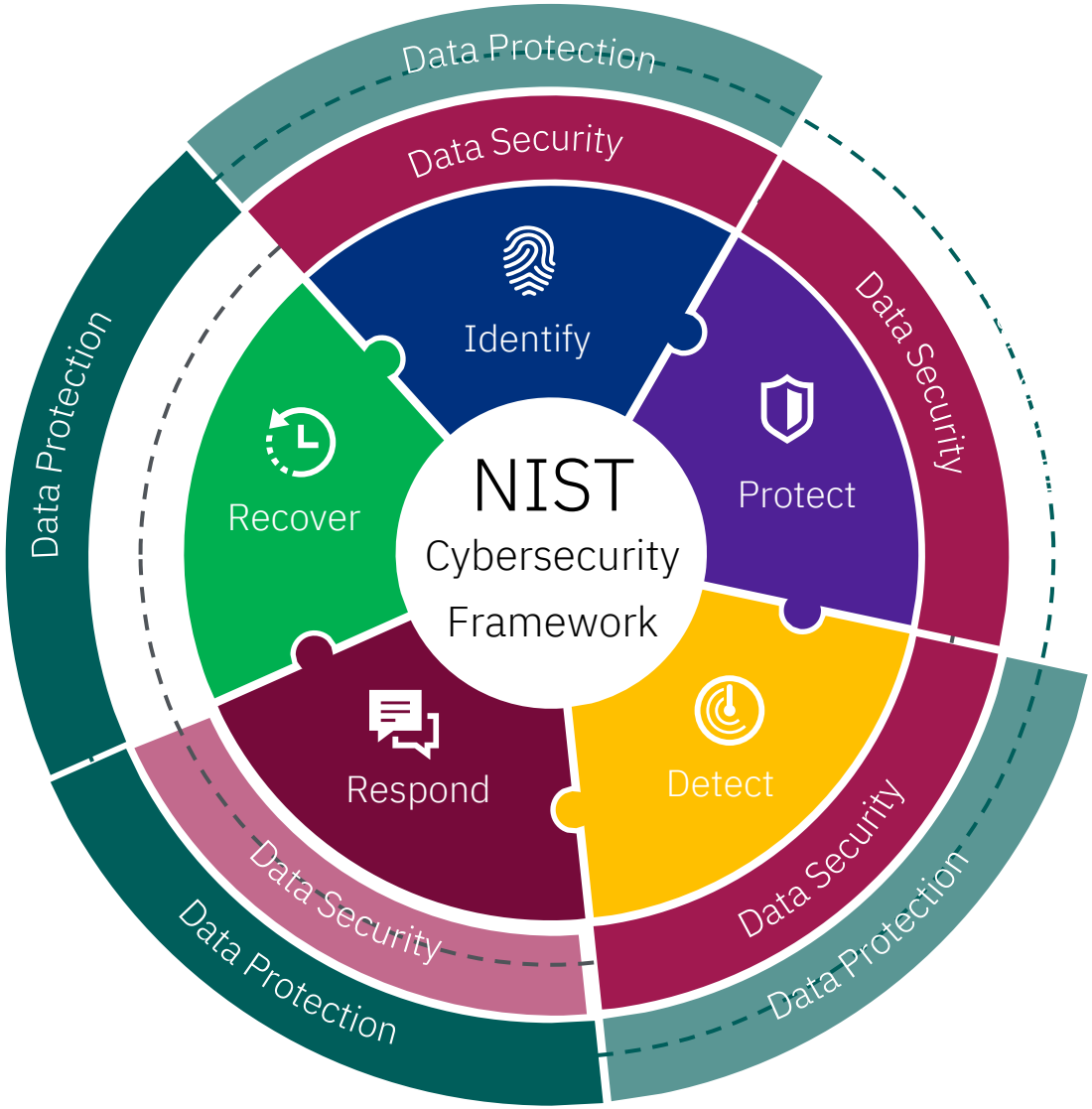
- The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
- Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment

# *The Need for **integrated** data security and protection = **DATA Resiliency***

## Data security
helps detect and prevent attacks, but nothing to recover

## Data protection
is primarily reactionary and does not help avoid attack

Together, data security and data protection fulfill the NIST framework
= Data resiliency



# Why traditional recovery solutions won’t protect you!

| | You have | What is required |
|---|---|---|
| Replication | Data is being replicated continuously but logical errors are also replicated instantaneously | Scheduled point in time copies stored in an isolated, secure location |
| Error detection | Immediate detection of system and application outages | Regular data analytics on point in time copies to validate data consistency |
| Recovery points | Single recovery point that likely will be compromised | Multiple recovery points |
| Isolation | All systems, storage and tape pools participate in the same logical system structure | Air gapped systems and storage so that logical errors and malicious intruders can not propagate |
| Recovery scope | Continuous availability and disaster recovery | Forensic, surgical or catastrophic recovery capabilities |

# What is an Immutable Copy?

**An immutable copy is a backup file that can't be altered in any way. An immutable copy is unchangeable and able to be deployed to production servers immediately in case of malware, ransomware, wiperware attacks or other data loss.**

# How to implement Point in Time copies to Speed up the recovery from cyber attacks

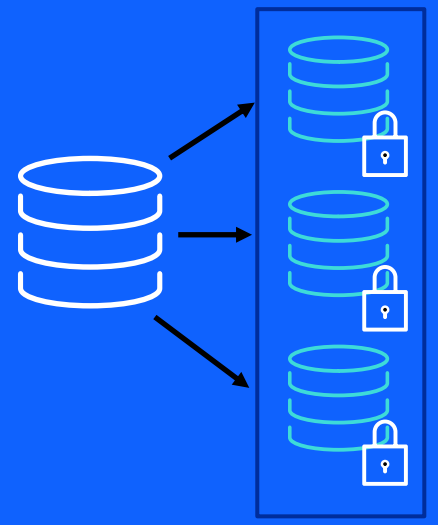
**Automatic**
creation of regular backup copies

**Immutable/unchangeable**
point-in-time copies of production data

**Isolated**
logical air-gap offline by design

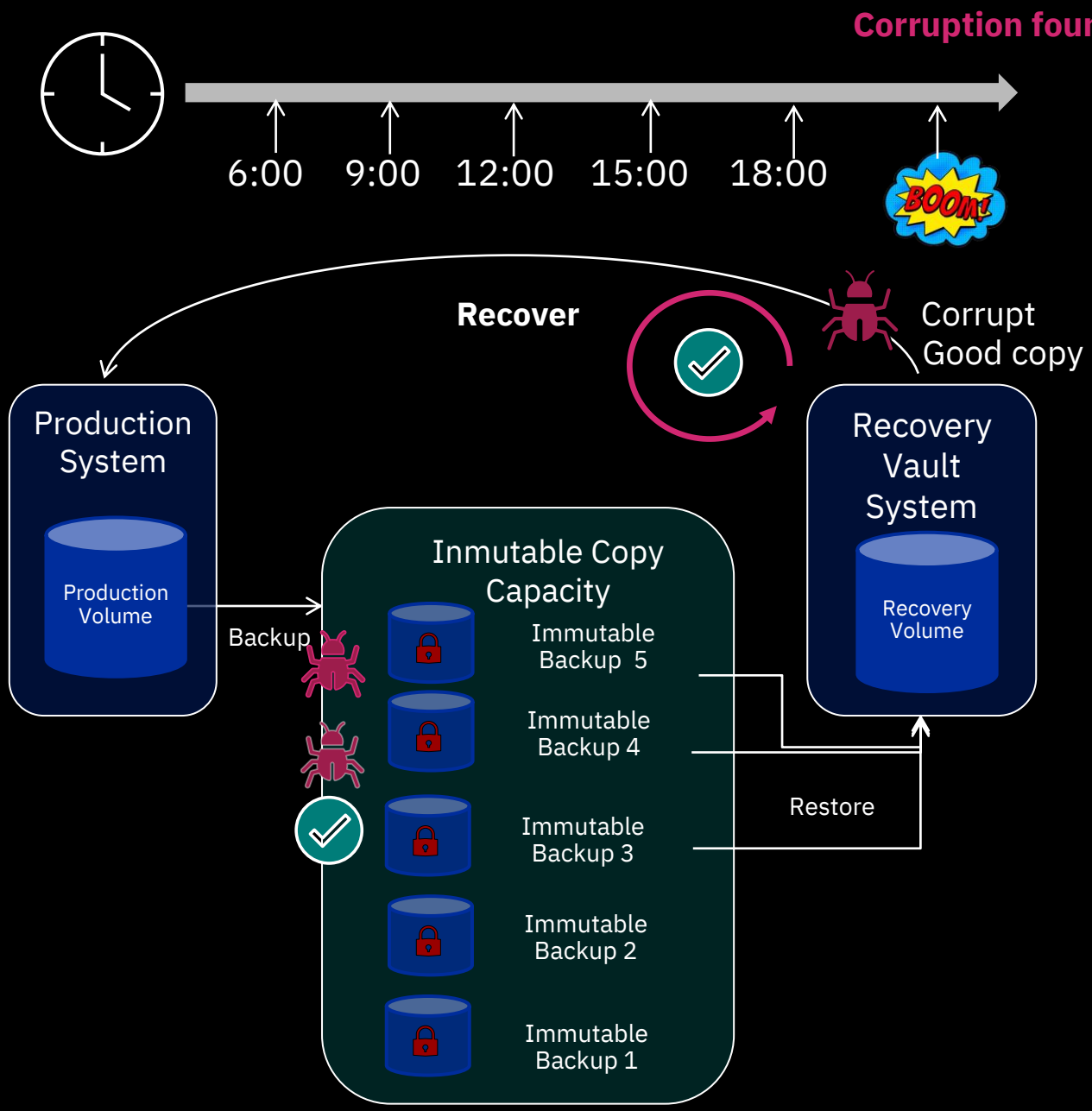
**Fast**
restore from copies on primary storage

Prevents modification or deletion of copies due to user error, malicious destruction, or ransomware attack

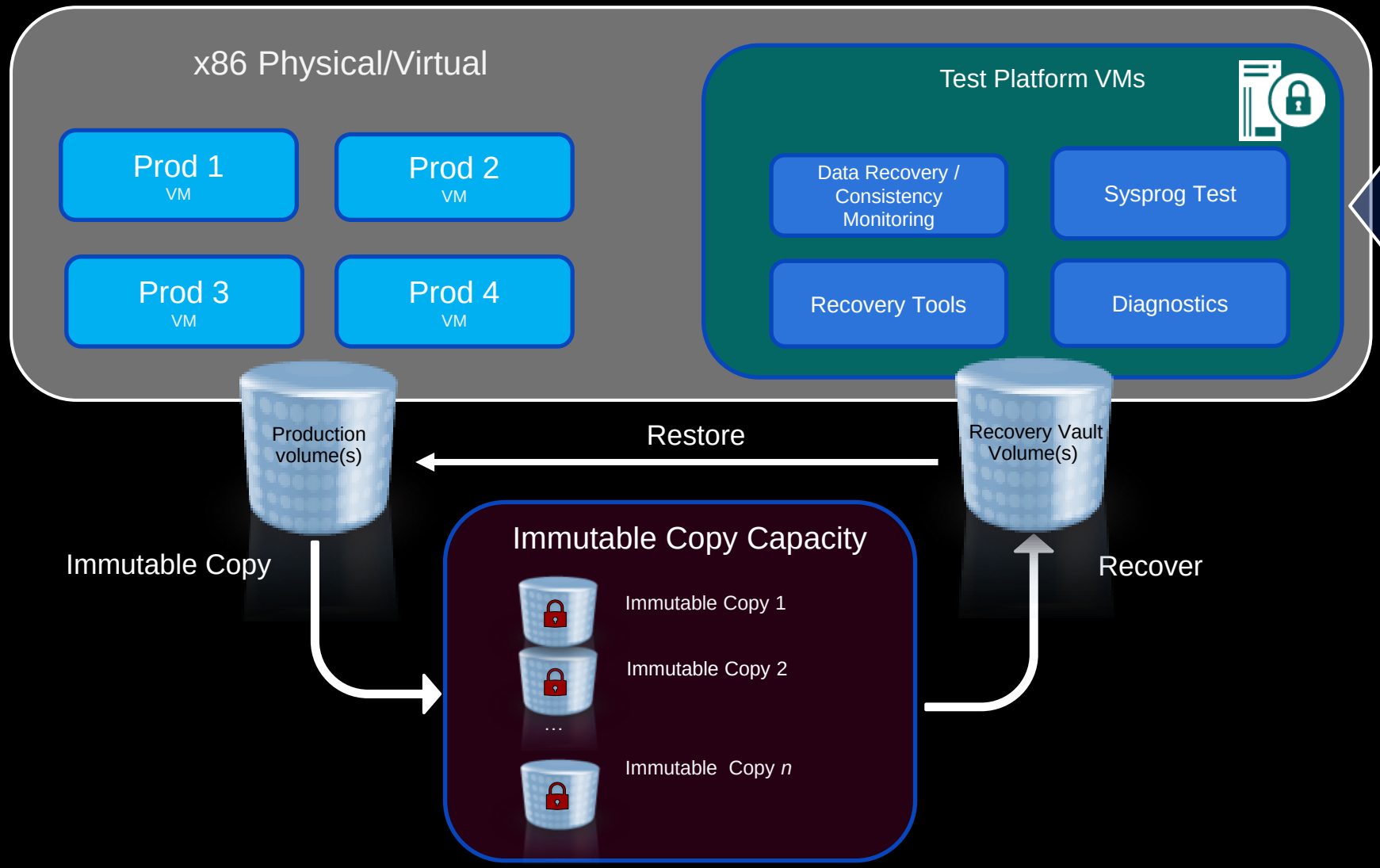


# Immutable Copies Provide

- **Logical Corruption Protection** to prevent sensitive point in time copies of data from being modified or deleted due to errors,  destruction or ransomware
- Data is accessible *only* after immutable copies are **recovered to a separate recovery volume**.
- **Proactive monitoring** for signs of attack
  - Identify Safe Volume to recover based on time index of identified attack
- Recovery volumes are used for:
  - Data validation
  - Forensic analysis
  - Restoration of production data



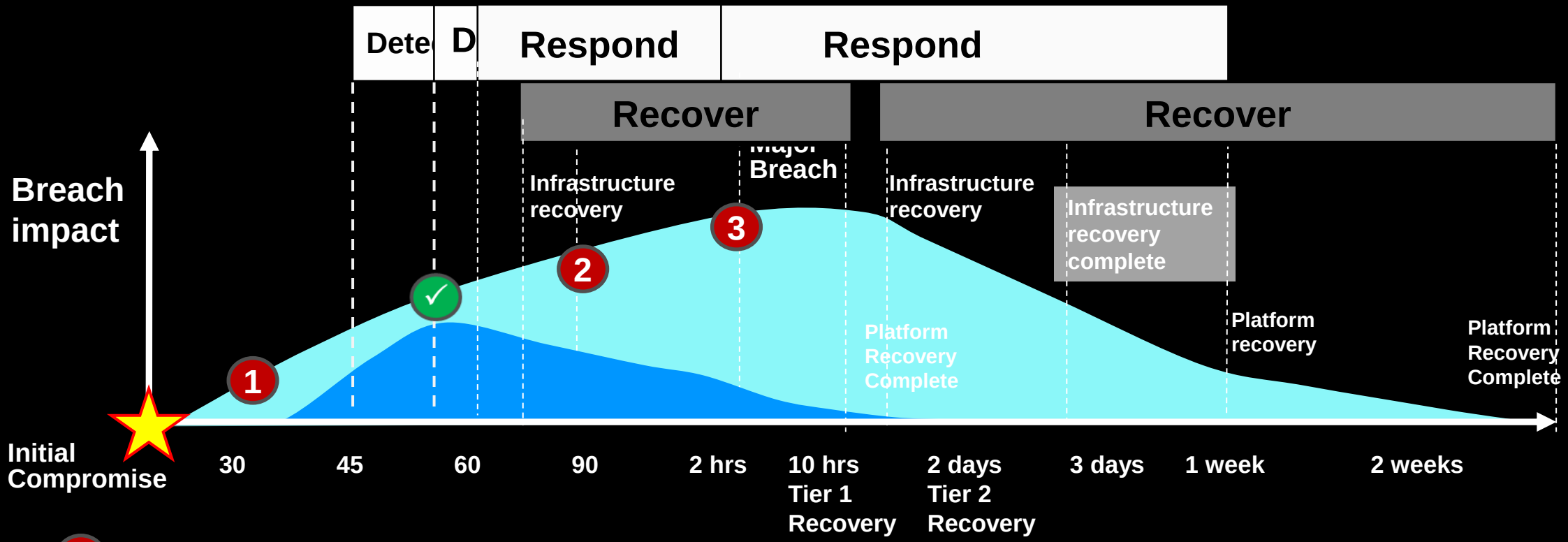
# Next Step: Create a Test Platform to identify problems, and minimize impacts




Cyber Vault Server/VMs

1. Establish analysis environment
2. Run diagnostic tools
3. Determine data validity
4. Promote back to production

# Cyber attack detection and recovery




1. Corruption of data occurs - but not yet detected
2. Without immutable copies and Data Resilient implementation 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

✓ Due to Immutable copies and the use of the Data Resilient implementation, data is continuously checked and corruption is found and corrected EARLIER & FASTER

# Start the 3 Step Process to Protect Your Data

## 1

### Make immutable copies of data

- Immutable SNAP Shot Copies
- Automated creation and restore of copies

## 2

### Test copies of data

- Isolated infrastructure to test copies
- Ensure copies not corrupted using application tools
- Test infrastructure logically or physically air-gapped
- Blueprint for testing and recovery process

## 3

### Automate process

- Automation of making and testing copies
- Automation of test & restore process

# Typical Current Environment

## Immutable Copies of Data

Most Don’t have this
Maybe Air Gap “Traditional Backup” based solution

## Proactive Monitoring

Almost all have a SIEM

## Data Resiliency

Methodology & Automation

## Rapid Recovery

**MOST can NOT do this**

## Data Copy Test and Validation

Many have application based scanning tools
e.g. DBA manage scanning and recovery of DB

# Look at what is needed!

What do we need?

We need tooling/solutions that:

- Detect potential attacks as early as possible; even using technology as AI and ML for behavioural analysis
- Identify at the database/file and even member level what has changed and when
- Ability to know what the last good version of the data was and where it's backed up
- Automation to generate the recovery points required to facilitate a surgical recovery

# Enterprise-grade cyber security and resiliency

**Data validation**
Detect data corruption early or certify that the copy is clean

**Forensic analysis**
Investigate the problem, determine the best recovery action

**Surgical recovery**
Extract data from the copy and logically restore back to production environment

**Catastrophic recovery**
Recover the entire environment back to a point in time copy

**Offline backup**
Backup copy of the clean environment to offline tape media

Oracle tools such as DBVerify, backup tools to validate checksum or run with db_checksum

Db2 tools such as Db2 inspect and db2dart

SQL Server tools such as checkdb or checktable

MongoDB tools – backups and oplog forward recovery

Warehouse databases – Typical to have a set of validation SQL that is run against the tables after each load job and use the output of that SQL against the live dbase to validate that the data in the tables was still good

SIEM Tools, Data Analytic Tools

Index Engines CyberSense

# You Will Need A Cyber Resilience Strategy

An effective cyber resilience strategy relies on several operational activities:

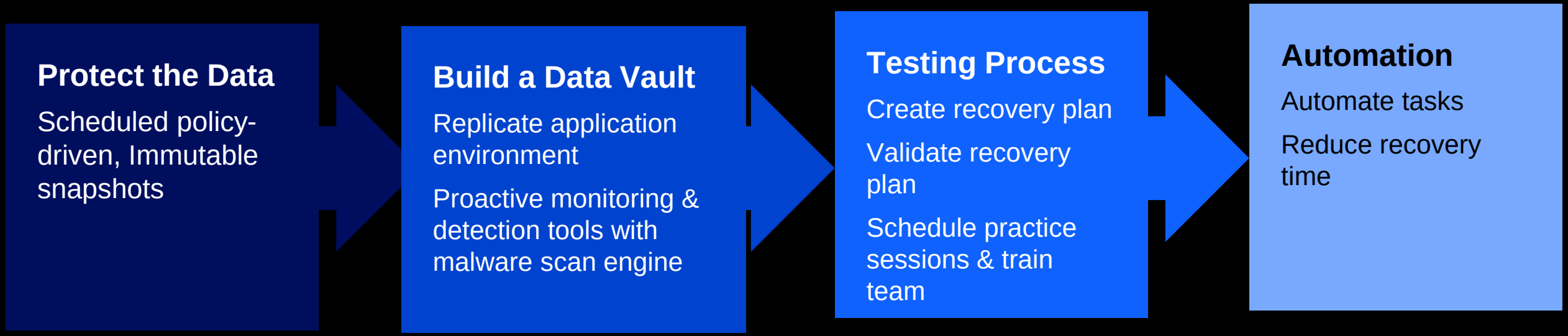
- Business continuity (BC)
- Disaster recovery (DR)
- Incident Response (IR)
- Cybersecurity Planning/Plans

The goal is to ensure the organization can resume operations as soon as possible in the aftermath of a ***successful*** cyber attack

In practice, the above elements usually exist in silos

A successful cyber resilience plan depends on understanding the interrelationships among these parts and how each component complements the functions of the others

# Roadmap to achieving Cyber Resiliency




**“Continue The Journey”**

# Cyber Resiliency

## Thank You For Your Time

Peter D. Bille – Storage Solution Specialist
Pdbille@ibm.com