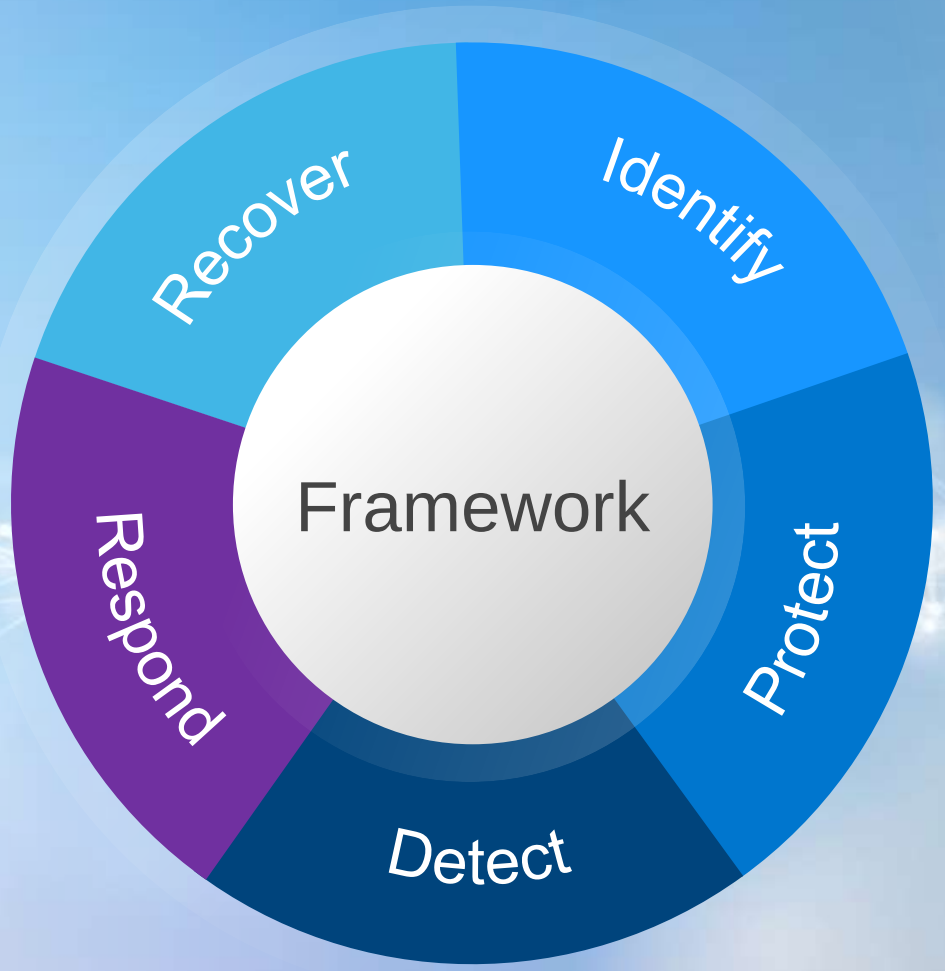
Cyber Recovery Vault

Dell Technologies – Data Protection Solutions
David Steinbrink

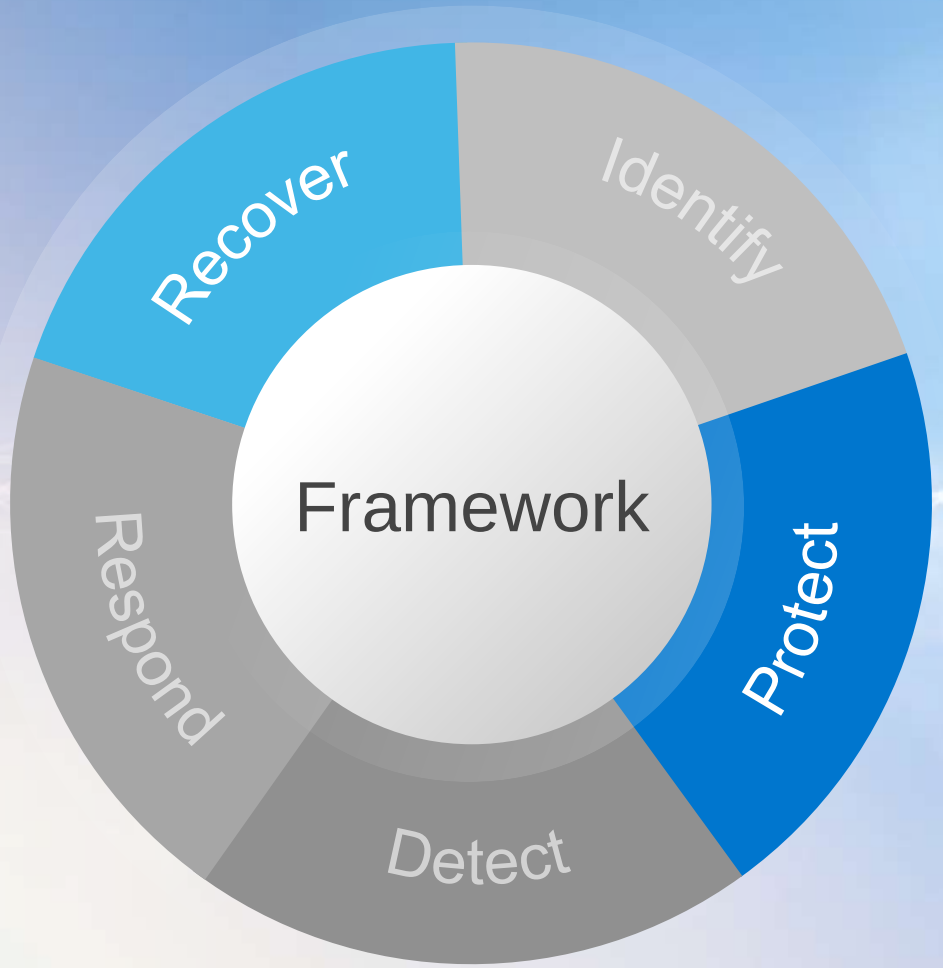
Cyber resilience is a strategy.

A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions.

Example: NIST Cybersecurity Framework



Source: https://en.wikipedia.org/wiki/Cyber_resilience



Cyber Recovery is a solution.

A data protection solution that isolates business-critical data away from attack surfaces.

Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality.

Source: https://en.wikipedia.org/wiki/Cyber_resilience

DELL Technologies

NIST Cyber Security Framework

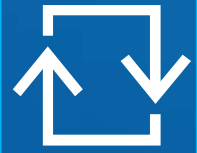
A high-level holistic strategy that helps organisations:

Identify

Protect

Detect

Respond



Recover

Data

Resources

Assess risk

Protect against the known bad.

Reduce the attack surface.

Detect suspicious and unknown threats

Mitigate the threat, understand the adversaries

Recover from the attack

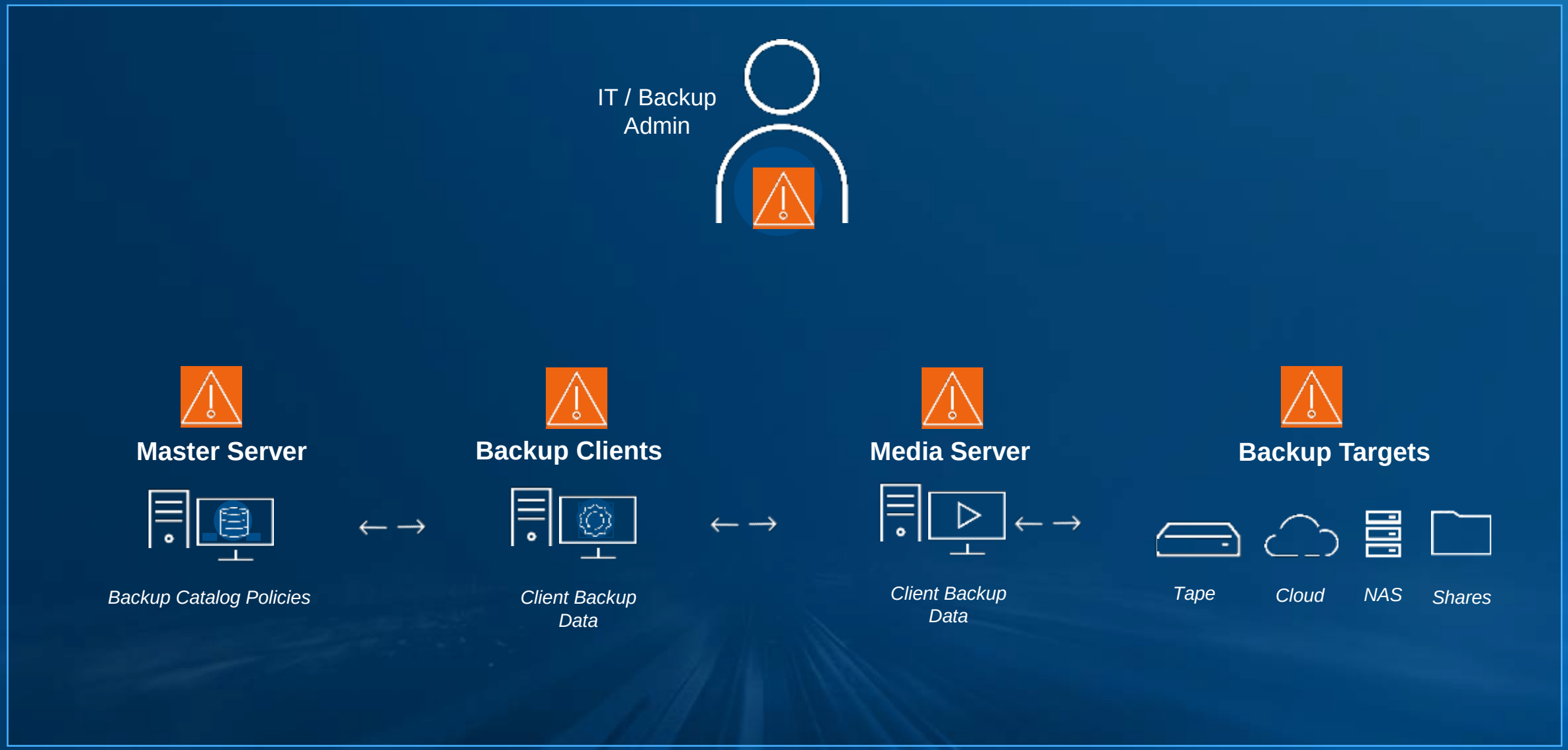
Before

During

After

Immutability is not offline

Cyber Attack Ziel: … die Datensicherungen



Cyber Recovery Requirements

Modern threats require modern solutions

Was ist ein Cyber Recovery Vault?

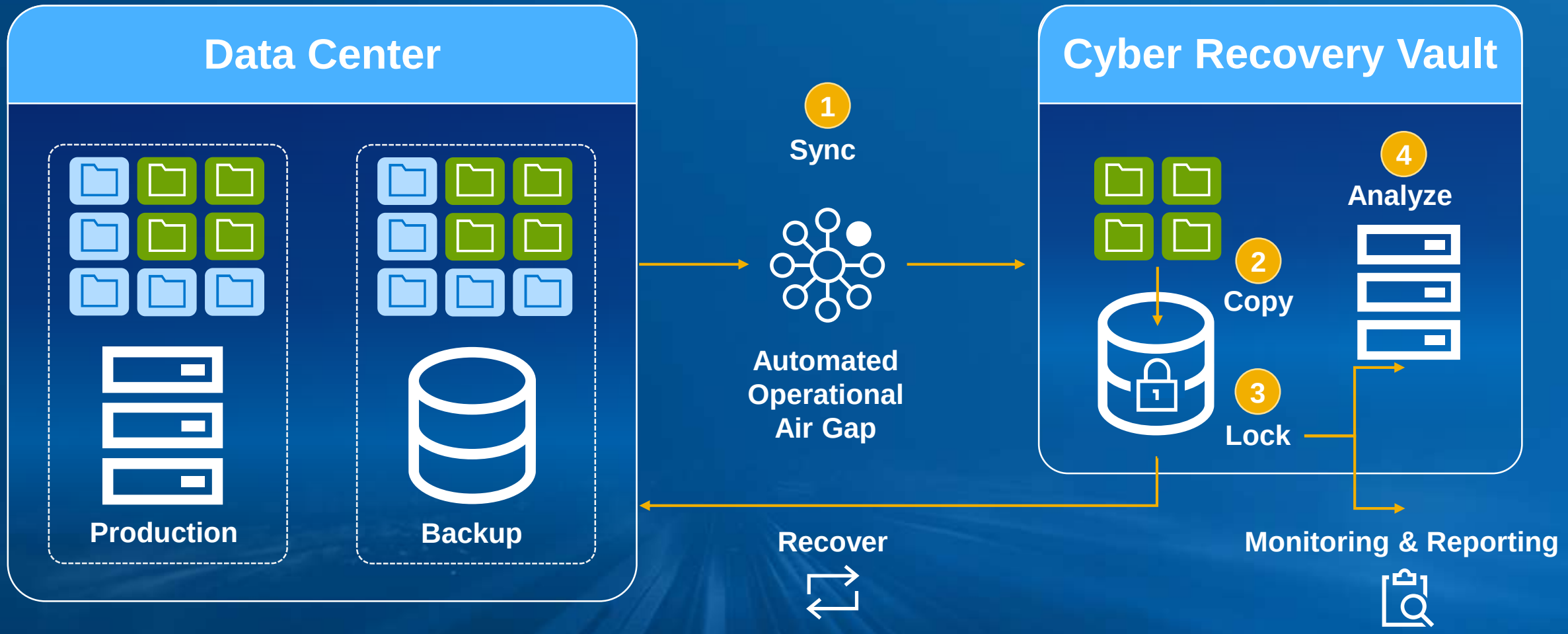
- ✓Erstellen einer separaten Umgebung.
- ✓Halten Sie die Angriffsfläche so klein wie möglich.
- ✓Machen Sie es so unabhängig vom Rest wie möglich.

- ✓Haben Sie ein separates Management-Team
- ✓Physischen Zugriff einschränken

- ✓Implementieren Sie Hardening und Retention Lock
- ✓Nutzen Sie ein Airgap und verwenden sie gehärtete Firewalls für das Reporting
- ✓1 LAN Anschluss ist ausreichend
- ✓Automatisierung und Steuerung von innen umsetzen
- ✓Reportfähig und Auditierbar (Analyse & Forensik)

PowerProtect Cyber Recovery

Data Vaulting For Critical Data



DELL Technologies

Defense in Depth

Detailed SOC Reporting

Data Diode

Same as Prod DD

Exposed <4hrs

IP Tables

Immutability

Time Tampering

Multiple Offline Copies

Advanced Analytics

Secure Test / Restore

No CIFS/NFS

2 Users / MFA

Restricted OS

Hardened System

Reverse Path Filtering

Industries smallest Attack Surface

AES256 & TLS | True airgap | Single Port | Point to Point

Replication

Production Data Domain

Vault Data Domain

No Remote access

DELL Technologies

How CyberSense Works

Machine learning enables early detection & rapid recovery from a cyber attack

SECURITY ANALYTICS
200+ statistics indicative of cyber attack

CORRUPTION DETECTED
Alert when suspicious activity is detected

COMPREHENSIVE INDEX
Changes in content over time

MACHINE LEARNING
Trained on thousands of trojans and attack vectors

POST ATTACK FORENSICS
Detailed reports, including last good backups for rapid recovery

CyberSense Provides

- Attack vector notification
- Ransomware detection
- Corrupted file details
- Data changes / deletions
- Breached user accounts
- Breached executables
- Last good backup copy

Analyse der Backups

CyberSense Analytics

100+ full content analytics that are indicative of data corruption

Metadata

Known ransomware extensions

Mass deletions/creations

Content Entropy

Based on full content. Entropy score from 0 to 99, with 99 representing encryption

Content

File extension mismatch from true type

Content corruption

Integrity

Validate the integrity of files, databases and backup images

CyberSense Analytics

Validate Data Integrity Over Time

Good Version
File EXT: .DOC
Filetype: WORD
Size: 28KB
Entro[illegible]

Monday

Tuesday

Last Good Version
File EXT: .DOC
Filetype: WORD
Size: 3,765KB
Entropy: 59

Corrupted
File EXT: .FUN
Filetype: Undefined
Size: 3,894KB
Entropy: 99

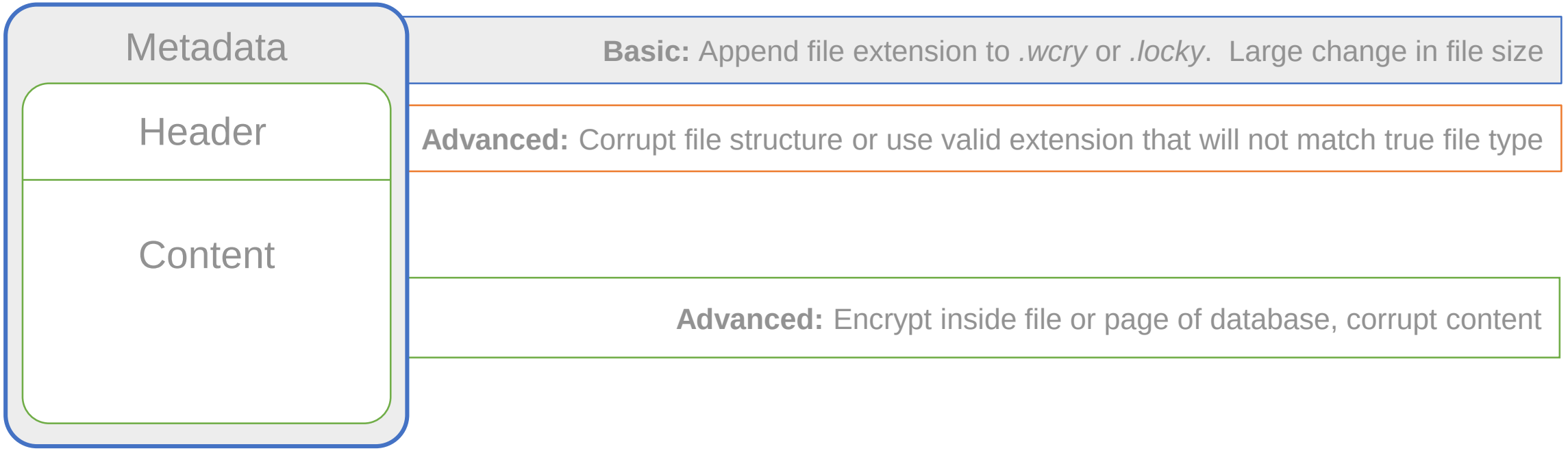
Wednesday

How Data is Corrupted

From Basic to Advanced Attacks

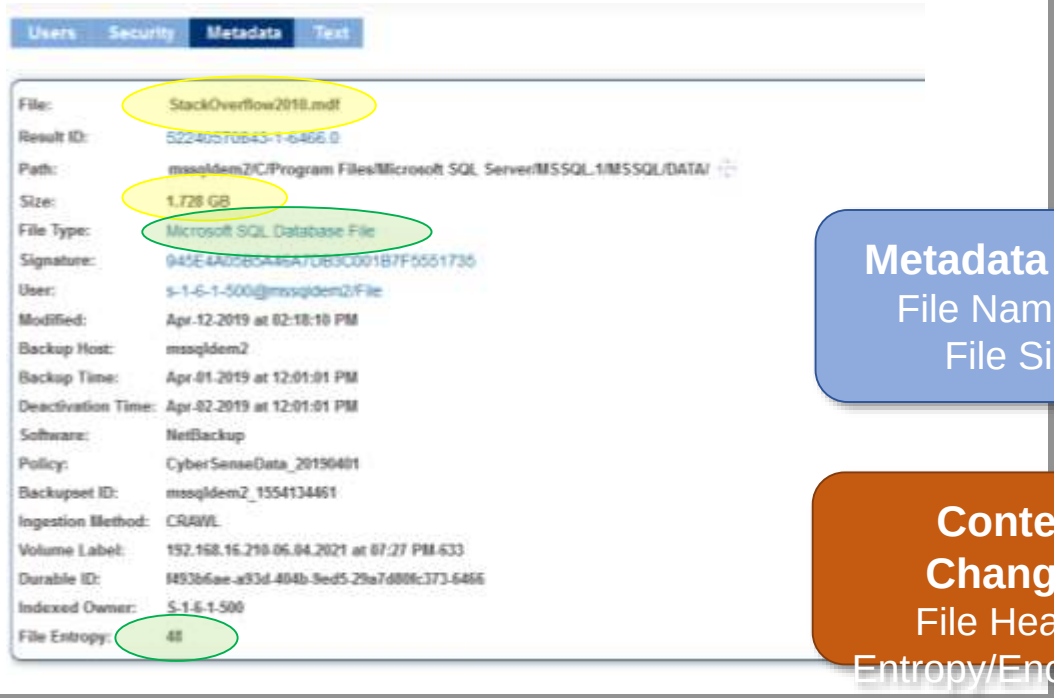
CyberSense **full content** analytics is **99.5%** confident in detecting suspicious behavior

Bad actors will start with basic corruption, then move to advanced when basic fails



Comparison of Metadata vs Content Analytics

AlphaLocker – Strong Encryption Maintaining Original File Name



Metadata Intact
File Name/Ext
File Size

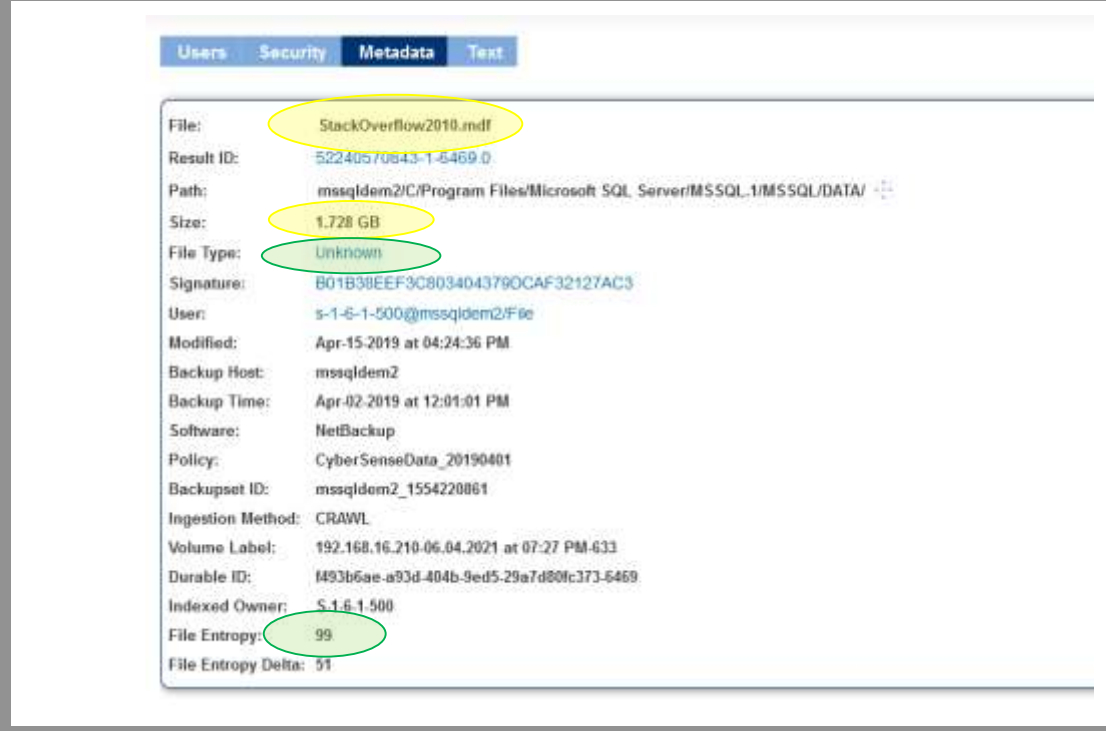
Content Changed
File Header
Entropy/Encryption

01 Pre-Attack Version

Last good version

02 Post-Attack Version

Corrupted file




DELL Technologies