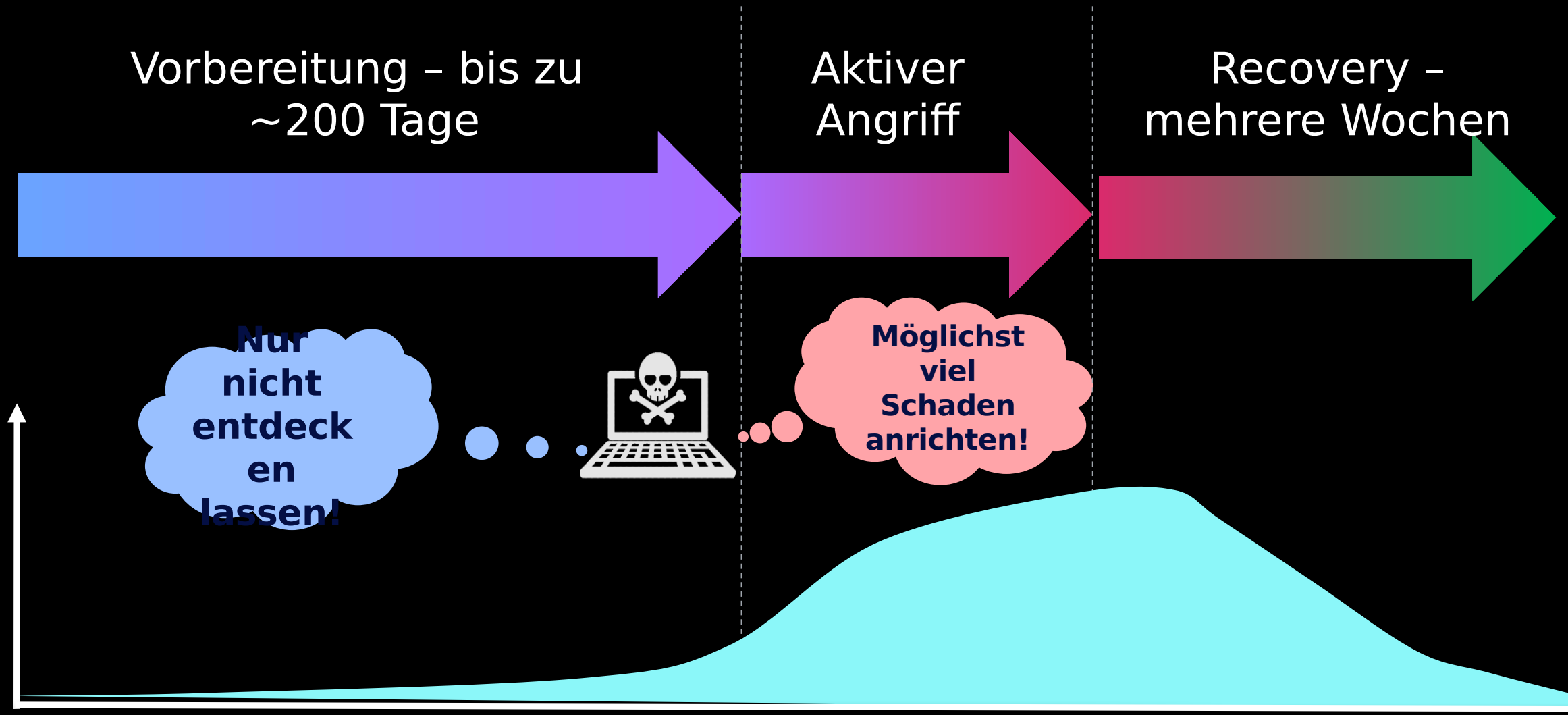
ADICOM

ADICOM Data Resilience by PREDATAR

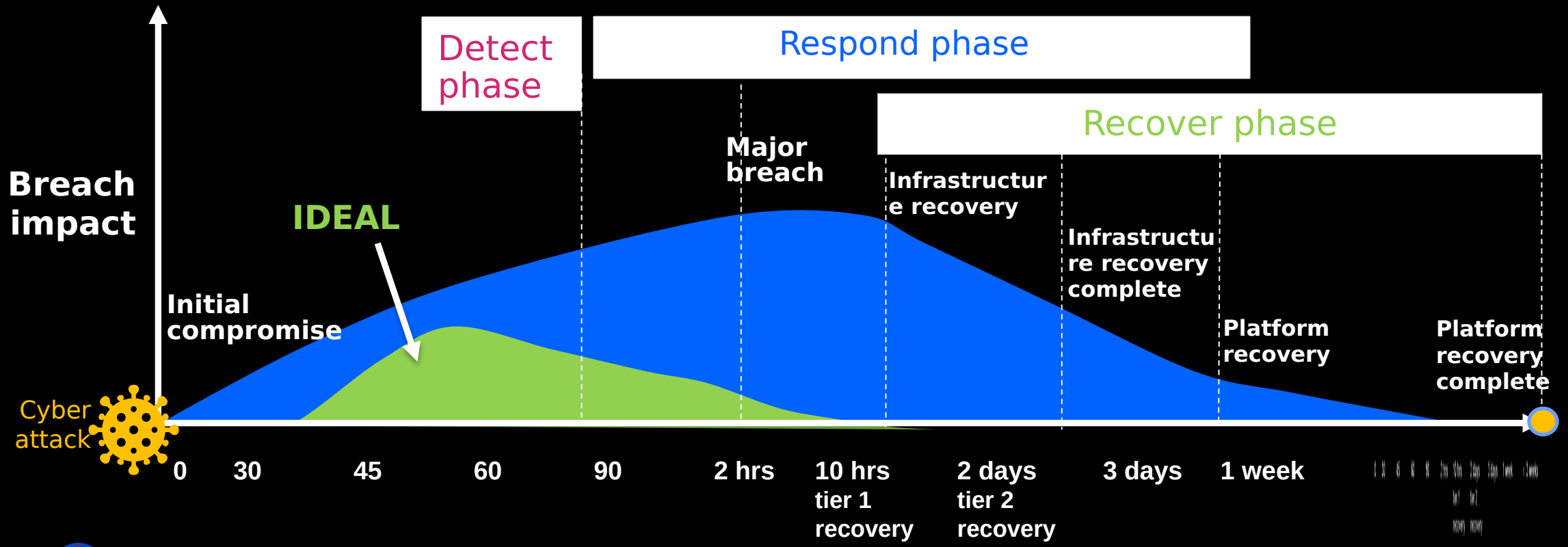
PREDATAR

„Alle wollen wiederherstellen, aber keiner will sichern.“

Ablauf eines Cyber-Angriffes



Chronologie eines Cyber Angriffs:



1. Datenkorruption- bleibt unentdeckt
2. Virus verbreitet sich weiter –Beginn Gegenmassnahmen
3. Recovery Prozess beginnt

Recovery Zeit > Tage oder Wochen, im Durchschnitt 23 Tage

Fertige Lösung für eine schnelle, komplette Wiederherstellung mit “sauberen” Daten

Analytics

Analyse und Benachrichtigungen für eine 100%ige Erfolgsrate bei der Erstellung Ihrer Backups

Orchestration

Automatisierte Wiederherstellungstests und orchestrierte Malware-Scans, um sicherzustellen, dass Ihre Daten schnell, sauber und vollständig wiederhergestellt werden können.

Die CHALLENGE

Ich **denke** ich **kann** alle meine Daten wiederherstellen

Ich bin mir **nicht sicher**, ob ich alle meine Daten wiederherstellen kann

Die Realität

<1%

Der Unternehmen testen jährlich ihre Backups auf Wiederherstellbarkeit

Global Storage Protect usage monitored by Predatar

21%

Wachstum an unentdeckten Ransomware in den letzten 12 Monaten

IBM Cyber Study (2025)

4 von 14

Backups sind im Restore fehlgeschlagen, als sie benötigt wurden

Global Storage Protect usage monitored by Predatar

Die 2 Optionen

REACTIVE

Entdecken von **Backupfehlern** im Desasterfall

PROACTIVE

Kontinuierliche Tests zur Sicherstellung der **Wiederherstellbarkeit** aller Daten

PLATTFORM-INTEGRATIONEN

Predatar lässt sich in viele führende Plattformen integrieren und baut seine Integrationen kontinuierlich aus.

Backup & Speicherung

IBM FLASHSYSTEMS DATA PROTECT STORAGE PROTECT+ STORAGE PROTECT Defender

COHESITY

veeAM

rubrik

PURESTORAGE

Zerto a Hewlett Packard Enterprise company

NOVASTOR

Sicherheit

TREND MICRO

Bitdefender

ClamAV

Microsoft Sentinel

QRadar

Hypervisor

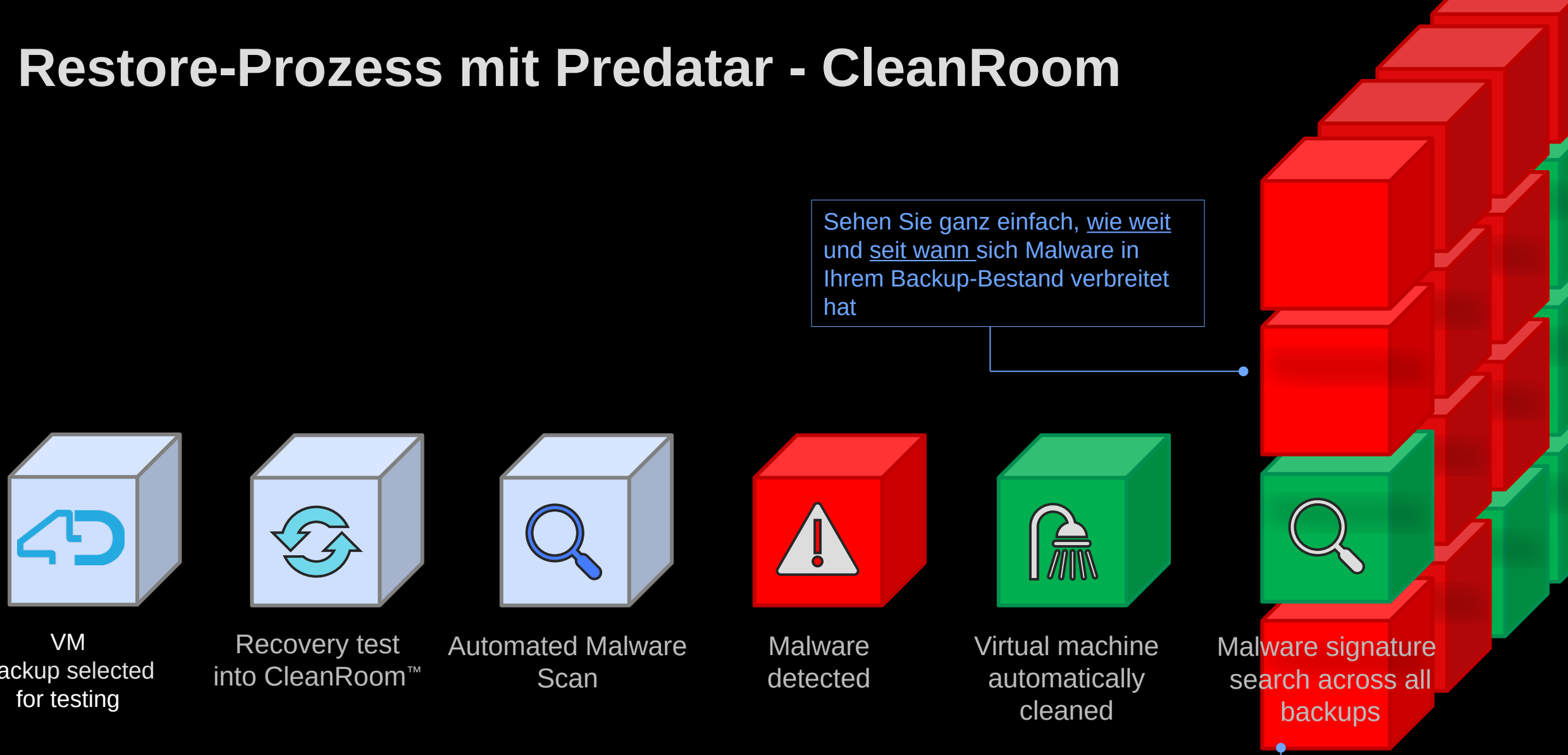
vmware

Microsoft Hyper-V

PROXMOX

In Planung 2026

Restore-Prozess mit Predatar - CleanRoom



Sehen Sie ganz einfach, wie weit und seit wann sich Malware in Ihrem Backup-Bestand verbreitet hat

VM
Backup selected for testing

Recovery test into CleanRoom™

Automated Malware Scan

Malware detected

Virtual machine automatically cleaned

Malware signature search across all backups

Verschieben Sie alle infizierten Nodes schnell in den CleanRoom™, um sie automatisch zu scannen und von Maleware zu reinigen

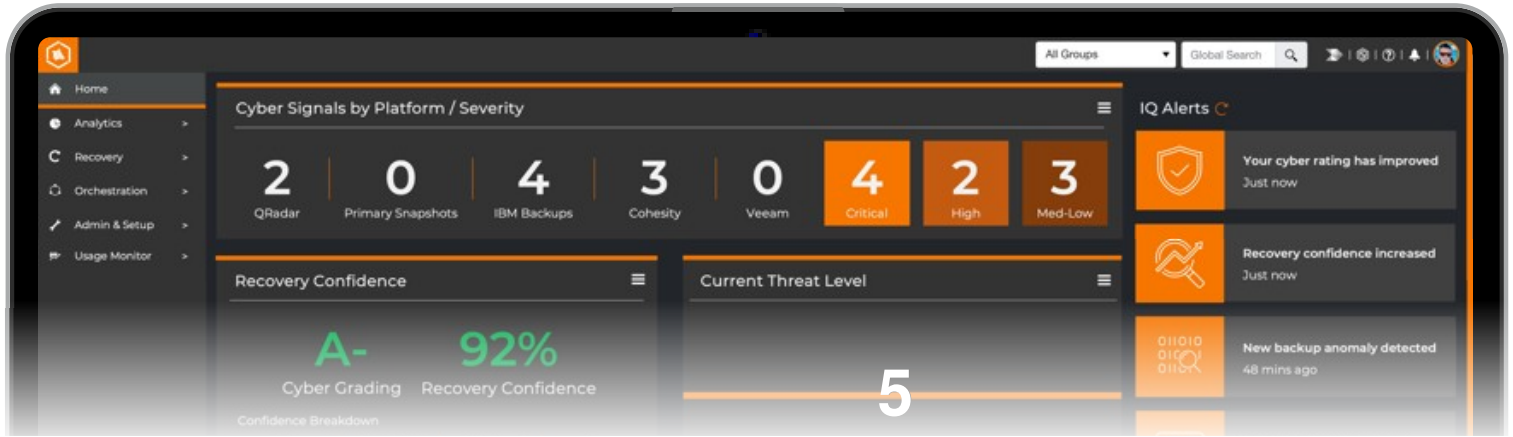
* Node ist selektiertes Backup einer VM oder VM-Gruppe

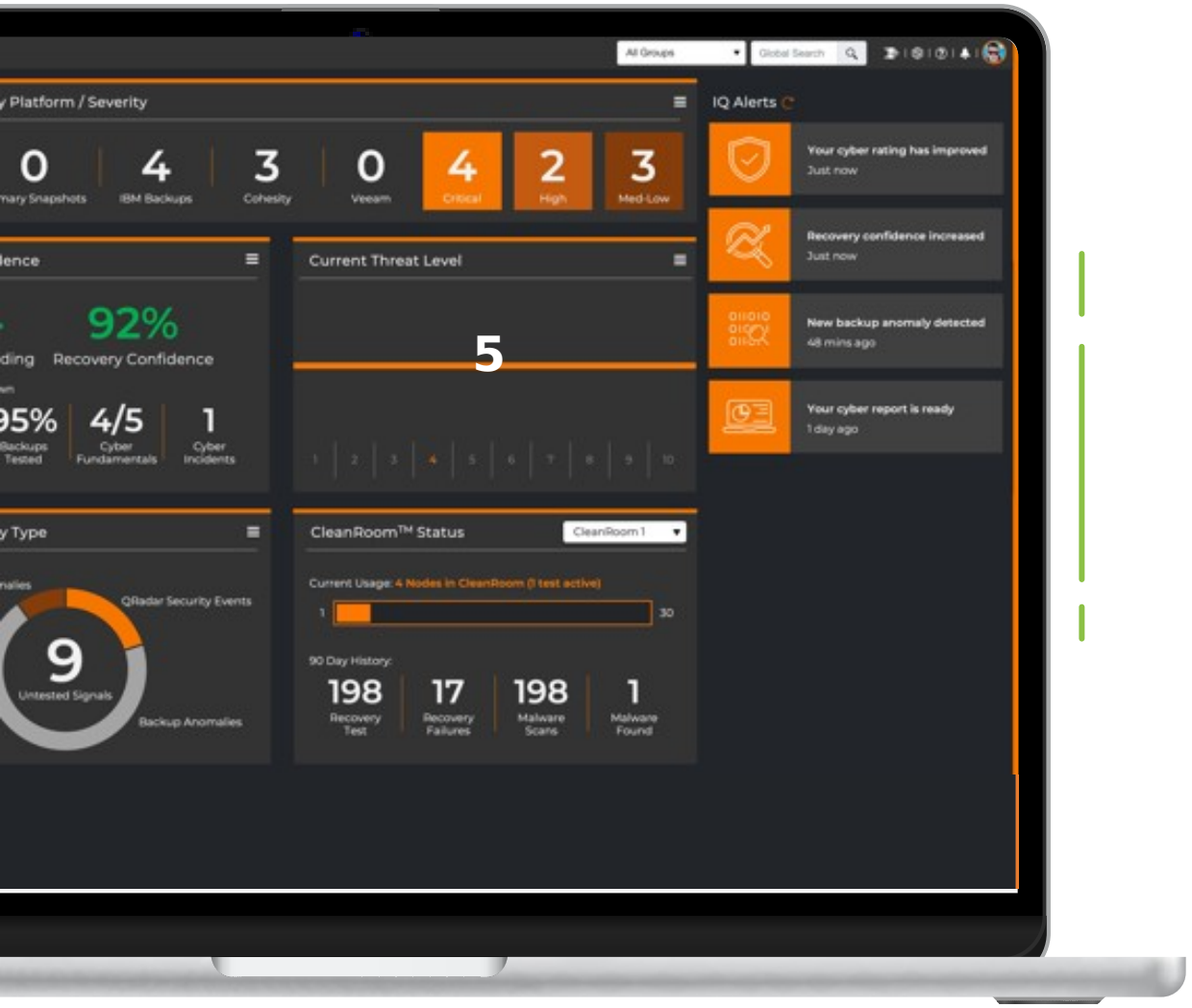
ZUSAMMENFASSUNG

Warten Sie nicht auf eine Krise, um Ihre Wiederherstellungsfähigkeit auf die Probe zu stellen.

Finden Sie die Gefahrensignale in Ihren Daten und nutzen Sie sie zu Ihrem Vorteil.

Optimieren Sie Ihre Wiederherstellungssicherheit mit der Predatar-Plattform und CleanRoom™




All Groups
Global Search
Platform / Severity
0
4
3
0
4
2
3
IBM Backups
Cohesity
Veeam
Critical
High
Med-Low
IQ Alerts
Your cyber rating has improved
Just now
Recovery confidence increased
Just now
New backup anomaly detected
48 mins ago
Your cyber report is ready
1 day ago
92%
Recovery Confidence
4/5
Cyber Fundamentals
1
Cyber Incidents
Current Threat Level
5
CleanRoom™ Status
CleanRoom 1
Current Usage: 4 Nodes in CleanRoom (1 test active)
1
30
90 Day History:
198
Recovery Test
17
Recovery Failures
198
Malware Scans
1
Malware Found
QRadar Security Events
9
Untested Signals
Backup Anomalies

Danke

Link zu unserer Erfolgsstory

Erfolgreich Ransomware Rückstände gefunden

https://predatar.com/2025/08/13/hidden-for-a-decade-uncovered-in-6-days/

Link zur Live Demo

LiveDemo

https://us.predatar.com/

User: preddemo2

PW: N0mad01!