

next level

# 21. anwendertreffen

Mi  
04.12.24



Angreifer



# GAME OVER



Server

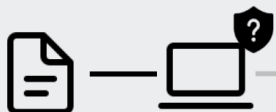


Reconnaissance

Weaponization

Command & Control

Actions on Objective



Unmanaged

POST-BREACH



# BETTER LUCK NEXT TIME?

NEXT TRY - BETTER LUCK?

Angreifer



Server



Reconnaissance

Weaponization

Command & Control

Actions on Objective



Unmanaged

POST-BREACH



BETTER LUCK NEXT TIME?

Technologie



Assets ?

Patches ?

Personal ?

KnowHow ?

## Initialer Einfallsvektor

- 50 % durch kompromittierte Zugangsdaten
  - › z.B. VPN Zugriff oder RDP mit Single Factor Authentication
  - › Multi-Factor Authentication (MFA) war in 39% der erfolgreichen Angriffe nicht aktiv
- 23 % durch Ausnutzung von Schwachstellen
  - › Sorgfältiges und schnelles Patchen ist und bleibt extrem wichtig

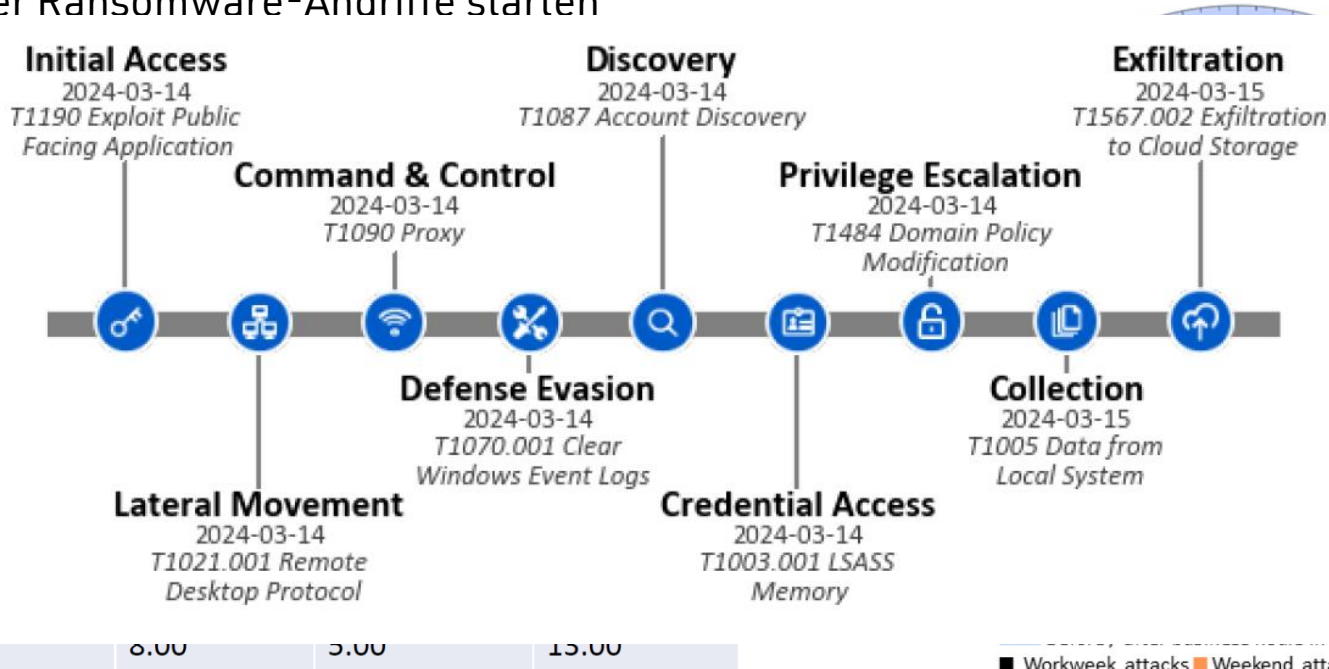
**Angreifer brechen nicht mehr ein,  
sie loggen sich ein!**

## Living off the Land – Nutzung vorhandener Tools

Angreifer passen sich Ihrer Infrastruktur an und nutzen hierbei existierende Dienste und Werkzeuge, die auch durch Ihre eigene IT verwendet werden.

- Sie loggen sich mit **Ihren eigenen Konten** ein.
- Sie nutzen **Systembefehle** für Benutzerverwaltung sowie das Auslesen von Arbeitsspeicher und Datenbanken.
- Sie schalten sich auf andere Systeme weiter, **genau wie Ihre eigene IT**.
- Wenn notwendig laden **sie legitime Werkzeuge** nach.
  - › Für Analyse, Datenexfiltration, Verschlüsselung und Fernsteuerung
- **Malware-Executables werden vermieden soweit möglich!**

- 91% der Ransomware-Angriffe starten außerhalb der Business Hours
- Ransomware-Angriffe dauern durchschnittlich 5 Tage durch

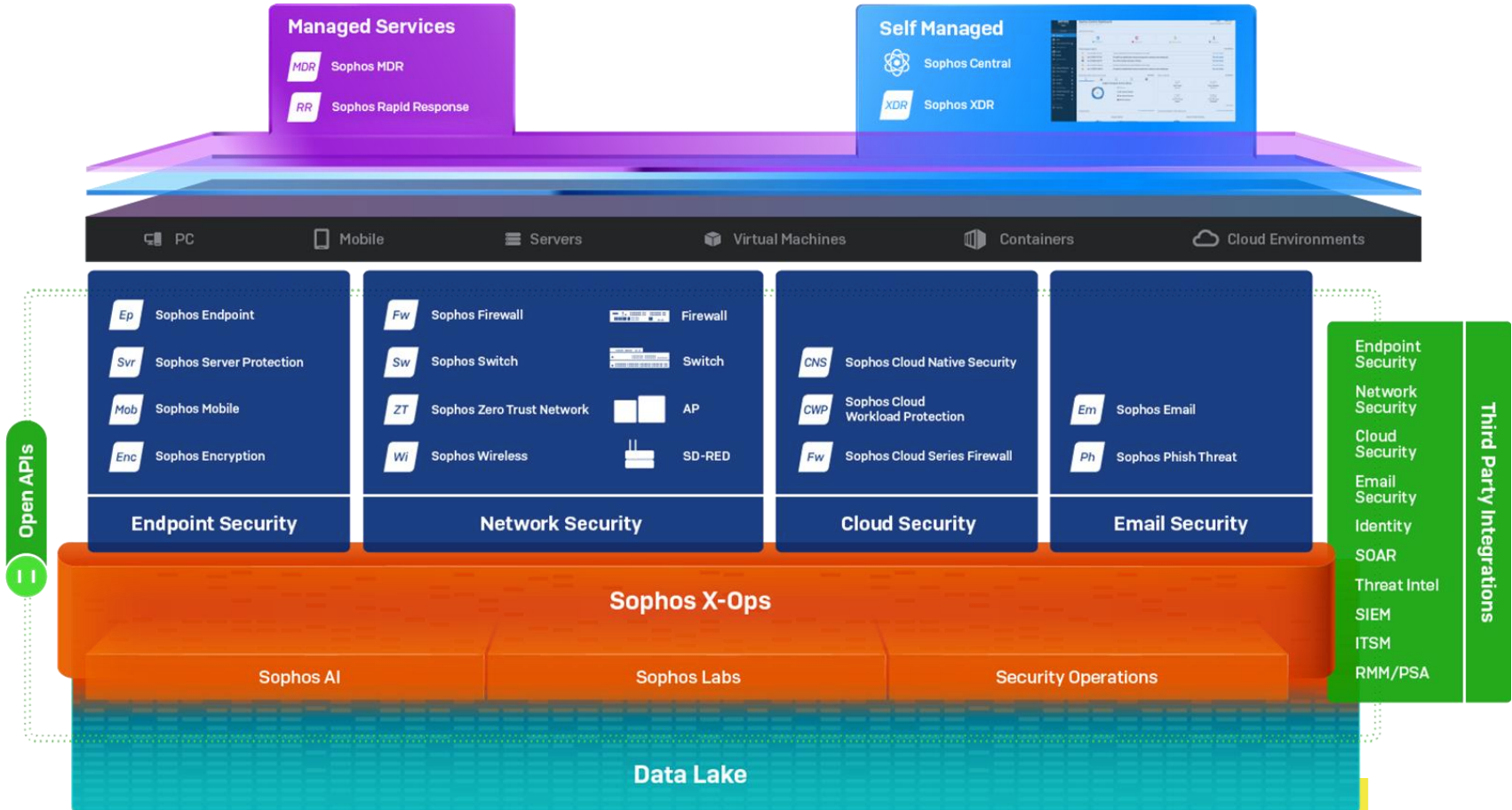


Verweildauer
Minimum
Maximum
Durchschnitt
Median

0.00	5.00	15.00
------	------	-------



# NEXT TRY – NEW POWERUPS



## 24/7 Überwachung, Untersuchung, und Response durch ein Expertenteam geliefert.



Ermöglicht durch extended detection and response (XDR) Fähigkeiten, die eine vollständige Sicherheitsabdeckung liefern.



Proaktives Threat Hunting, das durch hochtrainierte Analysten durchgeführt wird.



Analysten reagieren innerhalb von Minuten auf Bedrohungen, egal, ob ein umfassendes Incident Response oder Unterstützung bei der Entscheidungsfindung benötigt wird.



Ursachenanalyse von Bedrohungen und Empfehlungen zur Vermeidung künftiger Vorfälle zur Verringerung des Risikos.

# NEXT TRY - NEW POWERUPS AND FRIENDS



## SOPHOS

✓ Integrations included

Ep

Endpoint

WP

Workload

Mob

Mobile

Cld

Cloud

Fw

Firewall

Em

Email

ZT

ZTNA

NDR

Network

### Endpoint

✓ Included

Microsoft CROWDSTRIKE

SentinelOne TREND MICRO

Symantec by Broadcom BlackBerry CYLANCE

+ Others with Sophos XDR sensor agent

### Firewall

Barracuda

paloalto FORTINET

CHECK POINT CISCO Meraki

Forcepoint

SONICWALL WatchGuard

### Network

DARKTRACE

TRUST CANARY CISCO Umbrella

Skyhigh Security Securtec

VECTRA

zscaler

### Email

Microsoft 365  
✓ Included

Google Workspace  
✓ Included

mimecast

proofpoint

### Productivity

✓ Included

Microsoft 365

Google Workspace

### Cloud

orca security

+ AWS, Azure, and GCP integrations with Sophos Cloud Optix product

aws A Cloud

### Identity

Microsoft  
✓ Included

okta auth0

CISCO Duo CISCO ISE

ManageEngine

### Backup and Recovery

veeam

Acronis

# NEXT TRY - NEW POWERUPS INSIDES



## Event Sources

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identity
- Network

## Threat Analysis and Correlation

### Sophos XDR Data Lake

Collect → Contextualize → Correlate

Threat Intelligence + Automated Response + Advanced Threat Analytics

## Investigation and Response

### 24/7 Managed Detection and Response Services

Sophos MDR experts hunt, investigate, and eliminate attackers on your behalf

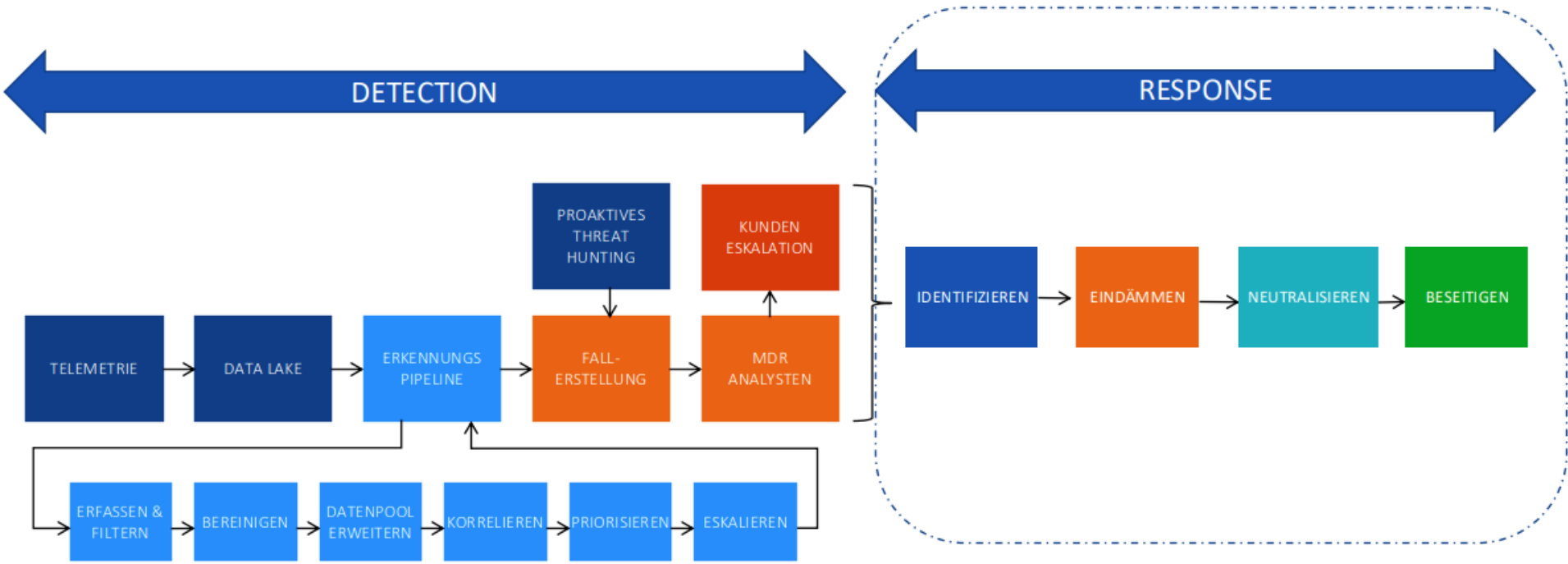
**38** Mean Time to Remediate  
mins



### Investigation and Response Platform

Sophos Central is your single platform for investigation, reporting, and management

Self-manage or collaborate with the Sophos MDR team



## Sophos X-Ops Powers MDR with Leading Threat Intelligence

### Security Professionals

Sophos team sharing queries, tools, and techniques from CISO to frontline



### MDR SecOps Analysts

Discovering new IOCs and hunting methods, in-the-wild impact



## Sophos X-Ops

500+ experts across threat intel, analysis, data engineering, data science, threat hunting, adversary tracking, and incident response, staffing 6 global SOCs in every major theater

### SophosLabs Researchers

Providing deep analysis of files, email, behaviors, URLs, IOCs, and DPI



### Sophos AI Data Scientists

Development and insights on advanced ML models, automation and detection for MDR and Sophos products



## Sophos MDR Servicestufen

Sophos MDR für  
Microsoft Defender

Sophos MDR  
Essentials

24/7 Überwachung, Bedrohungserkennung und Reaktion durch Experten	✓
Kompatibel mit Security-Werkzeugen anderer Hersteller	✓
Wöchentliches und monatliches Reporting	✓
Monatliches Briefing "Sophos MDR ThreatCast" zu aktuellen Bedrohungen	✓
Sophos Account Health Check – ist Sophos XDR richtig konfiguriert?	✓
Proaktive Bedrohungssuche durch Experten	✓
Stoppen und Eindämmen von Bedrohungen <small>Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung, Reaktion) oder Sophos XDR Sensor (Erkennung, Reaktion)</small>	✓
Direkter Telefon-Support bei Vorfällen	✓
Ursachenanalyse – und wie können erneute Angriffe verhindert werden?	
Vollständiges Incident-Response: komplette Neutralisierung von Bedrohungen <small>Voraussetzung: voller Sophos XDR Agent (Schutz, Erkennung und Reaktion)</small>	
Dedizierter Ansprechpartner beim Incident Response Team	
Sophos Breach Protection Warranty	

### Sophos MDR Essentials – Threat Response

#### Example Response Actions:

- Isolate host(s) utilizing Sophos Central
- Apply host-based firewall IP blocks
- Terminate processes
- Force log off user sessions
- Disable user accounts
- Remove malicious artifacts
- Add malicious hash to blocked items in Sophos Central

### Sophos MDR Complete – Full Incident Response

#### Example Response Actions:

##### All MDR Essentials Response plus:

- Dedicated incident response lead and process management
- Root cause analysis to identify initial access
- Identification of compromised assets with remediation support
- Malware triage and analysis with SophosLabs
- Review of all relevant logs to assist with response and remediation

THE NEXT LEVEL

Lmbit <>



**Herzlichen Dank !**

Timo Peters  
Solution Architect

+49 431 6703-142  
Timo.Peters@lmbit.de