SOPHOS

Sophos EDR und XDR: Anwendungsfälle

Erhältlich mit Intercept X Advanced with EDR, Intercept X Advanced with XDR, Intercept X Advanced for Server with EDR und Intercept X Advanced for Server with XDR

Beantworten Sie geschäftskritische IT-Operations- und Threat-Hunting-Fragen und ergreifen Sie bei Bedarf erforderliche Maßnahmen. Sowohl IT-Administratoren als auch Cybersecurity-Analysten profitieren von diesen leistungsstarken Funktionen.

Erledigen Sie IT-Security-Operations- und Threat-Hunting-Aufgaben:

- Wählen Sie aus vorformulierten, anpassbaren SQL-Abfragen
- Ergreifen Sie schnell Maßnahmen, sobald Ihnen die nötigen Informationen vorliegen
- Einsetzbar für Endpoints, Server, Firewalls, E-Mails, Cloud Hosts etc.

Sophos XDR

Anwendungsfälle: IT Operations

Sorgen Sie in IT Operations für eine erstklassige Einhaltung von Sicherheitsvorgaben. Einige Beispiele:

Geräte-Healthchecks

Erkennen Sie Geräte mit Performance-Problemen, greifen Sie remote auf diese zu und ergreifen Sie die erforderlichen Maßnahmen.

- Nach Geräten mit geringem Festplattenspeicher, hoher Speicher-/CPU-Auslastung oder ausstehendem Neustart suchen
- Remote auf Geräte zugreifen, um freien Festplattenspeicher zu schaffen, die Ursache einer hohen Auslastung zu finden und bei Bedarf einen Neustart vorzunehmen

Schwachstellen

Finden Sie Geräte mit Problemen oder Schwachstellen, die von Malware und Angreifern ausgenutzt werden könnten.

- Geräte mit Software-Schwachstellen, unbekannten Diensten oder nicht autorisierten Browser-Erweiterungen finden und gemeinsam oder unbefugt genutzte Anmeldeinformationen für Konten erkennen
- Remote auf Geräte zugreifen, um Patches zu installieren, unbekannte Dienste zu untersuchen und zu beenden, Browser-Erweiterungen zu deinstallieren und Anmeldeinformationen für Cloud-Konten zu aktualisieren

Unerwünschte Software

Finden Sie Software, die Probleme bei der Compliance oder der Produktivität verursachen kann.

- Unerwünschte Programme wie Spotify, Steam und Bittorrent finden
- Remote auf Geräte zugreifen und die Software deinstallieren

Konfigurations-Probleme

Finden Sie Geräte und Cloud Workloads mit Konfigurations-Problemen, die ein Sicherheitsrisiko darstellen könnten.

- Server mit aktiviertem RDP und SSH und Cloud-Sicherheitsgruppen mit offenen Netzwerk-Ports ermitteln sowie Public Cloud Hosts, Container etc. überwachen und inventarisieren
- Remote auf die Server zugreifen, RDP/SSH deaktivieren und überprüfen, ob Server die offenen Ports abhören

Compliance

Erkennen und beheben Sie Compliance-Probleme lokal und in der Cloud.

- Sensible Dateien finden und Konfigurationen für AWS-, Azure- und GCP-Umgebungen bewerten
- Remote auf Geräte zugreifen, um sensible Dateien zu löschen, und sichere Cloud-Konfigurationen gemäß CIS Benchmarks sicherstellen

Projekt-Rollouts

Prüfen Sie, ob IT-Projekte auf allen Geräten implementiert wurden.

- Überprüfen, ob Software auf Geräten bereitgestellt wurde, z. B. um den Fortschritt eines Rollouts zu messen
- Remote auf Geräte zugreifen, um eine erfolgreiche Bereitstellung zu gewährleisten und ggf. einen Neustart durchzuführen, um erforderliche Änderungen vorzunehmen

Probleme mit dem Büronetzwerk (erfordert XDR)

Erkennen und beheben Sie Netzwerkprobleme an allen Bürostandorten.

- Nachvollziehen, warum in einem Büro Netzwerkprobleme auftreten, die zu Performance-Einbußen führen
- Ermitteln, welche Anwendung das Problem verursacht

Geräteverwaltung (erfordert XDR)

Identifizieren und verstehen Sie die Geräte in der IT-Umgebung Ihres Unternehmens.

- Nicht verwaltete und ungeschützte Geräte wie Laptops, Mobiltelefone und IoT-Geräte erkennen
- Besseren Überblick über ältere oder nicht verwaltbare Geräte wie medizinische Spezialgeräte erhalten

Vorbereitung auf Unerwartetes (erfordert XDR)

Mit 30 Tagen Cloud-Speicher sind Sie auch auf unerwartete Ereignisse vorbereitet.

- Auf verloren gegangenen Geräten Verlaufsdaten von 30 Tagen auf ungewöhnliche Aktivitäten prüfen
- Nachvollziehen, was mit einem Gerät passiert ist – selbst wenn die Festplatte gelöscht oder das Gerät zerstört wurde

Anwendungsfälle: Threat Hunting

Spüren Sie evasive, subtile Bedrohungen auf und beseitigen Sie diese schnell. Einige Beispiele:

Netzwerkangriffe

Erkennen Sie Prozesse, die ungewöhnliche Zugriffsversuche auf das Netzwerk unternehmen.

- Prozesse erkennen, die versuchen, eine Verbindung über Nicht-Standardports herzustellen, oder ungewöhnlichen ausgehenden Datenverkehr von einem Cloud Workload erkennen
- Cloud-Sicherheitsgruppen analysieren, um Ressourcen zu erkennen, die über das öffentliche Internet zugänglich sind
- Remote auf das Gerät/den Workload zugreifen, den Prozess beenden und nach lateralen Bewegungen suchen

Geänderte Dateien

Suchen Sie nach Elementen, die auf unerwartete Weise geändert wurden.

- Prozesse identifizieren, die kürzlich Dateien oder Registry-Schlüssel geändert haben
- Remote auf das Gerät zugreifen, die Änderungen untersuchen und Maßnahmen ergreifen

Verschleierte Skripts

Dateilose, speicherbasierte Angriffe werden häufig als Angriffsvektor genutzt.

- Details zu unerwarteten PowerShell-Ausführungen genauer unter die Lupe nehmen
- Remote auf das Gerät zugreifen, zusätzliche forensische Tools ausführen und verdächtige Prozesse beenden

Getarnte Prozesse

Manche schädliche Prozesse tarnen sich, um unerkannt zu bleiben.

- Prozesse erkennen, die sich tarnen
- Remote auf das Gerät zugreifen, verdächtige Prozesse beenden und forensische Tools ausführen

MITRE ATT&CK Framework

Das MITRE ATT&CK Framework ist eine häufig verwendete Vorlage zum Identifizieren von Angriffstechniken.

- Mit Ihren eigenen oder Sophos-Abfragen Angriffstaktiken und Techniken von Angreifern identifizieren
- Basierend auf der identifizierten Technik gezielt mögliche Folgeangriffe untersuchen oder bestimmte Bereiche genauer überprüfen

Umfang eines Vorfalls

Verstehen Sie die Auswirkungen eines Vorfalls und welche Geräte und Benutzer betroffen waren.

- Geräte erkennen, von denen aus auf Links in Phishing-E-Mails geklickt wurde
- Sehen, welche Geräte Dateien von der Phishing-Website heruntergeladen haben, remote auf diese zugreifen und sie bereinigen

Analysezeiträume verlängern (erfordert XDR)

Nutzen Sie neben 90-tägiger Datenspeicherung auf dem Gerät 30 Tage Cloud-Daten.

- Daten von 30 Tagen analysieren, ohne dass das betroffene Gerät wieder online gehen muss
- Nachvollziehen, was mit Geräten passiert ist, die bei einem Angriff außer Betrieb gesetzt wurden

Umfangreiche Netzwerkdaten nutzen (erfordert XDR)

Integrieren Sie Netzwerkdaten in Ihre Threat-Hunting- und Analyse-Aktivitäten.

- Bezüge zwischen blockiertem Schadverkehr und anderen IoCs herstellen, um das Ausmaß eines Angriffs zu bestimmen
- ATP- und IPS-Erkennungen der Sophos Firewall zur Analyse verdächtiger Hosts und Geräte nutzen

Umfangreiche E-Mail-Daten nutzen (erfordert XDR)

Integrieren Sie E-Mail-Informationen, um mehr Transparenz über Ihre Umgebung zu erhalten.

- E-Mail-Header-Informationen mit anderen IoCs vergleichen, um einen Vorfall besser zu verstehen
- Verdächtige Dateien identifizieren und diese schnell von Geräten und aus O365-Mailboxen löschen

Weitere Informationen über Sophos EDR, XDR und die leistungsstarken Schutzfunktionen in Intercept X finden Sie unter www.sophos.de.

21-03-26 UC-DE (MP)

SOPHOS