SOPHOS

SOPHOS EDR: ANWENDUNGSFÄLLE

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

Sophos EDR dient IT-Administratoren und Sicherheitsanalysten zum Lösen von Anwendungsfällen bei IT Security Operations und Threat Hunting. Sie können damit Probleme schnell erkennen und entsprechende Maßnahmen ergreifen.

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, Cloud Hosts, Container, Sicherheitsgruppen etc.

Im Folgenden finden Sie einige der häufigsten Anwendungsfälle für die leistungsstarke EDR-Funktionalität.

Anwendungsfälle: IT Operations

Mit Sophos EDR sorgen Sie für eine erstklassige Einhaltung von Sicherheitsvorgaben. Hier einige Beispiele für Aufgaben, die Sie schneller erledigen können:

Geräte-Healthchecks

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

- Nach Geräten mit geringem Festplattenspeicher, hoher Speicher-/CPU-Auslastung oder ausstehendem Neustart suchen
- Remote auf Geräte zugreifen, um freien Festplattenspeicher zu schaffen, der Ursache hoher Auslastung auf den Grund zu gehen und bei Bedarf einen Neustart vorzunehmen

Sicherheitslücken

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

- Geräte mit Software-Schwachstellen, unbekannten Diensten oder nicht autorisierten Browser-Erweiterungen finden und gemeinsam oder unbefugt genutzte Anmeldeinformationen für Cloud-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. Sie können:

- 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. Sie können:

- 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. Sie können:

- Sensible Dateien (z. B. Finanzdaten) 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 Ihren Geräten implementiert wurden. Sie können:

- 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

Anwendungsfälle: Threat Hunting

Mit Sophos EDR erhalten Sie die nötigen Tools, um evasive, subtile Bedrohungen aufzuspüren und schnell zu beseitigen. Hier einige Beispiele für Kompromittierungs-Indikatoren, nach denen Sie suchen können:

Netzwerkangriffe

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

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

Geänderte Dateien

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

- Finden Sie Prozesse, die kürzlich Dateien oder Registry-Schlüssel geändert haben
- Greifen Sie remote auf das Gerät zu, überprüfen Sie die Änderungen und ergreifen Sie erforderliche Maßnahmen

Verschleierte Skripts

Dateilose, speicherbasierte Angriffe werden immer häufiger als Angriffsvektor genutzt. Sie können:

- 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. Beispiele:

- Erkennen Sie Prozesse, die sich als „services.exe“ tarnen
- Greifen Sie remote auf das Gerät zu, beenden Sie den verdächtigen Prozess und führen Sie forensische Tools aus

MITRE ATT&CK Framework

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

- Ihre eigenen oder in Sophos integrierte Abfragen nutzen, um potenzielle Angriffe zu erkennen, bei denen Angreifer gängige Taktiken und Techniken nutzen
- Basierend auf der Angriffstechnik 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. Sie können:

- 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

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

20-07-15 UC-DE (PS)

SOPHOS