LÖSUNGSFLYER

SIEM-Lösungen für den Mittelstand

Security Information and Event Management as a Service

Starke Kennwortrichtlinien, Firewalls, Virenscanner und ausgeklügelte Rechtekonzepte sind altbewährte Abwehrmechanismen, mit denen sich Unternehmen vor Cyberattacken schützen. Diese Mechanismen sind in Anbetracht der ausgeklügelten Angriffsszenarien heutzutage jedoch keinesfalls mehr ausreichend. Die zunehmende Anzahl an Meldungen über erfolgreiche Cyberangriffe in den Nachrichten ist schockierend. Betroffene beklagen hohe Schäden – sei es durch lange Ausfallzeiten, Datenverschlüsselung oder Lösegeldforderungen. Doch wie ist das möglich?

Die Erklärung ist relativ simpel: Cyberkriminelle wenden Methoden an, die von den oben genannten Sicherheitslösungen nicht erkannt werden. So entwickelte sich beispielsweise die Windows PowerShell zum bevorzugten Werkzeug für Cyberkriminelle, nicht zuletzt deshalb, weil sie ebenso gerne von der internen IT eingesetzt wird. In der Folge haben Verantwortliche in den IT-Sicherheitsabteilungen keinen Einblick mehr darauf, was auf den Clients und Servern im Unternehmen passiert – und können deshalb auch nicht gezielt auf Angriffe reagieren.

Lösungen bieten Security Systeme, wie z. B. Detection & Response oder sogenannte Security Information und Event Management Systeme (kurz SIEM). Das SIEM registriert alle Ereignisse und schlägt bei Angriffen Alarm. Die Auswertung erfolgt dabei in Echtzeit, auch bei Ereignissen, die weder der Virenscanner noch die Firewall erkennen würden.

Der „Managed Service" der Makro Factory bietet als besonderen Mehrwert, dass zusätzlich zu den effizienten Filtereinstellungen für die aktuell gängigen Bedrohungen unklare Events, durch geschulte Forensiker, analysiert und bewertet werden.

Wird eine Aktivität als Gefahr erkannt, wird das IT-Sicherheitspersonal sofort über das verdächtige Geschehen informiert und kann im Falle eines Angriffs schnell auf die Bedrohung reagieren. Auf Wunsch und in Absprache mit dem Kunden kann der Service auch automatisch reagieren und beispielsweise betroffene Geräte außer Betrieb nehmen. Es ist zu empfehlen, diese Systeme als gemanagte Lösungen zu betreiben, da unzureichendes Know-how oder Personalmangel in den IT-Abteilungen den effizienten, zielführenden Einsatz oftmals unmöglich und immer kostenintensiv macht.

SIEM AS A SERVICE FÜR KLEINE UND MITTELSTÄNDISCHE UNTERNEHMEN

In Zusammenarbeit mit der CyberSec24 GmbH bietet die Makro Factory drei SIEM-Lösungen als Managed Service für Interessenten ab 50 Endgeräte an. Die Einstiegslösung SIEM ONE ESSENTIALS PROTECT STANDARD ist bereits ab 6 Euro/Monat je überwachtes Endgerät erhältlich. Wir freuen uns auf Ihre unverbindliche Anfrage.

makrofactory
strategies for a virtual world

Makro Factory GmbH & Co. KG / An der RaumFabrik 30 / 76227 Karlsruhe / Tel +49 721 97 003 100 / info@makrofactory.com / www.makrofactory.com

FRAGEN & ANTWORTEN ZU SIEM AS A SERVICE

Für welche Unternehmensgrößen wird eine SIEM-Lösung empfohlen?

Aus IT-Security-Sicht sollte grundsätzlich jedes Gerät (unabhängig der Unternehmensgröße) überwacht werden, da Angreifer das Unternehmen nicht nur erpressen, sondern auch als Wirt für weitere Attacken gegen die eigenen Kunden einsetzen.
Der Einsatz einer SIEM-Lösung zur Überwachung wird aufgrund der Wirtschaftlichkeit ab 50 Geräte empfohlen. Auf expliziten Wunsch kann die SIEM-Lösung der Makro Factory jedoch auch bei einer kleineren Endgerätezahl implementiert werden.
Kunden mit mehr als 2.000 Endgeräten erhalten individuelle Angebote.

Welche Voraussetzungen sind nötig, um einen SIEM-Service nutzen zu können?

Um SIEM Essential, SIEM One bzw. SIEM 100 nutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- **Virenscanner von ESET**
  Auf jedem System muss ein Virenscanner von ESET installiert sein, damit die Daten entsprechend eingesammelt und ausgewertet werden können.

- **ESET Security Management Center (kurz ESMC)**
  Der SIEM-Service muss über die ESET Management Konsole angebunden sein. Wir bieten unseren Kunden ESET Endpoint Security als separaten Managed Service an. Dies garantiert nicht nur die korrekte Anbindung des SIEM-Services, sondern entlastet darüber hinaus die IT-Abteilung sehr effektiv.

Selbstverständlich können Administratoren dabei Zugriff auf das ESMC bekommen, um weiterhin wie gewohnt mit dem System zu arbeiten. Die eigene Verwaltung des ESMC ist ebenfalls möglich, allerdings kann Ihnen in diesem Fall eine 100%ige Funktion des SIEM-Services nicht garantiert werden.

Wo und wie lange werden die gesammelten Daten gespeichert?

Die gesammelten Daten werden in einem ISO 27001-zertifizierten Rechenzentrum der CyberSec24 GmbH in Frankfurt am Main, Deutschland gelagert. Sämtliche Systeme sind mit einer 2-Faktor-Authentifizierung gegen unbefugten Zugriff abgesichert.
Standardmäßig werden die Daten **7 Tage** lang gespeichert.
Auf individuellen Wunsch kann die Speicherdauer gegen einen geringen Aufpreis auf **14 Tage oder 30 Tage** angehoben werden.

Was kostet der SIEM-Service?

Die Kosten für den SIEM-Service staffeln sich nach Anzahl der Clients. Beginnend bei 6 €/Endgerät pro Monat für SIEM One Essentials Protect Standard, entwickelt sich der Preis mit dem Schutzbedarf des Interessenten.

Fragen Sie nach Ihrem persönlichen Angebot.

Sie benötigen weitere Informationen oder eine ausführliche Beratung? Sprechen Sie uns gerne an!

Ihr Vertriebsteam der Makro Factory

+49 721 97 003 861
sales@makrofactory.com

Unsere SIEM-Pakete im Vergleich

PAKETINHALTE	SIEM ONE ESSENTIALS PROTECT STANDARD	SIEM ONE	SIEM 100
Automatisierte Berichte nach vereinbarten Intervallen	✔	✔	✔
Prüfung der SIEM-Meldungen, Ereignisse (Skripte, Executables & Detections) durch CyberSec24 IT-Security Spezialisten	monatlich	täglich	täglich
Durchsprache der SIEM-Meldungen | Dauer: 1 Stunde	monatlich	wöchentlich	wöchentlich
Aufbewahrungszeit der Raw-Events (Datastore) | Dauer: 1 Woche	✔	✔	✔
Konzeptionelle Betreuung und Besprechung, Fragen (außerhalb des 60 Minuten-Slots)	nicht verfügbar	✔	✔
Einsatz im medizinischen Umfeld		✔	✔
Detection und automatisierte Response hinsichtlich der Top 100 Bedrohungen & Angriffsszenarien			✔
Monatliche Aktualisierung der Angriffsliste auf den aktuellen Stand der weltweiten Angriffsszenarien			✔
Automatisierter Bot-Net-Schutz (voraussichtlich ab Ende 2022)	monatlich	wöchentlich	wöchentlich
Empfehlungen zum weiteren Umgang mit aufgetretenen Bedrohungen auf den Endgeräten			✔
Wissenstransfer und Sensibilisierung zu IT-Security Themen	✔	✔	✔

Einmalige Einrichtungspauschale zur Konfiguration | entfällt bei Laufzeiten ab 3 Jahren

Grundvoraussetzung zum Betrieb: Jedes zu überwachende Endgerät benötigt eine ESET PROTECT Essentials bzw. ESET PROTECT Advanced Installation, die auf Wunsch als Service (Add-On) gebucht werden kann. Der Betrieb von ESET durch den Kunden ist auf eigenes Risiko möglich.

ADD-ON			
ESET PROTECT Essentials bzw. ESET PROTECT Advanced as a Service Abrechnung nach Endgerätestaffel pro Gerät und Monat	✔	✔	✔
Beratung bei der Umsetzung neuer IT-Projekte, im eigenen Hause (Assessments, Pentests, Netzwerkanalyse | Berechnung nach Aufwand	✔	✔	✔
Verlängerung der Aufbewahrungszeit der Raw-Events (Datastore) pro zusätzliche Woche, 1 Euro / Endgerät und Monat	✔	✔	✔
Auf Wunsch kundenspezifische Schulung und Fortbildung für IT und non-IT Mitarbeiter Angebot anfordern	✔	✔	✔
SIEM WEEKEND – tägliche Prüfung auch an Wochenenden und Feiertagen Abrechnung nach Endgerätestaffel pro Gerät und Monat.	nicht verfügbar	✔	✔

ADD-ON ZU SIEM ONE / SIEM 100: SECURITY OPERATION CENTER (SOC) AS A SERVICE			
SOC LITE 8x5 (verfügbar voraussichtlich ab März 2022): Permanent fortlaufende Prüfung von Ereignissen im Unternehmen | 8x5 Betrieb durch Fachpersonal Abrechnung nach Endgerätestaffel pro Gerät und Monat	nicht verfügbar	✔	✔
SOC Complete 24x7 (verfügbar voraussichtlich ab März 2022: Permanent fortlaufende Prüfung von Ereignissen im Unternehmen | 24x7 Betrieb durch Fachpersonal Abrechnung nach Endgerätestaffel pro Gerät und Monat	nicht verfügbar	✔	✔

Makro Factory GmbH & Co. KG / An der RaumFabrik 30 / 76227 Karlsruhe / Tel +49 721 97 003 100 / info@makrofactory.com / www.makrofactory.com