SECURITY INFORMATION &
EVENT MANAGEMENT (SIEM)

Wir finden die Nadel im Heuhaufen

Die Herausforderung

In einer modernen IT-Infrastruktur gibt es diverse Komponenten, die wertvolle Informationen liefern können. Dabei werden häufig riesige Mengen an Event-Daten generiert, die ohne Korrelation oder maschinelle Unterstützung nicht auswertbar sind. Diese enthalten zum Beispiel Informationen über Betriebskennzahlen einzelner Systeme bis hin zu Sicherheitsereignissen wie beispielsweise wiederholten fehlgeschlagenen Anmeldeversuchen, Kommunikation mit maliziösen IP-Adressen oder dem Erlangen von Administratorrechten, welche Indizien für Security-Incidents sein können. Somit besteht die Herausforderung bei der Erkennung und Behandlung von Security Incidents darin, die sicherheitsrelevanten Informationen in den Eventdaten zu erkennen, so dass eine Sicherheitsanalyse erst möglich wird.

Die Lösung

Um bei dieser Menge an Ereignissen in ihrer Infrastruktur Vorfälle ausfindig zu machen und untersuchen zu können, wird eine Next Generation SIEM-Plattform mit Threat Intelligence, UEBA (User- and Entity Behaviour Analysis) und Maschine-Learning-Fähigkeiten etabliert.

Das SIEM-System normalisiert, analysiert und korreliert Ereignisdaten aus der IT-Infrastruktur und identifiziert so Sicherheitsereignisse, die einer Analyse und ggf. Remediation bedürfen. Zusammenhänge zwischen einzelnen sicherheitsrelevanten Ereignissen werden erkannt und sichtbar gemacht. Ein SIEM als Detective Control liefert Einsicht in sicherheitsrelevante Ereignisse und Security Incidents in der eigenen IT-Infrastruktur und ist somit eine unabdingbarere Komponente einer Sicherheitsarchitektur. Hierdurch können IT-Security Vor-

Die Top 10 Anwendungsfälle

Authentifizierung-Aktivitäten – erkennen Sie ungewöhnliche Authentifizierungsversuche oder Authentifizierungsversuche außerhalb der Geschäftszeiten

Gemeinsame Accounts – bemerken Sie, wenn mehrere Systeme Session-Anfragen für einen Benutzer-Account stellen

Session-Aktivitäten – stellen Sie Session-Dauer und inaktive Sessions fest, bei denen Daten im Zusammenhang mit Session-Logins verwendet werden

Verbindungsdetails – identifizieren Sie verdächtiges Verhalten, wie zum Beispiel Verbindungsversuche zu geschlossenen Ports, blockierte interne Verbindungen, Verbindungen zu verdächtigen Zielen

Verdächtige Administrationspraktiken – überwachen Sie inaktive und deaktivierte Accounts, Accounts mit unveränderten Passwörtern und verdächtige Account-Management-Aktivitäten

Datendiebstahl – weisen Sie versuchte Daten-Exfiltration und Datenlecks zum Beispiel in E-Mails oder auf Fileshares nach

Schwachstellenkorrelation – korrelieren Sie Sicherheitsschwachstellen in Abhängigkeit von anderen verdächtigen Ereignissen

Statistische Analyse – überwachen Sie zum Beispiel das Verhältnis von eingehender zu ausgehender Bandbreitennutzung, Datennutzung pro Anwendung oder ungewöhnliche Reaktionszeiten diverser Applikationen

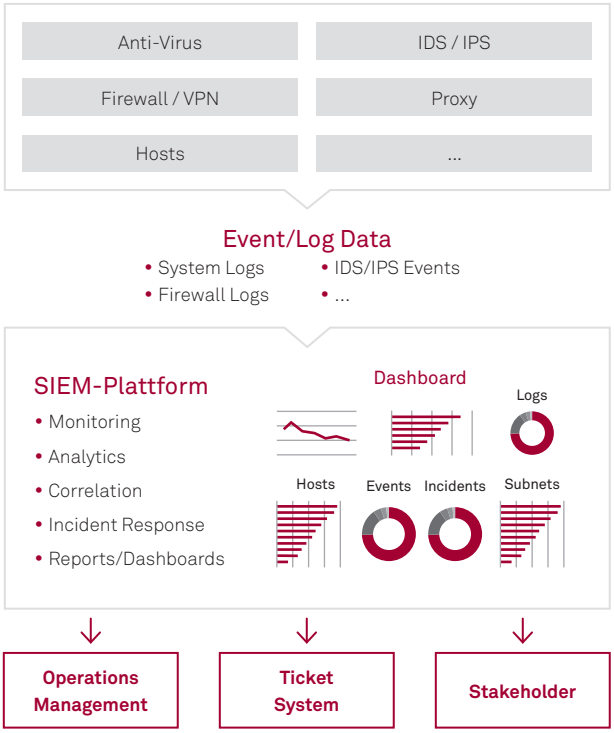
Intrusion Detection und Infection – erkennen Sie mit den Logdaten aus IDS/IPS-, Antivirus, Anti-Malware-Systemen Angriffe und führen Sie automatisierte Gegenmaßnahmen durch

Systemänderungen – lokalisieren Sie Konfigurationsänderungen, Auditkonfigurationsänderungen, Richtlinienänderungen, Richtlinienverletzungen usw.

fälle erkannt und alarmiert werden, die sonst nicht gefunden werden, so dass geeignete Gegenmaßnahmen ergriffen werden können.

Security Incidents werden durch Incident Analyse- und Response Prozesse behandelt. Durch Reporting, Dashboards und Compliance Reports wird der Sicherheitsstand der IT-Infrastruktur visualisiert und für das Management dokumentiert. So verbessert sich auch ihre Gesamtsicht auf die Organisationssicherheit.

Aufbau eines SIEM-Services (exemplarisch)



SIEM als Managed Service

Die msg services ag bietet SIEM-Lösungen für Ihr Unternehmen als Managed Service in unterschiedlichen Ausführungen an. Sie haben die Möglichkeit, sich für eine SIEM-Lösung auf unserer Managed Service Plattform zu entscheiden. Hier können wir – neben dem Betrieb der Plattform – auch erste Analyse- bzw. Incident Response-Maßnahmen übernehmen.

Andererseits besteht die Möglichkeit, die SIEM-Plattform in Ihrer eigenen Infrastruktur zu implementieren (On-Premises), den Betrieb und die Verwaltung dennoch in der Verantwortung der msg services ag zu belassen. Auch hier übernehmen wir optional Analyse- und Incident-Response-Tätigkeiten.

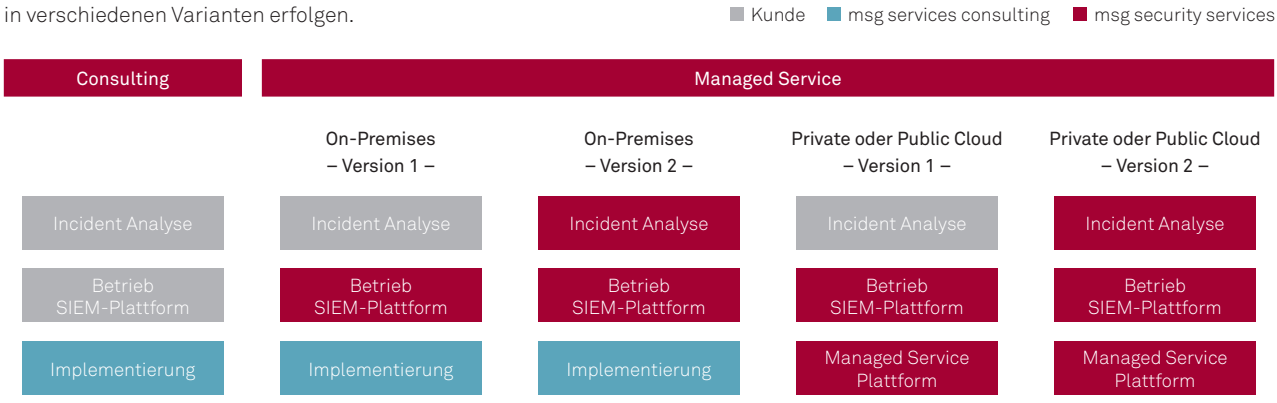
Zudem bieten wir Ihnen Consulting-Leistungen bei der Auswahl und Implementierung einer SIEM-Lösung und der Etablierung der zugehörigen Prozesse in Ihrem eigenen Unternehmen an, so dass Sie die Möglichkeit haben, den Plattform-Betrieb sowie die Incident-Response-Maßnahmen selbst zu bewältigen.

Alles auf einen Blick

Durch übersichtliche und benutzerdefinierbare oder vorgefertigte Dashboards können Sie jederzeit einen Überblick über das aktuelle Geschehen in ihrer IT-Infrastruktur erhalten – sei es beispielsweise Kommunikation mit Threat-Sourcen oder eine Übersicht über alle erkannte Malware. Durch Compliance-Dashboards erhalten sie jederzeit eine Übersicht darüber, wie ihre Infrastruktur die Vorgaben aus Security-Policies und IT-Governance erfüllt.

SIEM für Ihr Unternehmen

Die Realisierung einer SIEM-Lösung für ihr Unternehmen kann in verschiedenen Varianten erfolgen.



msg services ag | Max-von-Eyth-Str. 3 | 85737 Ismaning/München
Telefon: +49 89 96101-0 | Fax: +49 89 96101-2535 | www.msg-services.de | sales@msg-services.de