VON XSOAR ZU GOOGLE SOAR: EIN STRATEGISCHER WECHSEL MIT WEITBLICK

Cybersecurity ist ein sich ständig wandelndes Spielfeld. Steigende Bedrohungslagen, komplexe IT-Infrastrukturen und eine wachsende Flut an Sicherheitswarnungen: Unternehmen brauchen Security-Lösungen, die nicht nur leistungsfähig, sondern auch flexibel und nahtlos integriert sind. Die Wahl der richtigen Security Orchestration, Automation, and Response (SOAR)-Plattform ist ein entscheidender Faktor für den effizienten Betrieb eines Security Operations Centers (SOC).

Unternehmen, die ihre Sicherheitsprozesse automatisieren und effizienter gestalten möchten, stehen oft vor der Frage: Ist die aktuelle Lösung noch optimal oder gibt es leistungsfähigere Alternativen? In diesem Beitrag betrachten wir den Wechsel von XSOAR zu Google SOAR aus einer strategischen Perspektive und beleuchten nicht nur die Vorteile einer einheitlichen Google-Sicherheitsarchitektur, sondern auch die Herausforderungen, die sich dabei ergeben können.

WAS IST SOAR, XSOAR UND GOOGLE SOAR?

SOAR (Security Orchestration, Automation and Response) bezieht sich auf Plattformen, die Sicherheitsoperationen automatisieren und orchestrieren, um eine schnellere und effizientere Reaktion auf Sicherheitsvorfälle zu ermöglichen. Sie helfen dabei, Prozesse zu vereinheitlichen und wiederholbare Aufgaben zu automatisieren. **XSOAR** (früher Demisto) von Palo Alto Networks ist eine führende SOAR-Lösung, die viele Sicherheitsfunktionen und Automatisierungen in einer einzigen Plattform vereint. **Google SOAR** (früher Siemplify), das inzwischen als Teil des Google Security-Ökosystems verfügbar ist, bietet eine umfassende Lösung, die eng mit Google SIEM und der Threat Intelligence integriert ist und damit neue Synergien für eine effiziente Sicherheitsarchitektur ermöglicht.

WARUM EIN WECHSEL ERFORDERLICH WERDEN KANN

Die Wahl der richtigen SOAR-Plattform hängt von verschiedenen Faktoren ab – darunter Integration, Skalierbarkeit und betriebliche Effizienz. Eine ursprünglich passende Lösung kann mit der Zeit an Grenzen stoßen, insbesondere wenn sich technologische Anforderungen oder Geschäftsstrukturen weiterentwickeln.

Typische Herausforderungen, die einen Wechsel erforderlich machen können, sind:

- Begrenzte Flexibilität: Manche SOAR-Systeme sind stark auf ein bestimmtes Sicherheitsökosystem ausgerichtet, was die Integration in heterogene IT-Landschaften erschwert.
- Kostenintensive Skalierung: Mit steigenden Datenmengen können Lizenz- und Betriebskosten erheblich wachsen, wodurch die Wirtschaftlichkeit leidet.
- Fehlende native SIEM-Integration: Wenn SOAR und SIEM nicht optimal zusammenarbeiten, sind zusätzliche Schnittstellen und manuelle Anpassungen erforderlich – ein hoher Wartungsaufwand für Security-Teams.

Moderne Sicherheitsplattformen setzen zunehmend auf eine engere Verzahnung von SIEM, SOAR und Threat Intelligence, um Automatisierungspotenziale bestmöglich auszuschöpfen. Ein Wechsel zu einer umfassend integrierten Lösung kann daher strategische und operative Vorteile bieten.

ALLES AUS EINER HAND: WARUM GOOGLE SOAR ÜBERZEUGT

Der Einsatz von Google SOAR bringt strategische Vorteile, insbesondere durch die enge Verzahnung mit anderen Google-Sicherheitslösungen. Drei zentrale Aspekte sprechen für die Plattform:

1. Nahtlose Integration mit Google Security Operations SIEM

Da sowohl das SIEM als auch das SOAR aus dem gleichen Ökosystem stammen, arbeiten sie enger zusammen als bei einer Kombination aus Lösungen verschiedener Hersteller. Beispielsweise können Vorfälle in Google SOAR mit nur wenigen Klicks weiter analysiert werden, indem zusätzliche Log-Daten aus Google Security Operations SIEM direkt abgerufen werden. In anderen SOAR-Systemen müsste diese Funktion erst aufwendig implementiert werden.

2. Verbesserte Automatisierung und Playbook-Verwaltung

Die Möglichkeit, Sicherheitsvorfälle durch Playbooks automatisiert zu bearbeiten, ist ein zentrales Element jeder SOAR-Lösung. Google SOAR bietet:

- Eine intuitive Playbook-Oberfläche, die eine effiziente Verwaltung von Workflows ermöglicht.
- KI-basierte Unterstützung, die relevante Bedrohungsinformationen automatisch zusammenfasst und Handlungsempfehlungen gibt.
- Eine tiefere Integration mit Google Cloud-Diensten, die Sicherheitsanalysen und Reaktionsmaßnahmen vereinfachen.

3. Google Threat Intelligence als zentrale Quelle

Mit der Übernahme von VirusTotal und Mandiant hat Google sein Threat Intelligence-Angebot massiv erweitert und verfügt nun über eine der weltweit umfassendsten Bedrohungsdatenbanken. Diese Daten fließen direkt in Google SOAR ein und bieten entscheidende Vorteile:

- Erweiterte Kontextinformationen für fundierte Entscheidungen: Google SOAR bietet direkten Zugriff auf umfassende Threat-Intelligence-Daten, um verdächtige IP-Adressen, Domains oder Hash-Werte in Echtzeit zu analysieren. Durch die automatische Korrelation von Bedrohungsinformationen aus verschiedenen Quellen lassen sich Angriffsmuster schneller erkennen. Zudem ermöglicht die Risikobewertung eine gezielte Priorisierung von Vorfällen, sodass SOC-Teams sich auf die kritischsten Bedrohungen konzentrieren können.
- Attack Surface Management für die Identifikation und Bewertung potenzieller Einstiegspunkte für Angreifer: Die Integration mit Mandiant ASM ermöglicht es, Sicherheitslücken kontinuierlich zu erkennen und zu priorisieren. Dadurch können Bedrohungen schneller mit Kontext angereichert und Abhilfemaßnahmen gezielt umgesetzt werden.
- Dynamische Analyse verdächtiger Dateien (Sandboxing): Potenziell schädliche Dateien können in einer isolierten Umgebung (Sandbox) ausgeführt werden, um ihr Verhalten zu analysieren. So lassen sich Malware oder andere Bedrohungen erkennen, bevor sie in das Unternehmensnetzwerk gelangen.

DER WECHSEL – HÜRDEN UND LÖSUNGEN

Der Übergang von einer etablierten SOAR-Plattform zu einer neuen Lösung erfordert eine sorgfältige Planung, um Betriebsunterbrechungen zu vermeiden und eine reibungslose Integration sicherzustellen. Dabei sind mehrere Aspekte zu berücksichtigen:

1. Migration der Playbooks und Automatisierungen: SOAR-Playbooks enthalten die gesamten Sicherheits-Workflows, von der Erkennung bis zur Reaktion auf Vorfälle. Da Google SOAR derzeit nur eine geringere Verschachtelungstiefe bei Playbooks erlaubt, müssen einige Abläufe umstrukturiert werden. Durch die engere Verknüpfung mit Google SIEM können jedoch einige manuelle Prozesse entfallen.

2. Integration mit bestehenden Kunden-IT-Landschaften: Jedes Unternehmen nutzt unterschiedliche Security-Tools – von Microsoft Defender über Sophos bis hin zu SentinelOne. Während Google SOAR viele native Integrationen bietet, müssen für Drittanbieter-Lösungen individuelle Anpassungen vorgenommen werden.

3. Parallelbetrieb und Testphase: Um Risiken zu minimieren, ist es sinnvoll, eine Testphase mit Parallelbetrieb von XSOAR und Google SOAR durchzuführen. Erst nach erfolgreicher Validierung sollte die vollständige Umstellung erfolgen.

BLICK IN DIE ZUKUNFT: WOHIN GEHT DIE REISE MIT GOOGLE SOAR?

Google setzt auf eine Cloud-first-Strategie, was Vorteile, aber auch Einschränkungen mit sich bringt. Zukünftig sollen SOCs alle Kundenumgebungen in einer zentralen Oberfläche verwalten können – mit vollständig getrennten Datenstrukturen. Damit ist eine echte Mandantentrennung möglich. Google bewegt sich verstärkt in Richtung eines geschlossenen Ökosystems, was die Integration mit externen Tools möglicherweise erschwert. Dennoch: Die Vorteile einer einheitlichen Plattform für SIEM, SOAR und Threat Intelligence überwiegen in vielen Anwendungsfällen.

FAZIT: GOOGLE ALS TEIL EINER LANGFRISTIGEN SICHERHEITSSTRATEGIE

Der Wechsel auf eine neue SOAR-Plattform zeigt, wie wichtig eine strategische Weiterentwicklung in der Cybersecurity ist. Eine Lösung muss nicht nur aktuelle Anforderungen erfüllen, sondern auch langfristig skalierbar und flexibel bleiben. Google SOAR bietet durch seine enge Verzahnung mit Chronicle SIEM und den Google Threat Intelligence-Diensten eine leistungsfähige Alternative zu etablierten Lösungen. Dennoch erfordert eine Umstellung eine sorgfältige Planung, um Playbooks zu migrieren, bestehende Integrationen zu erhalten und den Wechsel reibungslos zu gestalten. Wer eine hochintegrierte, cloudbasierte Security-Architektur sucht, findet in Google SOAR eine leistungsstarke Lösung. Eines ist dabei sicher: Security Automation entwickelt sich rasant weiter – und Google spielt dabei eine führende Rolle.