WHITEPAPER

ON-PREM-SIEM IM UMFELD VON RÜSTUNGSUNTERNEHMEN

Souveränität, Kontrolle und operative Realität – mit Gegenüberstellung Cloud-SIEM vs. On-Prem-SIEM

Rüstungsunternehmen stehen vor der gleichen grundsätzlichen cybersicherheitsrelevanten Bedrohungslage wie andere industrielle Organisationen: steigende Angriffsfrequenz, hochprofessionelle Akteure, verkürzte Time-to-Exploit und eine stetig wachsende Abhängigkeit von digitalen Prozessen. Gleichzeitig unterscheiden sich ihre Rahmenbedingungen fundamental. Sicherheitsarchitekturen müssen hier nicht nur wirksam, sondern souverän, nachvollziehbar und politisch belastbar sein.

In diesem Spannungsfeld wird der Einsatz von SIEM-Technologien häufig pauschal diskutiert – Cloud-basiert als moderner Standard, On-Premises als vermeintlich überholt. Eine solche Vereinfachung greift zu kurz. Gerade im Umfeld von Rüstungsunternehmen entscheidet Kontrolle statt Skalierung.

Cloud-SIEM-Plattformen bieten klare Vorteile: schnelle Bereitstellung, elastische Skalierung, global gepflegte Detection-Regeln und den Zugriff auf umfassende Threat Intelligence. Diese Stärken entfalten ihren Nutzen jedoch nur dort, wo Daten frei bewegt werden dürfen und regulatorische sowie geopolitische Abhängigkeiten akzeptiert werden können. Für Rüstungsunternehmen ist dies nur eingeschränkt möglich.

SIEM-Daten enthalten hochsensible Informationen über Systeme, Rollen, Entwicklungs- und Produktionsprozesse sowie Lieferketten. Bereits Metadaten erlauben Rückschlüsse, die aus Sicht nationaler Sicherheitsinteressen nicht außer Haus gegeben werden dürfen. Cloud-SIEM setzt jedoch zwangsläufig voraus, dass Daten den eigenen Sicherheitsperimeter verlassen – unabhängig davon, ob von Sovereign- oder Hyperscale-Clouds gesprochen wird.

Hinzu kommt die faktische Abhängigkeit von externen Analyse-, Regel- und KI-Pipelines. Je stärker Cloud-SIEM auf automatisierte Korrelation und KI-gestützte Priorisierung setzt, desto schwieriger wird die fachliche Nachvollziehbarkeit einzelner Entscheidungen. Für auditierte, freigabepflichtige Umgebungen ist dies ein erheblicher Zielkonflikt.

Ein weiterer häufig unterschätzter Aspekt ist die Betriebsfähigkeit im Krisen- oder Verteidigungsfall. Rüstungsunternehmen müssen davon ausgehen, auch bei geopolitischen Spannungen, Sanktionen oder eingeschränkter Netzanbindung funktionsfähig zu bleiben. Cloud-SIEM ist per Definition extern, netzabhängig und vertraglich limitiert. Ein On-Prem-SIEM hingegen kann auch isoliert, autonom und unter eingeschränkten Kommunikationsbedingungen betrieben werden.

On-Prem-SIEM ist dabei eher ein Betriebsmodell und weniger ein rein technisches Produkt. Es erfordert qualitätsgesicherte Logquellen, tiefes Verständnis der eigenen Systeme, klar definierte Use Cases und verbindliche Reaktionsprozesse. Viele SIEM-Projekte scheitern nicht an der Technologie, sondern an fehlender Verantwortung, überzogenen Erwartungen oder mangelnder Priorisierung.

Anstelle zusätzlicher Hardware ist Know-how der ausschlaggebende Faktor bei Skalierung bezüglich SIEM. Gerade in hochspezialisierten Rüstungsumgebungen lassen sich wirksame Detection-Modelle nicht aus Standardkatalogen ableiten. Sie entstehen aus Eigenverständnis und kontinuierlicher Weiterentwicklung.

Ein belastbares On-Prem-SIEM-Zielbild folgt daher dem Prinzip Fokus vor Breite. Wenige sicherheitskritische Use Cases – etwa Identitätsmissbrauch, privilegierte Zugriffe, laterale Bewegungen oder Partnerzugriffe – erzeugen mehr Wirksamkeit als eine Vielzahl generischer Alarme.

GEGENÜBERSTELLUNG: Cloud-SIEM vs. On-Prem-SIEM

Kriterium	Cloud-SIEM	On-Prem-SIEM
Datensouveränität	Externe Verarbeitung, rechtliche Abhängigkeiten	Volle Kontrolle im eigenen Sicherheitsperimeter
Nachvollziehbarkeit	Begrenzte Transparenz bei KI und Regelwerken	Volle Einsicht in Logik und Korrelation
Krisenresilienz	Netz- und Providerabhängig	Autarker Betrieb auch isoliert möglich
Regulatorische Eignung	Eingeschränkt für VS- und Rüstungsumfeld	Geeignet für hochregulierte Umgebungen
Skalierung	Technisch einfach skalierbar	Skalierung primär über Know-how
Betriebsaufwand	Geringerer Initialaufwand	Höherer Initial- und Betriebsaufwand

Fazit

Der Einsatz von SIEM-Technologien im Umfeld der Rüstungsindustrie ist weit mehr als eine Tool- oder Architekturfrage. Er ist eine strategische Entscheidung über Souveränität, Kontrollfähigkeit und Resilienz. Cloud-SIEM bietet Effizienz und Geschwindigkeit, setzt jedoch strukturelle Abhängigkeiten voraus, die mit den sicherheitspolitischen, regulatorischen und operativen Anforderungen von Rüstungsunternehmen nur begrenzt vereinbar sind.

Unter diesen Rahmenbedingungen ist On-Prem-SIEM ein bewusst gewähltes Betriebsmodell und keine überholte Alternative. Es erlaubt vollständige Kontrolle über Daten, Analyseprozesse und Reaktionen – auch bei außergewöhnlichen oder krisenhaften Vorkommnissen. Diese Vorteile gehen mit höherem Aufwand einher, insbesondere beim Aufbau von Know-how, Prozessen und klaren Verantwortlichkeiten. Genau darin liegt jedoch der zentrale Wert: Statt sie auszulagern, wird Sicherheit beherrschbar gemacht.

Der Erfolg eines On-Prem-SIEM bemisst sich nicht an Funktionsumfang oder Datenmengen. Ausschlaggebend ist die Fähigkeit, relevante Angriffe zuverlässig zu erkennen, einzuordnen und kontrolliert zu bewältigen. Für Rüstungsunternehmen bedeutet dies: weniger Technologiegläubigkeit, mehr Fokus auf operative Realität, Entscheidungsfähigkeit und souveräne Sicherheitsarchitekturen.

IHR KONTAKT

MANUEL NOE
Geschäftsführung
telefon +49 6262 9262594
email manuel.noe@is4it-kritis.de

IS4IT KRITIS GmbH
Kraichgaublick 13
74847 Obrigheim
telefon +49 6262 9262594
www.is4it-kritis.de