

Leistungsbeschreibung

Splunk Enterprise Security

Inhalt:

I.	Das Unternehmen	2
II.	Auftragsgegenstand	2
A.	Allgemeine Anforderungen	2
1.	Integration SIEM und SOAR.....	2
2.	Betrieb	2
3.	Hochverfügbarkeit.....	2
4.	Skalierung und Clusterfähigkeit.....	2
5.	Konfiguration.....	3
B.	SIEM-Komponente	3
1.	Logeinlieferung	3
2.	Lognormalisierung	3
3.	Abfragesprache und Erkennungsregeln	3
4.	Logging und Audit.....	3
5.	Workload Management	4
C.	SOAR-Komponente	4
1.	Casemanagement	4
2.	Automation.....	4
3.	Integrationen.....	4
D.	Support und Pflege	5
E.	Splunk Services	5

I. Das Unternehmen

Die Techniker Krankenkasse (TK) ist eine bundesweite Krankenkasse mit rund 9,6 Millionen Mitgliedern und insgesamt rund 12,4 Millionen Versicherten. Als gesetzliche Krankenversicherung ist die TK eine Körperschaft des öffentlichen Rechts mit Selbstverwaltung.

II. Auftragsgegenstand

Auftragsgegenstand ist die Lieferung des Security Information and Event Management System (SIEM) mit integrierter Security Orchestration, Automation and Response (SOAR) für das interne Security Operations Center (SOC) des Herstellers Cisco/Splunk (Produktbezeichnung „Splunk Core + Enterprise Security (ES) Premier Edition“ im Folgenden „Anwendung“ genannt). Ziel ist der Aufbau einer leistungsfähigen, zukunftssicheren Lösung zur Überwachung, Korrelation und Analyse sicherheitsrelevanter Ereignisse sowie zur automatisierten Unterstützung von Incident-Response-Prozessen.

Die Anwendung muss vollständig on-Premise in der IT-Infrastruktur der TK betrieben werden können.

Der AN hat der TK die Lizenzen für die Anwendung im benötigten Umfang (siehe Nr. 3.1 des Vertrags) zu liefern und dafür zu sorgen, dass Softwarepflege und Support durch den Hersteller erbracht wird.

A. Allgemeine Anforderungen

1. Integration SIEM und SOAR

Die Komponenten SIEM und SOAR der Anwendung müssen ab Installation eng miteinander integriert funktionieren, ohne dass dafür eigene Anpassungen oder externe Plugins notwendig sind. Beide Komponenten müssen nahtlos in der gleichen Benutzeroberfläche bedienbar sein. Zu bearbeitende Incidents müssen an einer zentralen Stelle angezeigt und bearbeitet werden. Sowohl die Ergebnisse des SIEM beim Erstellen des Incidents als auch alle Anreicherungen durch SOAR-Automatisierungen müssen dort sichtbar sein. Automatisierungen des SOAR müssen über Funktionen direkt auf die Datenbasis zugreifen können, die im SIEM zu einem Incident geführt hat.

2. Betrieb

Die Anwendung muss auf virtualisierten Red Hat Enterprise Linux 9 (und nachfolgenden Versionen) Servern lauffähig sein. Die Server müssen weiterhin vollständig in der standardisierten Server Verwaltung der TK integriert sein (keine virtuelle Appliance). Die Verwaltung der Anwendung stellt die Systemcompliance sicher und führt automatische Updates des Betriebssystems durch und erzwingt eine Basiskonfiguration.

3. Hochverfügbarkeit

Die Anwendung muss hochverfügbar im Modus "Active-Active" betreibbar sein. Das heißt, alle Komponenten müssen gleichzeitig auf mehreren Servern aktiv laufen und die Last muss über eingebaute Mechanismen verteilt werden. Fällt eine Komponente, ein Server oder ein Rechenzentrum aus, müssen die verbleibenden Server sich die Last automatisch neu aufteilen und die Verfügbarkeit sicherstellen. Es darf maximal zu geringen Verzögerungen in der Verarbeitung (< 5 Minuten bis alle Daten ohne Datenverlust wieder zur Verfügung stehen) oder einem Neuladen der Benutzeroberfläche kommen, nicht etwa zu vollständigen Ausfällen in der Logverarbeitung oder manuellen Eingriffen, um die Anwendung wieder verfügbar zu machen.

4. Skalierung und Clusterfähigkeit

Fallen in Zukunft mehr zu verarbeitende Daten an, sodass die bestehenden Server im Cluster diese nicht mehr ausreichend schnell verarbeiten können, muss das Cluster um Server erweitert werden

können, ohne das Cluster neu aufzusetzen. Die Anwendung muss mindestens auf bis zu 2 TB pro Tag Ingest bei einer Aufbewahrungszeit von 180 Tage erweitert werden können.

Die Last muss von der Anwendung automatisch auf mehr Server verteilt werden, um eine ausreichend schnelle Verarbeitung wieder sicherzustellen.

Zusätzlich zu dieser Art der Erweiterung muss die Anwendung auch die Integration mehrerer Cluster als eine einzelne Datenbasis unterstützen. Mehrere, verteilte Cluster für die Datenverarbeitung müssen in einer zentralen Benutzeroberfläche durchsuchbar sein, Regelwerke müssen auf diese zentrale Datenbasis bezogen greifen statt nur auf Daten in den jeweils einzelnen Clustern.

5. Konfiguration

Die Konfiguration der Anwendung muss als Config-as-Code möglich sein. D. h. jede Aktion, welche in der GUI ausgeführt werden kann, muss auch über eine Konfigurationsdatei oder API ausgeführt werden können.

B. SIEM-Komponente

1. Logeinlieferung

Das Einliefern von Logs an die SIEM-Komponente im Push-Verfahren muss über verschiedene Standard-Protokolle möglich sein. Mindestens müssen HTTP, HTTPS und das Einliefern von Logdaten über definierbare TCP/UDP-Sockets unterstützt werden. Zudem muss das SIEM im Pull-Verfahren Protokolle unterstützen, um Logs von externen Services abzuholen. Von Haus aus oder über fertige, installierbare Module müssen Events aus MSSQL-, Postgres-, Oracle- und SAP HANA-Datenbanken, aus Azure Event Hubs und simple REST APIs abgeholt werden können. Neu sendende Logquellen müssen automatisch korrekt erkannt, geparkt, normalisiert und integriert werden.

2. Lognormalisierung

Vorgefertigte (installierbare) Module müssen vorhanden sein, um Parsing und Normalisierung gängiger Logtypen vorzunehmen, mindestens für die Logtypen Microsoft Windows Security, Linux auditd, Apache Access, Apache ModSecurity und Netskope. Zusätzlich müssen eigene Parsings angelegt werden können, um eigene Logtypen korrekt zu normalisieren. Werte aus Standardformaten wie Syslog, JSON und CEF müssen auf einfache Weise extrahiert werden können. Komplexes Parsing über reguläre Ausdrücke muss ebenfalls möglich sein.

3. Abfragesprache und Erkennungsregeln

Die Datenbasis an Logs muss zentral mittels einer Abfragesprache durchsuchbar sein. Zur Erstellung von Abfragen muss es Hilfestellungen geben (bspw. interaktiver Editor oder Autovervollständigung). Die Anwendung muss vordefinierte Regeln mitbringen, die gängige Angriffe erkennen, oder sie müssen als Module installierbar sein. Diese müssen auch manuell angepasst werden können. Eigene Erkennungsregeln müssen in einer Abfragesprache definierbar sein und es muss Hilfestellungen zu ihrer Erstellung geben (bspw. interaktiver Editor oder Autovervollständigung, low-/no-code). Alle Erkennungsregeln müssen versioniert vorliegen, sodass der aktuelle Stand mit älteren Versionen verglichen und einfach zurückgerollt werden kann.

Die Ausführung der Regeln muss bei der Dateneinlieferung nahezu in Echtzeit erfolgen können.

4. Logging und Audit

Aktionen von Usern auf der Plattform müssen automatisch vollständig protokolliert werden.

Eine Änderungs- und Ausführungshistorie muss bei Playbooks vorhanden sein.

Die SIEM-Komponente muss die Möglichkeit vorsehen, threat intelligence feeds nativ einzubinden.

Die Daten in der SIEM-Komponente müssen in Dashboards visualisierbar sein, für z.B. KPIs. Dabei muss die Anwendung eine einfache Möglichkeit zur Erstellung für eigene Dashboards bieten. Zudem ist eine Anbindung an die Software Grafana zur Visualisierung erforderlich.

5. Workload Management

Es muss effiziente Möglichkeiten geben, die Ressourcennutzung der Plattform zu steuern und zu überwachen. Dafür müssen genutzt Ressourcen durch Anfragen von Usern dokumentiert werden. Zudem muss es möglich sein, bestimmten Usern oder Gruppen Ressourcen exklusiv zur Verfügung zu stellen oder ein Limit bei der maximalen Nutzung zu setzen. Ebenso muss es die Möglichkeit geben, Anfragen zu priorisieren.

Diese Anforderungen gelten für interaktive (durch User initiiert) und nicht interaktive (zeitlich ausgelöst) Suchen.

C. SOAR-Komponente

1. Casemanagement

Mehrere Incidents müssen zusammengefasst oder verknüpft werden können, sodass eine Bearbeitung zentral erfolgen kann und am Ende klar erkenntlich ist, dass diese zusammengehören. Falls es bereits ähnliche Incidents mit den gleichen Daten gibt, muss dies automatisch erkannt und im Incident sichtbar gemacht werden.

Die Anzahl der User mit Zugriff auf das Casemanagement darf nicht beschränkt sein.

2. Automation

Incidents müssen über vordefinierte und eigene Automatisierungen mit Daten angereichert werden können. Dabei muss Python als Programmiersprache zur Automatisierung unterstützt werden. Fertige Trigger müssen dafür sorgen, dass eigene Automatisierungen beim Erstellen, beim Update und beim Schließen eines Incidents ausgeführt werden.

Automatisierungen müssen die Möglichkeit von "human in the loop" Freigaben bieten. Der User muss vor Bestätigung die Möglichkeit haben, die auszuführenden technischen Details einzusehen.

Playbooks müssen testbar sein, ohne direkt eine Aktion auszuführen.

Die Anzahl der User mit Zugriff (als Admin bzw. Editor) auf die Automation darf nicht beschränkt sein.

3. Integrationen

Es muss verschiedene Integrationen für marktübliche Tools geben. Diese Integrationen müssen vom Hersteller selbst oder von Drittanbietern bereitgestellt werden können.

Insbesondere Microsoft Defender for Endpoint (MDE) muss mittels fertiger Integration eingebunden werden können. Incidents aus MDE müssen in der Anwendung ebenfalls zu einem Incident führen und bearbeitet werden können. Automatisierungen müssen auf diese Incidents ebenfalls anwendbar sein und ein Abschluss des Incidents in der Anwendung muss den Incident in MDE ebenfalls schließen.

D. Support und Pflege

Der AN hat dafür zu sorgen, dass die Software durch den Hersteller gepflegt wird. Die Softwarepflege umfasst insbesondere:

- Bereitstellung und Einspielung von Fehlerkorrekturen (Bugfixes),
- Bereitstellung und Einspielung von Sicherheitsupdates,
- Bereitstellung von Funktionsupdates (Minor-/Major-Releases), soweit zur Sicherstellung des ordnungsgemäßen und sicheren Betriebs erforderlich.

Der AN hat dafür zu sorgen, dass die TK direkten Zugriff auf Support des Herstellers hat. Störungsmeldungen können per Telefon, Mail oder über ein Supportportal erfolgen.

E. Splunk Services

In den bereitgestellten Lizenzen sind Credits für Schulungen (Education program - EDU) und technische Unterstützung (OnDemand Services - ODS) direkt durch den Hersteller enthalten.

Während der Vertragslaufzeit werden jährlich 700 EDU Credits zur Verfügung gestellt, welche für Schulungen durch Splunk genutzt werden können. Eine aktuelle Liste der verfügbaren Schulungen wird durch Splunk bereitgestellt. 1 EDU Credit entspricht 10 USD.

Außerdem werden 10 ODS pro Quartal bereitgestellt, welche für die technische Unterstützung von Splunk Experten durch die TK genutzt werden können. Die möglichen Verwendungen der ODS Credits werden durch Splunk in einer Liste bereitgestellt und umfassen z. B. „Ask a Security Expert“ oder „Upgrade Readiness Assessment“.

Anlagen:

- Vorgaben aus IT-Sicht (Anlage L1)
- Splunk Support SLA (Anlage L2)