# Grundlagen für SIEM- und SOAR-Einführung: Praxisbericht

SIEM und SOAR: BAITmen für den Bankbetrieb.

**Autor:**

**Swer Rieger,**
**Senior Consultant**
**Security und Produkte,**
**Consist Software Solutions GmbH.**

▷ Auf Bankbetriebe prasseln jede Menge gesetzliche Regelwerke ein, was die IT-Sicherheit betrifft. In Standards und Normen sind deren genaue Anforderungen definiert. Die resultierenden Compliance-Vorgaben setzen sich zusammen aus:

- Mindestanforderungen an das Risikomanagement (MaRisk),
- BAIT (Bankaufsichtliche Anforderungen an die IT, herausgegeben von der BaFin),
- KAMaRisk (Mindestanforderungen an das Risikomanagement von Kapitalgesellschaften),
- Datenschutzgesetze (DSGVO, TMG, TKG)
- ISO/IEC-Standards der 2700x-Reihe,
- BSI IT-Grundschutz,
- ISF Standard of Good Practice for Information Security 2018,
- Common Attack Pattern Enumeration and Classification (CAPEC),
- NIST SP800 R.x,
- SANS Whitepaper

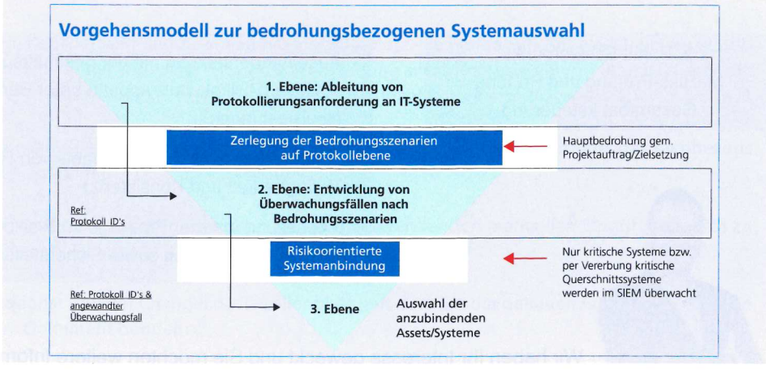
Systeme für Security Information and Event Management (SIEM) und SOAR (Security Orchestration, Automation and Response) sind neben ihrer eigentlichen Aufgabe, die IT Security zu gewährleisten, auch in der Weise nutzbar, die Einhaltung gesetzlicher und interner Regelungen zu dokumentieren, beziehungsweise bei deren Nichteinhaltung die ergriffenen Maßnahmen.

Denn es reicht heutzutage nicht mehr, IT-Security nur noch an technischen Komponenten festzumachen, wie Firewalls, Intrusion Detection, Schwachstellen-Scanner, Virenscanner, Anti-Viren-Software oder Web-Filter. In Sicherheitskonzepte müssen immer auch Prozesse und Mitarbeiter einbezogen werden, damit sie funktionieren. Mit einem SIEM lässt sich eine hohe Transparenz über die Aktivitäten auf den genutzten Systemen herstellen. Man erkennt auf einen Blick, wo sicherheitskritische Aktivitäten ablaufen, kann diese nachverfolgen, die Bearbeitung dokumentieren und über die aktuelle Lage berichten. Ein SOAR ermöglicht die automatisierte Abarbeitung von Verdachtsfällen: bei heutigen komplexen Systemumgebungen eine große Hilfe.

## I. SIEM und SOAR im Einsatz

Das SIEM wird mit Log-Daten (Events) von Servern, Datenbanken, Netzwerkkomponenten, des Active Directory und Anwendungen gefüttert, zusätzlich können aus externen Quellen Listen (Indicators of Compromise), mit potenziellen und bekannten bösen IPs, URLs und anderen Mustern (Pattern) genutzt werden, um über geeignete Auswertungen (Regeln) verdächtige Sachverhalte und Angriffe (Incidents) zu erkennen.

**Abbildung 1: Vorgehensmodell zur bedrohungsbezogenen Systemauswahl**




Sicherheitsvorfälle werden vom SIEM an die SOAR-Plattform weitergeleitet und dort geclustert (Automation). So kann der Case Load erheblich reduziert werden. Mit der Weiterleitung an die eingebundenen Security Tools wird der Response-Prozess gestartet (Orchestration and Response).

### 1. Wie werden aus Events Incidents?

In der Praxis hat sich gezeigt, dass es umfangreiche Regelsammlungen zur Eventauswertung gibt, die als Muster gut geeignet sind, aber die spezifischen Regeln für eine Firma doch ein erhebliches Feintuning (Projekt) erfordern, um die relevanten Incidents zu generieren, die auch wirklich einer Nachbearbeitung bedürfen. Bei deren Nachbearbeitung kann durch Automatisierung mit einem SOAR, wie beschrieben, viel Effizienz gehoben werden.

Über ein Vorgehensmodell zur bedrohungsbezogenen Systemauswahl (s. Abb. 1 und 2), werden die Anforderungen auf Protokollebene identifiziert und daraus Überwachungsfälle (Controls) entwickelt. Die Überwachung erfolgt dann mit **automatisierten Analysen** (Regeln) der Logdaten im SIEM und generiert Incidents. Dank des automatisierten Regelfilters werden aus sehr vielen Events wenige wirklich relevante Incidents.

Die Analyse, ob ein Incident Maßnahmen erfordert, um die Sicherheit zu erhalten oder wieder herzustellen, erfolgt i. d. R. manuell durch Spezialisten (Security-Analysten). Bei größeren Organisationen sind diese Spezialisten in einem Security Operation Center (SOC) organisiert. Definierte Prozesse zur Incident-Bearbeitung mit Einbindung der weiteren Firmenorganisation sind ein weiterer Bestandteil eines SOC.

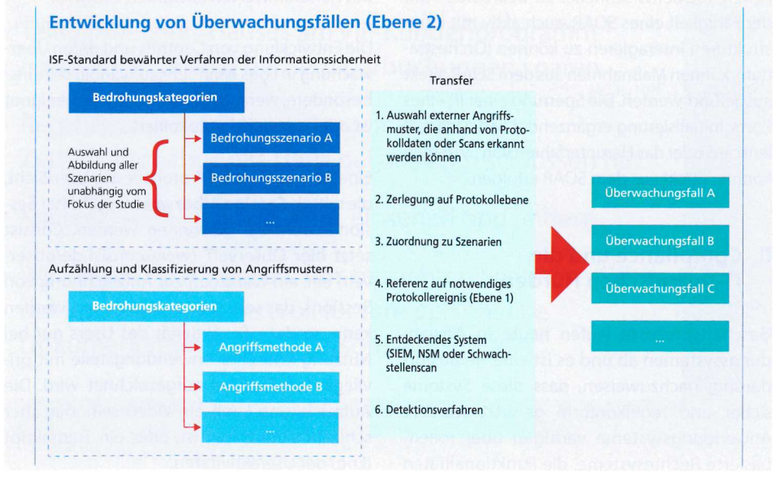
### 2. SOAR ergänzt SIEM

Die Incidents aus einem SIEM müssen bearbeitet werden. Incident-Management-Systeme sind dazu grundsätzlich geeignet und die meisten SIEMs können auch Incidents in solche Systeme überführen, worin dann die weitere Bearbeitung manuell erfolgen müsste. Am Markt gibt es einige gute SIEM-Systeme.

Consist setzt beispielsweise Splunk ein, das der aktuelle Gartner-Report als führendes SIEM-System ausweist (https://www.splunk.com/en_us/form/gartner-siem-magic-quadrant.html). In jedem Fall ist es wichtig, das SIEM genau **an** die **individuellen Unternehmensgegebenheiten anzupassen**. Ziel ist es in diesem Zusammenhang, die Anzahl der zu pflegenden Regeln

» Es reicht heutzutage nicht mehr, IT-Security nur noch an technischen Komponenten festzumachen. «

**Abbildung 2: Entwicklung von Überwachungsfällen**



» Ziel ist es in diesem Zusammenhang, die Anzahl der zu pflegenden Regeln möglichst klein zu halten, aber dennoch den Anforderungen zu genügen. «

möglichst klein zu halten, aber dennoch den Anforderungen zu genügen.

In der Praxis schnappt sich heute ein Security-Analyst den Incident und analysiert weiter. Je nach Incident wird geklärt, ob einzelne Systeme betroffen sind, spezielle User involviert sind, aktuelle Bedrohungen eine Rolle spielen oder Ähnliches. Die Events im SIEM werden unter verschieden Blickwinkeln analysiert. Da der Rückgriff auf das SIEM oder andere Sicherheitssysteme notwendig ist, wäre es eine erhebliche Arbeitserleichterung, wenn dies gleich aus dem Incident Management heraus erfolgen könnte, zumal dann auch leicht die Dokumentation der Analyse automatisch erfolgen kann.

Hier setzt ein SOAR ein. Es ist verknüpft mit Sicherheitssystemen, primär einem SIEM, es können aber auch andere Systeme, wie ein IDS oder Schwachstellenscanner direkt sein. Das SOAR nimmt deren Incidents auf und arbeitet diese in vordefinierten Prozessen (Playbooks) ab. Es reichert diese mit Informationen an, kann aber auch Incidents final bearbeiten, wenn Playbooks dies vorsehen. Die Praxis in Security-Teams hat gezeigt, dass eine große Zahl der Incidents schnell mit Standardüberprüfungen (Analysen) abgearbeitet werden können und so nur noch die Dokumentation für spätere Auswertungen wichtig ist.

Bei anderen Incidents fallen immer gleiche Analysen an, die schon automatisiert ablaufen können und dann dem Security-Analysten helfen, Incidents schneller zu bearbeiten. Mit der Fähigkeit eines SOAR, auch aktiv mit Infrastrukturen interagieren zu können (Orchestration), können Maßnahmen aus dem SOAR direkt ausgeführt werden. Die Sperrung einer IP, eines Ports, Initialisierung ergänzender Schwachstellenscans oder das Herunterfahren von Systemen können direkt aus dem SOAR erfolgen.

## II. Compliance und die IT-technischen Hürden

Geschäftsprozesse laufen heute in Anwendungssystemen ab und es ist eine Herausforderung, nachzuweisen, dass diese Systeme sicher und regelkonform genutzt werden. Anwendungssysteme verfügen über rollenbasierte Rechtesysteme, die Funktionalitäten für User frei schalten oder sperren. Im laufenden Betrieb sind privilegierte User notwendig. Administratoren für Datenbanken und Basissysteme seien hier genannt. Deren Tätigkeiten erfordern privilegierte Berechtigungen, die jedoch nicht bei der Ausführung der normalen Geschäftsprozesse genutzt werden dürfen. Gleichzeitig sind privilegierte User immer auch Einfallstore für die **Kompromittierung von Systemen und Daten**. Es ist also unbedingt notwendig, privilegierte User, auch in ihrem eigenen Interesse, zu überwachen und permanent zu prüfen, ob deren Privilegien missbräuchlich genutzt werden. Die Heraufstufung von Usern zu privilegierten Usern ist eines der Überwachungsziele.

Füttert man die Logs (Ereignisprotokoll eines Programms) von Anwendungssystemen, speziell Audit- und Securitylogs, können in vielen Systemen die Aktivitäten privilegierter User überwacht werden. In der Praxis hat sich jedoch gezeigt, dass Logs oft nicht ausreichen – weitere Datenquellen müssen genutzt werden. Beispielsweise reicht auch bei SAP die Analyse der Audit- und Security-Logs nicht aus, hier muss auf weitere Informationen zurückgegriffen werden.

Die Entwicklung der **Überwachungsfälle** (Controls) muss für jedes Anwendungssystem erfolgen, damit Regeln definiert werden können. Ein Überwachungsfall entsteht auch, wenn ein privilegierter User die Berechtigung für einen Mitarbeiter erweitert, so dass dieser Transaktionen mit höheren Werten ausführen kann.

Die Entwicklung von Controls und deren Überwachung in Logs kann sehr aufwändig sein, insbesondere, wenn die Anwendung ungeeignet ist oder gar nicht protokolliert.

Eine Alternative sind Protokolle aus User-Sicht, die mittels **Session-Überwachung** (früher Session-Recording) gewonnen werden. Consist setzt hier ObserveIT (www.consist.de/observeit) ein, ein Werkzeug zur Aufzeichnung von Sessions, das sehr granular gesteuert werden kann, so dass die Aktivität des Users nur bei Nutzung kritischer Anwendungsteile mit privilegierten Rechten aufgezeichnet wird. Die Aufzeichnung kann ein Video sein, das aber schlecht auswertbar ist, oder ein Transskript (Log) der Useraktivitäten.

### SeminarTIPPs

**IT-Sicherheit Kompakt, 24.09.2019, Frankfurt/M.**

**FCH Innovation Days 2019, 24.–25.06.2019, Berlin.**

**Hackerangriffe & Cyber-Attacken: Reaktion und Prävention, 25.09.2019, Frankfurt/M.**

**www.FC-Heidelberg.de**

» SIEM und SOAR generieren automatisch die Dokumentation der aktuellen Sicherheitslage. «

**BuchTIPPs**

**Held/Kühn (Hrsg.): Praktikerhandbuch IT- und Informationssicherheitsbeauftragter, 2018.**

**Weimer (Hrsg.): Bearbeitungs- und Prüfungsleitfaden: Datenschutz, IT-Sicherheit & Cyberrisiken, 4. Aufl. 2017.**

**www.FC-Heidelberg.de**

## III. Compliance mit SIEM und SOAR

SIEM und SOAR generieren automatisch die Dokumentation der aktuellen Sicherheitslage – genauer: Protokolle zu Sicherheitsvorfällen, die sich aus der Überwachung relevanter Controls ergeben. Die eingeleiteten Maßnahmen sind in den Protokollen enthalten, sofern diese systemgestützt erfolgen. Bei manuellen Eingriffen müssten diese bei der Incident-Bearbeitung händisch im System ergänzt werden.

Die Compliance-Überwachung erfolgt primär über eine Dokumentation, die das Monitoring der privilegierten User enthält. Bei definierten **kritischen Systemzugriffen**, beispielsweise: SAP-Notfall-User führt Buchungen aus, technischer User meldet sich im Dialog an oder Datenbankadministrator ändert Tabelleninhalte eines Anwendungssystems, sollen Alarme ausgelöst werden.

Die Bearbeitung der generierten Incidents lässt sich in einem SOAR so steuern, dass alles dokumentiert wird und damit auch auswertbar ist. Die reine Dokumentation kann automatisiert erfolgen. Kritische Incidents (Alarme) bedürfen weiterer Analysen und Maßnahmen, die ebenfalls dokumentiert werden. So bieten Analysen, ob bestimmte Überwachungen in bestimmten Systemen mit zunehmender Häufigkeit anschlagen, wesentliche Hinweise, hier genauer hinzusehen.

## IV. Aus einem konkreten Projekt bei einer Bank

### 1. Aufgabe

Privilegierte User und Admins sollen beim Zugriff auf Anwendungssysteme und deren Komponenten überwacht werden. Ein zentrales unabhängiges Sicherheitsinformationsmanagement sollte hierfür in Betrieb gehen.

### 2. Herausforderung

Mehr als 40 heterogene bankfachliche Anwendungssysteme mit sehr hohem Schutzbedarf, einschließlich eines SAP-Systems, mussten datentechnisch (Logs und Protokolle aus Systemdatenbanken und Anreicherungen aus den Anwendungssystemen) an ein SIEM (Splunk) angebunden werden.

### 3. Lösung

Anhand aktueller Standards und Normen (siehe oben) wurden die Überwachungsanforderungen definiert, die Systeme in Risikogruppen eingestuft und bei den „hoch" eingestuften Anwendungssystemen der Transfer in Überwachungsregeln (Auswertungen auf den Logs mit Ergänzungen) definiert.

Der Start erfolgte mit einem Proof of Concept, in dem das Monitoring des SAP-Systems getestet wurde. Im Projektteam hatte die Bank dann die Projektleitung inne und steuerte das Know-how zu Fachanwendungen über ihre Fachanwendungsbetreuer bei. Consist übernahm mit seinen Splunk- und Security-Consultants die Konzeption und Umsetzung mit Splunk.

Das SIEM ist für das in der Bank übliche Staging (Entwicklungs-, Test- und Produktivstage) ausgelegt, wobei der Transfer von Apps, Dashboards, Konfigurationen und Suchen (Regeln) von einer zur nächsten Stage des SIEM weitgehend automatisiert erfolgt.

Alerts und Dokumentation sind wesentliche Bestandteile des Systems. Das Projektteam übergab das System nahtlos in die Betreuung der Managed Services von Consist. Der laufende Betrieb mit allen notwendigen Anpassungen des SIEM an alle Datenanbindungen und Regeln wird dort ausgeführt.

Die Bank arbeitet mit den Auswertungen aus dem System und prüft bei Alarmen, ob Maßnahmen ergriffen werden müssen. Da das System die bankfachlichen Anwendungen umfasst und nicht die Basissysteme, ist die Alarm/Incidentbearbeitung durch die Fachanwendungsbetreuer und die Verantwortlichen der Fachabteilungen möglich. Eine übergreifende Kontrolle erfolgt durch die Security-Abteilung der Bank.

### 4. Kundennutzen

Die Einbindung privilegierter User ins kontinuierliche Monitoring senkt Risiken und vermindert die Bedrohungsfläche, weil Kompromittierungen schneller entdeckt werden können. Die Aufdeckung von Insider Threats wird erleichtert. Durch systemübergreifende Normierungen der Datenhaltung des SIEM (bei Splunk als Common Information Model (CIM) bekannt), ergänzend zu den Rohdaten, ist das System auch künftig gut erweiterbar und robust gegen Änderungen in den Anwendungssystemen.

Das System speichert alle Daten **revisionssicher** im Rohformat. Die Incidentbearbeitung dokumentiert das System automatisiert und bietet Auditfunktionalitäten für die Incidentbearbeitung und den Betrieb des Systems. BSI-, EZB- und BaFin-Sicherheitsanforderungen werden so erfüllt[1]. □

[1] Weitere Informationen:
Über Consist: www.consist.de
Presse-Service: www.consist.de/presse

**PRAXISTIPPS**

- ☐ Security-Know-how und -Erfahrung sind die Basis für SIEM- und SOAR-Projekte.
- ☐ SIEM und SOAR sind ein starkes Gespann.
- ☐ Ziel muss es sein, die Zahl der Regeln im SIEM zu minimieren.
- ☐ SOAR ist der Schlüssel zur Effizienzverbesserung in Security-Teams.
- ☐ Anwendungssysteme liefern häufig ungeeignete Logs, Abhilfe kann selektives Sessionrecording sein.