

ISACA Security Use-Cases Leitfaden Umsetzung im Mittelstand

D. Schugardt

Februar 2026



Wie sind wir auf das Thema gekommen?

Die Suche nach dem SIEM der SIEMs als Lösung für alle Kundengrößen zu akzeptablem Preis

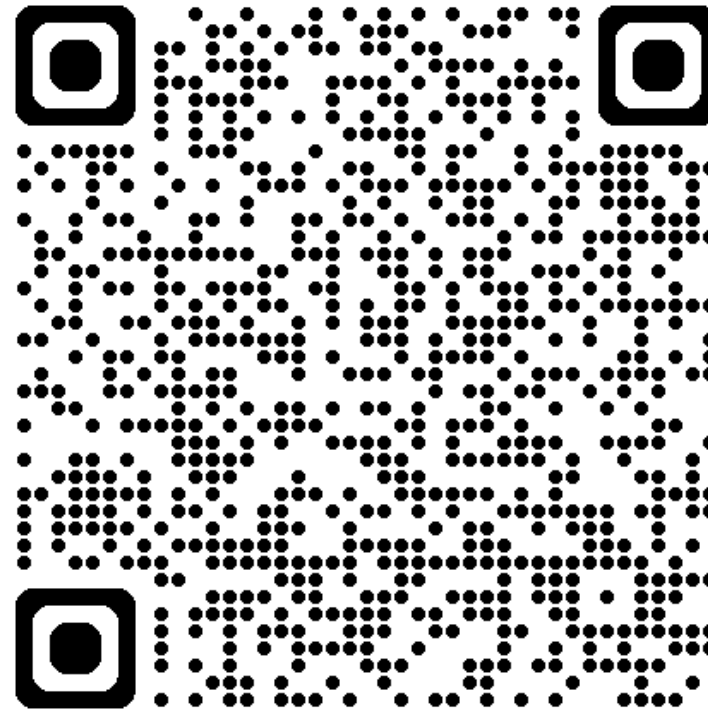
In der Praxis das Problem der ständigen Anpassung und kein Ende in Sicht

Gemeinsam in der Fachgruppe Cyber-Security des ISACA e. V. beginnt 2022 die Suche nach einer Lösung



Quelle: <https://de.wikipedia.org/wiki/User:DoenerTier82>

Worum geht es?



[Security Use-Cases – ein Katalog
– ISACA Germany Chapter e. V.](#)



Was sind Security Use-Cases?

Ein Security Use-Case beschreibt, wie ein Angriffsszenario erkannt werden soll.

Dies geschieht in Form einer technischen Sicherheitskontrolle, mit dem Ziel, auf das Angriffsszenario möglichst frühzeitig zu reagieren.



Brute-Force-
Angriffe

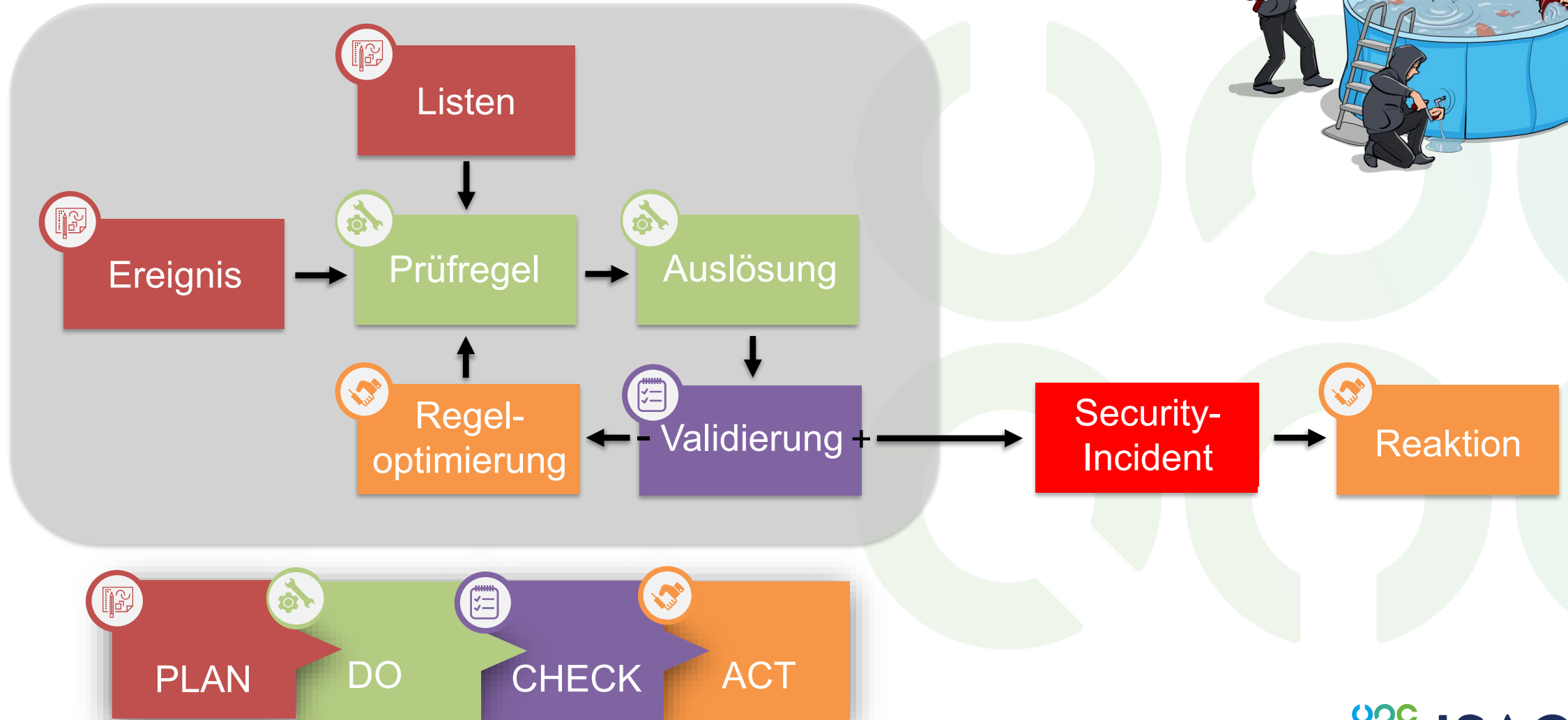
Daten-Ausleitung

Änderung von
sicherheitsrelevanten
Konfigurationseinstellungen

Löschung von
Ereignisprotokollen

...

Schema eines Security Use-Cases



Ereigniscodes

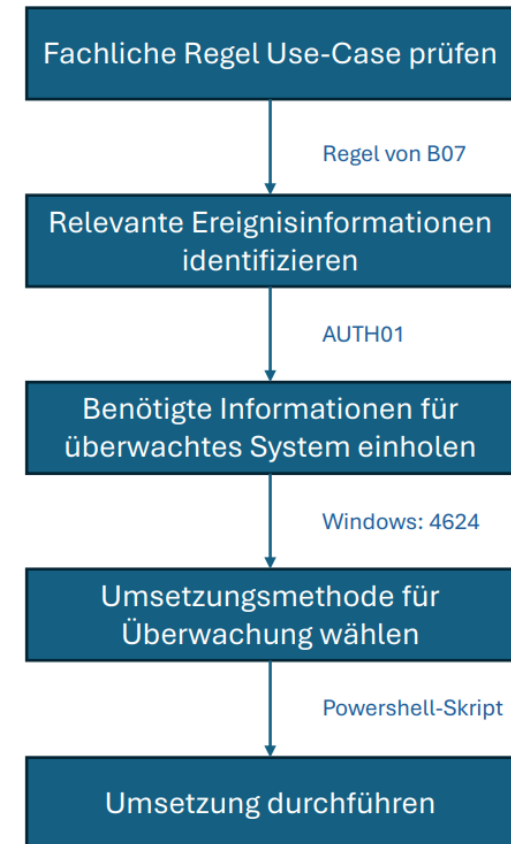
Ereigniscode	Bedeutung
ACCT01	Berechtigungsänderung an einem Benutzerkonto (bspw. Zuweisung einer anderen Rolle)
ACCT02	Berechtigungsänderungen an einer Rolle, Gruppe oder Vergleichbarem (inhaltlich, nicht Mitglieder)
ACCT03	Änderungen am Objekt eines Benutzerkontos (Beschreibungen, User Record, ...) oder einer Gruppe (Zuweisung Mitglieder, ...)
ACCT04	Anlage eines Benutzerkontos oder einer Gruppe
ACCT05	Löschung eines Benutzerkontos oder einer Gruppe
ALERT01	Warnmeldung eines Sicherheitssystems, bspw. Virenfund durch ein Antivirus-System, Warnmeldung eines IDS/IPS-Systems usw.
APP01	Ein System, eine Applikation oder Ähnliches wird gestartet
APP02	Ein System, eine Applikation oder Ähnliches wird gestoppt
APP03	Ein System, eine Applikation oder Ähnliches ist erreichbar
AUTH01	Anmeldung (»Login«) mit einem Benutzerkonto
AUTH02	Abmeldung (»Logout«) von einem Benutzerkonto
CONFIG01	Konfiguration (nicht Protokollierung) wird geändert
CONFIG02	Sicherheitsrelevante Konfiguration (nicht Protokollierung) wird geändert
CONFIG03	Konfigurationen von Regelwerken oder Inhalten (»Content«)
DATA01	Lesender Datenzugriff
DATA02	Schreibender Datenzugriff
DET01	Ein Gerät oder System wurde erkannt, typischerweise im Rahmen einer Service Discovery via Netzwerkscan
HB01	Ereignis, das anzeigt, dass noch Protokolldaten von einem Quellsystem ankommen (»Heartbeat« für die Protokollquelle)
LOCK01	Sperrung eines Benutzerkontos aufgrund fehlerhafter Anmeldung
LOCK02	Manuelle Sperrung eines Benutzerkontos
LOG01	Löschung von Protokollen
LOG02	Veränderung von Protokollen



Beispiel einer Use-Case Umsetzung

Fachliche Beschreibung der Regel des
Use-Case B07:
Verwendung spezieller Benutzerkonten

WENN
das Ereignis AUTH01.*
für System Z
mit Benutzer B
EINTRITT,
UND
(B,Z) oder (B,*) sind enthalten in <GL_SPEZIELLENUTZER_01>
UND
(B,Z) oder (B,*) ist nicht enthalten in <NL_ZUGELASSENENUTZER_01>
UND
Z ist nicht enthalten in <NL_ZUGELASSENESYSTEME_01>
DANN
löse aus

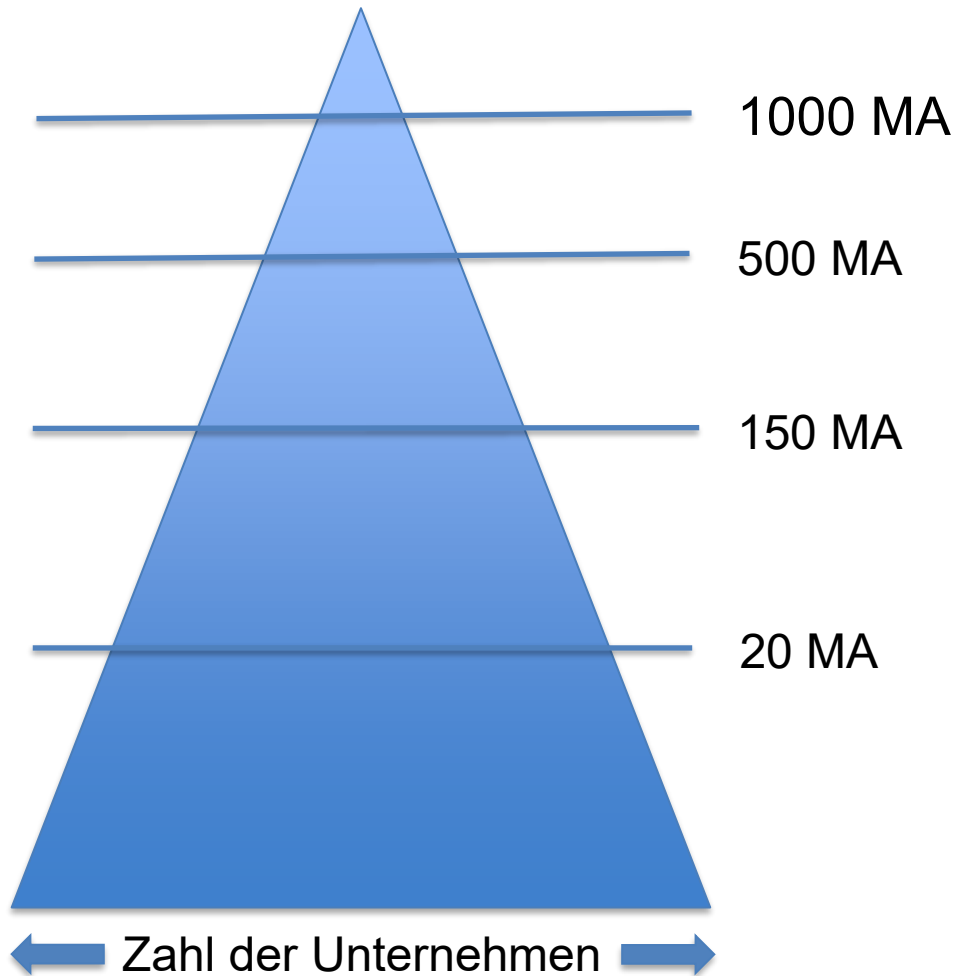


Beispiel

Powershell-Skript
Umsetzung



Wer sind unsere Zielgruppen?



Zielgruppen:

Alle

Herausforderung:

Welche Use-Cases sind für eine grundlegende Überwachung erforderlich?

Lösung:

Erstellung eines "Landschafts-Konzepts", das sich auf die Unternehmensgröße bezieht, die typischen Assetklassen berücksichtigt und somit die Ermittlung der sinnvollen Basis-Use-Cases vereinfacht.



Das Modell der Auswertungsniveaus

B01 – Löschung von Ereignisprotokollen
 B02 – Änderung von Ereignisprotokollen.....
 B03 – Änderung der Protokollierungsfunktion
 B04 – Deaktivierung der Protokollierungsfunktion...
 B05 – Änderung von sicherheitsrelevanten
 Konfigurationseinstellungen
 B06 – Deaktivierung von Sicherheitslösungen
 B07 – Verwendung spezieller Benutzerkonten
 B08 – Erkennung von Brute-Force-Angriffen
 (mehrere Benutzerkonten)
 B09 – Erkennung von Brute-Force-Angriffen

AN 1

9 Use Cases

elementar

AN 2

16 Use Cases

+ erste Info zu Netz /
Usern / Security-
Lösungen

AN 3

14 Use Cases

+ detaillierte Info zu
Netz / Usern / Security-
Lösungen / SW; SIEM

AN 4

3 Use Cases

+ Info zu schützens-
werten Daten und
Zugriffswegen, kom-
plex und spezifisch



B40 – Ungewöhnliche Netzwerkaktivität außerhalb
 der Geschäftszeiten
 B41 – Unzulässiger Zugriff auf sensible Daten
 B42 – Unzulässiger Zugriff auf System- und
 Konfigurationsdaten

Dokumentation der empfohlenen Use-Cases



Zuordnung zu den Elementen in Abbildung 1	Bezeichnung	erforderlich / empfohlen / optional	Inhalte
	ID	erforderlich	im Unternehmen vergebene ID für diesen Use-Case
	Name	erforderlich	Bezeichnung des Use-Cases
	Kurzbeschreibung mit Detektionsziel	erforderlich	Beschreibung, was detektiert werden soll
	Adressierte Risiken	erforderlich	Beschreibung, welche Risiken adressiert werden
	Verantwortliche	erforderlich	Verantwortliche für den Use-Case
	Stand	erforderlich	Datum dieser Beschreibung
	Letzte Prüfung	erforderlich	Datum der letzten Prüfung: Prüfung ob dieser Use-Case erforderlich ist, die genannten Risiken adressiert und die Detektionsziele erfüllt sind.
	Status	erforderlich	Status dieses Use-Cases, beispielsweise entwurf, freigegeben, nicht anzuwenden
Ereignis Listen	Erforderliche Informationen	erforderlich	erforderliche Informationen bzw. Daten
	Benötigte Positiv- und Negativlisten	erforderlich	Listenaufstellung mit Inhalten, soweit erforderlich
	Reaktionstyp	erforderlich	Warnmeldung, Bericht, andere ...
	Kritikalität	erforderlich	normal (1), hoch (2), sehr hoch (3)
	Dringlichkeit	erforderlich	normal (1), schnell (2), unverzüglich (3)
Regel-optimierung	Typische True-Positives (kritisch)	empfohlen	Auflistung der Arten von True-Positives, also Fälle korrekter Detektionen
	Typische True-Negatives (unkritisch)	empfohlen	Auflistung der Arten von True-Negatives, also in welchen Fällen gewollt nicht detektiert werden soll
	Typische False-Positives (unkritisch)	empfohlen	Auflistung der Arten von False-Positives, also in welchen Fällen detektiert werden könnte, obwohl das grundsätzlich nicht erwünscht ist
	Typische False-Negatives (kritisch)	empfohlen	Auflistung der Arten von False Negatives, also wenn tatsächliche Fälle nicht detektiert werden könnten
Prüfregel, Auslösung	Fachliche Beschreibung Regel	erforderlich	Fachliche Beschreibung, wie der Use-Case funktioniert
	Gruppierung	empfohlen	Nach was werden die detektierten Ereignisse bzw. erstellten Warnmeldungen gruppiert
	Optionen und Anmerkungen	optional	Ergänzungen, bspw. Sonderverhalten, Spezialfälle, besondere Art der Durchführung, Abhängigkeiten oder ähnliches
Reaktion	Reaktion	erforderlich	Welche typischen Reaktionen hier durchgeführt werden. Dies kann abstrakt ("allgemeine Detail- und Umfeldanalyse") oder konkret ("Überprüfung ob betroffenes Benutzerkonto jünger als 1 Tag ist, falls ja Aktivität ... durchführen")
	Referenz ATT&CK Techniques	empfohlen	Referenz ATT&CK Techniques und Subtechniques, siehe hier: https://attack.mitre.org/tactics/enterprise/
	Referenz BSI	empfohlen	Referenz BSI IT-Grundschutz wenn möglich
	Referenz ATT&CK Tactics	erforderlich	Die Zuordnung zu den entsprechenden ATT&CK Tactics, siehe hier: https://attack.mitre.org/tactics/enterprise/

Dokumentation der implementierten Use-Cases

Zuordnung zu den Elementen in Abbildung 1	Bezeichnung	erforderlich / empfohlen / optional	Inhalte
	ID	erforderlich	im Unternehmen vergebene ID für diese Use-Case-Umsetzung
	Name	erforderlich	Bezeichnung der Use-Case-Umsetzung
	Kurzbeschreibung mit Detektionsziel	erforderlich	Beschreibung, was diese konkrete Ausprägung detektieren soll
	Adressierte Risiken	erforderlich	Beschreibung, welche Risiken durch diese konkrete Ausprägung adressiert werden
	Verantwortliche	erforderlich	Verantwortliche für die Umsetzung
	Stand	erforderlich	Datum dieser Beschreibung
	Letzte Prüfung	erforderlich	Datum der letzten Prüfung dieser Umsetzung auf Wirksamkeit
Ereignis Listen	Status	erforderlich	Status dieser Umsetzung, typischerweise Entwurf, Produktiv, Obsolet
	Erforderliche Informationen	erforderlich	für die Umsetzung erforderliche Informationen bzw. Daten
	Benötigte Positiv- und Negativlisten	erforderlich	Listenaufstellung mit Inhalten, soweit erforderlich
	Reaktionstyp	erforderlich	Warnmeldung, Bericht, andere ...
	Kritikalität	erforderlich	normal (1), hoch (2), sehr hoch (3)
	Dringlichkeit	erforderlich	normal (1), schnell (2), unverzüglich (3)
	Priorität	empfohlen	Je kleiner, desto wichtiger. Berechnet sich grundsätzlich $P = 10 - \text{Kritikalität} * \text{Dringlichkeit}$
	Typische True-Positives (kritisch)	empfohlen	Auflistung der Arten von True-Positives, also Fälle korrekter Detektionen durch die Umsetzung
	Typische True-Negatives (unkritisch)	empfohlen	Auflistung der Arten von True-Negatives, also in welchen Fällen die Umsetzung gewollt nicht detektiert werden soll
Regel-optimierung	Typische False-Positives (unkritisch)	empfohlen	Auflistung der Arten von False-Positives, also in welchen Fällen die Umsetzung detektieren könnte, obwohl das grundsätzlich nicht erwünscht ist
	Typische False-Negatives (kritisch)	empfohlen	Auflistung der Arten von False-Negatives, also wenn tatsächliche Fälle durch die Umsetzung nicht detektiert werden könnten
	Fachliche Beschreibung Regel	erforderlich	Fachliche Beschreibung der Umsetzung
Prüfregel, Auslösung	Technische Regel	erforderlich	Technische Beschreibung (konkretes Regelwerk) der Umsetzung. Sollte ebenfalls die Frequenz, also wie oft die Regel ausgeführt wird (Echtzeit, alle 5 min, jede Stunde, ...) beinhalten.
	Auslösebedingungen	optional	Was muss getan werden, um den Use-Case auszulösen.
	Assetklassen	erforderlich	Für welche Assetklassen (Windows-Server, Firewall-System-Modell xy, ...) die Detektion in dieser Form funktioniert.
	Gruppierung	empfohlen	Nach was werden die durch die Umsetzung detektierten Ereignisse bzw. erstellten Warnmeldungen gruppiert
	Hinweise und Anmerkungen	optional	Ergänzungen zu der Umsetzung, bspw. Sonderverhalten, Spezialfälle, besondere Art der Durchführung, Abhängigkeiten oder ähnliches
	Reaktion	erforderlich	Welche typischen Reaktionen hier durchgeführt werden. Dies kann abstrakt ("allgemeine Detail- und Umfeldanalyse") oder konkret ("Überprüfung ob betroffenes Benutzerkonto jünger als 1 Tag ist, falls ja Aktivität ... durchführen")
	Referenz Use-Cases	erforderlich	Die IDs, z.B. B01, der durch diese Umsetzung abgedeckten Use-Cases sollten hier referenziert werden.
	Referenz ATT&CK Techniques	empfohlen	Referenz ATT&CK Techniques und Subtechniques, siehe hier: https://attack.mitre.org/tactics/enterprise/
	Referenz BSI	empfohlen	Referenz BSI IT-Grundschutz wenn möglich
	Referenz ATT&CK Tactics	erforderlich	Die Zuordnung zu den entsprechenden ATT&CK Tactics, siehe hier: https://attack.mitre.org/tactics/enterprise/



Standard-Bericht zum Aufbau und zur Überprüfung

Unternehmen	Beispiel GmbH
Unternehmensspezifische Risikobewertung bzgl. Assets durchgeführt?	Nein
Abgenommen am	01.02.2024
Abgenommen von	Max Mustermann, CIO

Typ	Auswertungsniveau -> v Assetklasse Use-Cases ->	1	1	1	1	1	1	1	1	1
		B01	B02	B03	B04	B05	B06	B07	B08	B09
I	Windows-Clients	x	x	x	x	x	x	x	x	x
I	Windows-Server	x	x	x	x	x	x	x	x	x
I	Antivirus	x	x	x	x	x	x	x	x	x
I	Internet-Router	1	x	x	x	x	x	x	x	x
I	Mailserver	x	x	x	x	x	x	x	x	x
I	WebProxy	x	x	x	x	x	x	x	x	x
I	Firewall, basic (bis Layer 3)	x	x	x	x	x	x	x	x	x
I	Non-Windows-Server	x	x	x	x	x	x	x	x	x
I	Webserver	x	x	x	x	x	x	x	x	x
I	Active Directory / LDAP	x	x	x	x	x	x	x	x	x
I	WLAN-Router	x	x	x	x	x	x	x	x	x
I	NTP-Programm / - Server	x	x	x	x	x	x	x	x	x
I	Remote-Zugang/VPN	x	x	x	x	x	x	x	x	x
I	eigener DNS-Service	x	x	x	x	x	x	x	x	x
I	Netzwerkdrucker	x	x	x	x	x	x	x	x	x
I	Zentrale Laufwerke	x	x	x	x	x	x	x	x	x
...	--- (weitere)	-	-	-	-	-	-	-	-	-

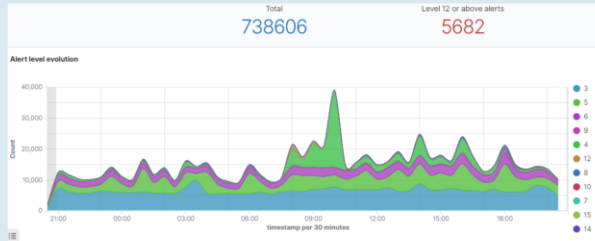


X umgesetzt, keine Einschränkung

eingeschränkt oder nicht umgesetzt, ID (1, 2, ...) mit Begründung und ggf. Risikobewertung

1 nicht umgesetzt, weil die Logs in der Appliance gekapselt sind. Risikoakzeptanz: ID xxxx-yyy

Security Use-Cases mit WAZUH SIEM



Wazuh-Blog
Alles rund ums Thema Wazuh

Datenschutz
Anleitungen

Use-Cases

Erfahren Sie, wie Unternehmen mit dem ISACA Use-Case-Katalog Cybersecurity-Strategien strukturieren, Bedrohungen frühzeitig erkennen und generische Use-Cases effizient in Wazuh umsetzen können.

Strukturierte Cybersecurity für moderne Unternehmen

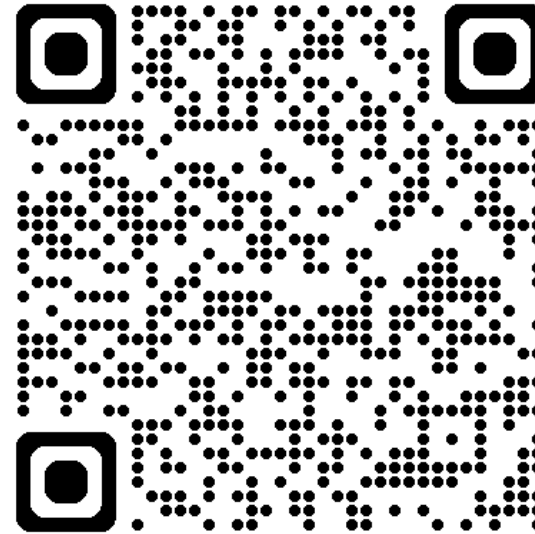
Cyberangriffe werden immer komplexer – und die Herausforderung, Sicherheitsvorfälle effizient zu erkennen, wächst täglich. Der ISACA-Leitfaden „Use Case Katalog“ bietet hier eine wertvolle Grundlage: Er beschreibt praxisorientierte Use-Cases zur Erkennung, Prävention und Analyse von IT-Sicherheitsvorfällen – unabhängig von bestimmten Tools oder Herstellern.

Unternehmen profitieren besonders vom generischen Ansatz, der die Übertragbarkeit der Use-Cases auf Plattformen wie Wazuh, Splunk oder Microsoft Sentinel ermöglicht. Damit wird der Leitfaden zu einem mächtigen Werkzeug für alle, die Cybersecurity strategisch und nachhaltig denken.

Was steckt hinter dem ISACA Use-Case-Katalog?

Der Leitfaden ist eine praxisnahe Anleitung zur Entwicklung, Bewertung und Umsetzung von Security-Use-Cases. Er beschreibt, wie aus generischen Sicherheitsanforderungen konkrete SIEM-Regeln entstehen – und stellt dazu ein einheitliches Modell bereit.

Den ISACA Katalog findet man [hier](#).



<https://wazuh-blog.max-it.de/anleitungen/use-cases/>

