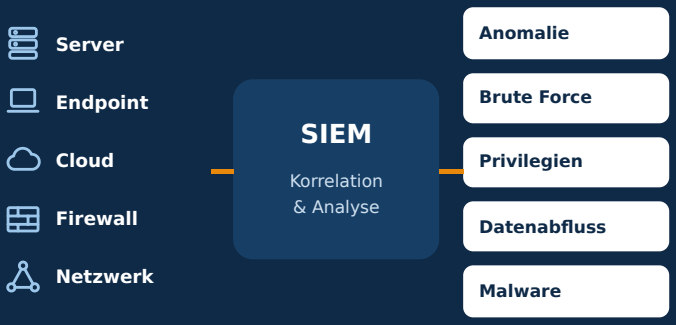
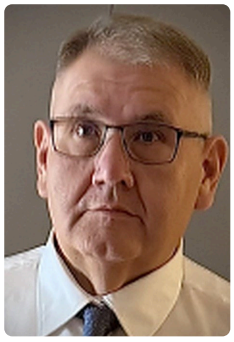
SIEM USE-CASE-SCHULUNG

Angriffserkennung nachweisbar schulen

Security Use-Cases verstehen, anwenden und prüfbar dokumentieren.

Use-Cases zur Erkennung von Anomalien und Angriffen





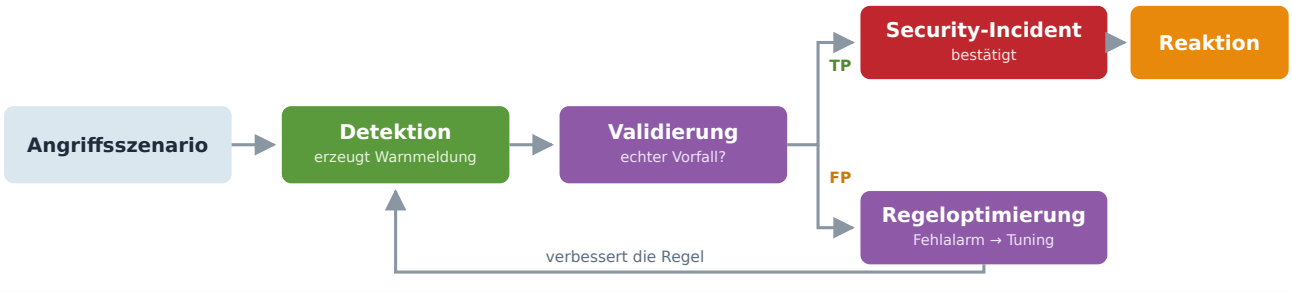
Heinrich Markus Schulte
IT-Auditor · Sachverständiger

42 Security Use-Cases

An1–An4 · L01–L05 · MITRE ATT&CK®

Herstellerneutral. Praxisnah. Audit-fähig.

Angriffe erkennen. Use-Cases steuern. Wirksamkeit nachweisen.



Abdeckung statt Bauchgefühl
Welche Angriffe erkennen Sie heute – und welche nicht? Die Schulung macht das messbar.

Pflicht sauber belegt
Angriffserkennung nach § 31 Abs. 2 BSIG und DORA Art. 10 nachvollziehbar dokumentieren.

Aus der Praxis
Steckbriefe, Regelsprache und Logcodes, die der Betrieb morgen anwenden kann.

42	63	61	~4,5 h	75 %	DE + EN
Use-Cases	Lektionen	Lernkontrollen	Lernzeit	Bestehen	Sprachen

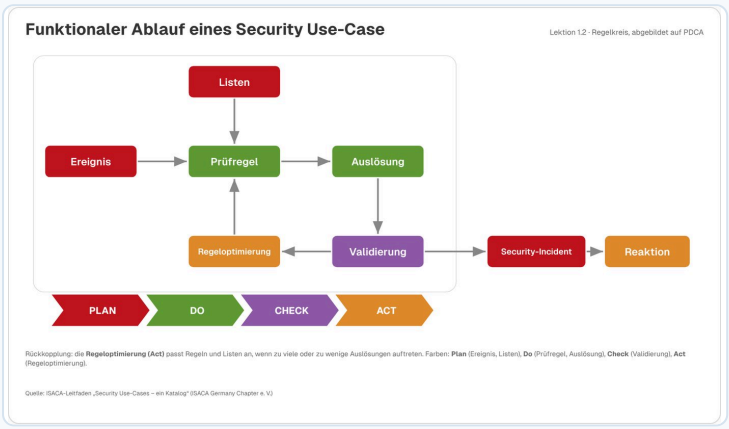
Testzugang oder Demo anfragen

Schulungsseite öffnen

12 Monate Zugang einschließlich Updates · Deutsch und Englisch · DSGVO-freundlich, ohne Werbe-Tracker

Angriffserkennung ist kein Tool-Thema.

Warum Security Use-Cases Governance, Betrieb und Audit verbinden müssen



Funktionaler Ablauf eines Security Use-Cases – von Ereignis und Prüfregel über Auslösung bis zur Reaktion, im PDCA-Zyklus.

Ein SIEM allein erkennt noch keinen Angriff. Entscheidend ist, welche Ereignisse überwacht werden, wie Regeln aufgebaut sind, welche Ausnahmen gelten und ob die Wirksamkeit nachvollziehbar nachgewiesen wird.

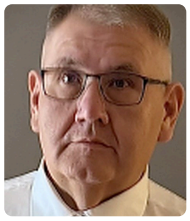
Die Schulung übersetzt den systemunabhängigen Ansatz des Leitfadens „Security Use-Cases – ein Katalog" des ISACA Germany Chapter e. V. in einen konkreten Lern- und Nachweisprozess. 42 Use-Cases werden nach Auswertungsniveau An1 bis An4 eingeordnet und mit den IT-Landschaften L01 bis L05, MITRE ATT&CK® und BSI IT-Grundschutz verknüpft.

Für den IT-Betrieb heißt das: Ereigniscodes, Regelsprache, Positiv- und Negativlisten, Tuning und Steckbriefe werden greifbar. Für Governance und Audit entsteht eine belastbare Sicht auf Abdeckung, begründete Abweichungen, Maßnahmen und Rezertifizierung.

RECHTSRAHMEN & BEZÜGE

§ 31 Abs. 2 BSIG · **§ 30 BSIG** · **DORA Art. 10** · **ISO/IEC 27001 A 8.16** · **BSI IT-Grundschutz** · **MITRE ATT&CK®**

Keine Zertifizierung und kein Prüftestat. § 31 Abs. 2 BSIG verpflichtet Betreiber kritischer Anlagen zum Einsatz von Systemen zur Angriffserkennung.



PRÜFERBLICK

Heinrich Markus Schulte
IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

> *In Prüfungen sehe ich selten fehlende Technik – aber oft fehlende Begründung, warum genau diese Use-Cases laufen und andere nicht.*

GOVERNANCE

Use-Cases nach Landschaft und Niveau auswählen, Abdeckung steuern, Berichte für Management und Audit aufbauen.

BETRIEB & SOC

Ereigniscodes, Regeln, Listen und Tuning mit der Windows-/Linux-Logcode-Referenz praktisch nutzen.

AUDIT & NACHWEIS

Abdeckungsmatrix, Prüfpunktelogik, Maßnahmenplan und eine online prüfbare Bescheinigung.

METHODIK

42 Use-Cases, An1–An4, L01–L05 und MITRE ATT&CK® systemunabhängig verbunden.

Fragen, die Aufsicht und Prüfer stellen

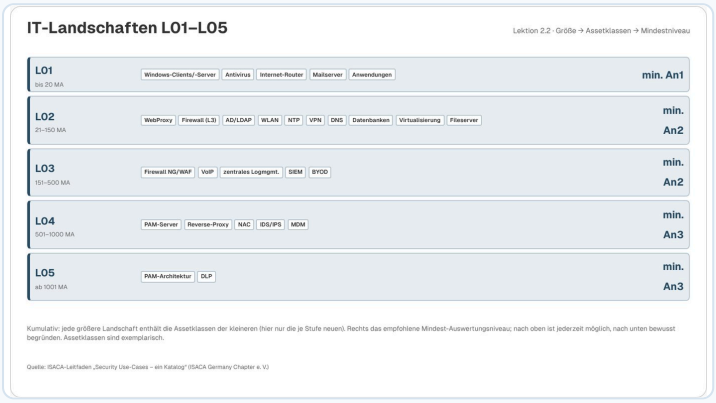
- Welche Use-Cases sind für Ihre IT-Landschaft das Minimum – und warum?
- Wie wird die Wirksamkeit der Regeln geprüft und dokumentiert?
- Welche ATT&CK®-Taktiken sind nicht abgedeckt, und wer hat das akzeptiert?
- Wie oft werden Regeln, Listen und Ausnahmen überprüft?

Auswählen · Abdecken · Regeln bauen · Tunen · Nachweisen · Verbessern

SIEM USE-CASE-SCHULUNG

Ablauf, Nutzen und Pakete

Vom systemunabhängigen Use-Case-Katalog zum wirksamen Betriebs- und Auditprozess



IT-Landschaften L01–L05 mit dem jeweils empfohlenen Mindest-Auswertungsniveau.

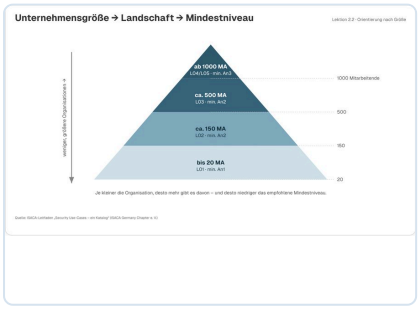
Was Sie lernen

1. **Grundlagen & Methode**
   Use-Case-Begriff, Ablauf, Protokolle zentralisieren und korrelieren
2. **Niveaus & Landschaften**
   An1–An4, L01–L05, Auswahl und Priorisierung
3. **Regeln, Listen, Tuning**
   abstrakte Ereignisse, Regelsprache, True/False Positive
4. **42 Use-Cases B01–B42**
   Steckbriefe mit Ereignis, Prüfregel, Auslösung, Reaktion
5. **MITRE ATT&CK® & BSI**
   Taktik-Abdeckung, Navigator-Layer, IT-Grundschutz-Bezüge
6. **Nachweis & Audit**
   Abdeckungsmatrix, Abweichungen, Maßnahmen, Bericht

FÜR WEN **IT-Governance · ISB · Auditoren · IT-Betrieb · SOC · Risikomanagement · Geschäftsleitung**

IHR MEHRWERT

- **Abdeckung steuern**
  Use-Cases nach Landschaft und Auswertungsniveau priorisieren.
- **Betrieb befähigen**
  Regeln, Listen und Tuning direkt in die Praxis übertragen.
- **Audit-fähig**
  Abdeckungsmatrix und Maßnahmen nachvollziehbar dokumentieren.
- **Herstellerneutral**
  Methodik statt Toolwerbung – übertragbar auf jedes SIEM.



Größe → Landschaft → Niveau



Bericht: Assetklassen × Use-Cases



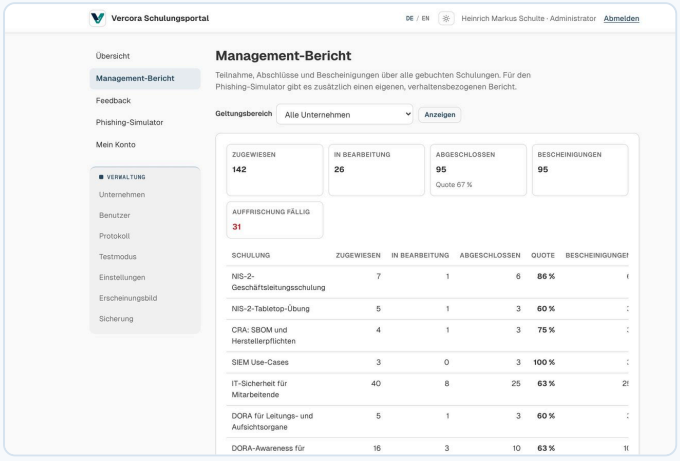
Ereigniscodes → Logcodes

PAKET & BUCHUNG Add-on zum Abo oder als Einzelplatz mit 12 Monaten Zugang · inklusive Bericht- und Audit-Vorlagen, ATT&CK®-Referenz und Logcode-Referenz mit über 400 Audit-Events.

So läuft es ab

Vom Zugang bis zum belastbaren Nachweis der Angriffserkennung

Im Vercora Schulungsportal inklusive



- **Teilnehmerverwaltung:** Plätze buchen, Personen anlegen, persönliche Einladungslinks ohne Passwort
- **Fortschritt & Management-Bericht:** Teilnahme, Abschlüsse und fällige Auffrischungen als PDF für die Leitung
- **Nummerierte Bescheinigung:** PDF mit Online-Echtheitsprüfung, Protokoll und eigenem Nummernkreis
- **Wiederholungsintervall:** je Schulung 6, 12, 24 oder 36 Monate – das Portal zeigt, wann nachgeschult wird
- **Ihr Erscheinungsbild:** auf Wunsch mit Ihrem Logo und Ihrer Farbe – auch auf Bescheinigung und Bericht
- **Sicher & datensparsam:** Anmeldung mit zweitem Faktor, Hash-Ketten-Protokoll, keine Werbe-Tracker

Der Schulungsprozess im Überblick

1 Buchen
Einzelplatz, Lizenz oder Add-on zum Abo

2 Lernen
digitaler Lernpfad mit 63 Lektionen

3 Anwenden
Use-Cases, Regeln und Tuning übertragen

4 Nachweisen
Bescheinigung und Abdeckungsmatrix

5 Auffrischen
12 Monate Updates, Intervall frei wählbar

Was Sie erhalten

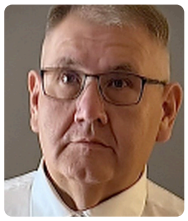
42 Use-Cases
vollständiger Katalog B01–B42 als Steckbriefe

Referenz-Werkzeuge
MITRE ATT&CK®-Referenz & Navigator-Layer, BSI-Bausteine, 400+ Windows-/Linux-Audit-Events

Audit-Dokumente
Abdeckungsmatrix, Prüfpunkte, Abweichungen und Maßnahmenplan als Vorlage

Prüfbarer Abschluss
75 % Bestehensgrenze, nummerierte, online verifizierbare Bescheinigung

PRÜFERBLICK



Heinrich Markus Schulte

IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

Angriffserkennung überzeugt im Audit erst, wenn Auswahl, Regel und Wirksamkeit lückenlos belegt sind.

Demo oder Testzugang anfragen

itschulte.de/schulungen.html

Sachverständigenbüro Schulte
Grünberger Weg 9 · 40627 Düsseldorf · +49 211 93375777 · sachverstaendiger@itschulte.de