Qualitätsmerkmale zur Prüfung, Auswahl und Steuerung von IT-Dienstleistern zur operativen IT-Sicherheit

finanz informatik

Über mich

Desiree Sacher-Boldewin

- Fachberater für Zentrale Operative IT Sicherheitsarchitektur @ Finanz Informatik
- 10+ Jahre Erfahrung in der Finanz Industrie als IT Sicherheits-Engineer & Security Analyst

Finanz Informatik

- Zentraler IT Dienstleister und Digitalisierungspartner der Sparkassen-Finanzgruppe
- 32k Server / 324k Systeme, inkl. Selbstbediensysteme

Haftungsausschluss

Die hier geäußerten Meinungen und Ansichten sind meine eigenen und stellen nicht die Meinung meines Arbeitgebers dar

finanz informatik

Ziel & Warum?

Nachhaltige Sicherheit mittels **intelligenter Prozesse**, sowie **effizienten Arbeitsabläufen und Erkennungsfähigkeiten**

Intelligente Prozesse - Warum?

- Anleiten von Nachwuchstalenten, damit sie Denkweisen und Zusammenhänge verstehen und lernen die richtigen Fragen zu stellen

Effiziente Arbeitsabläufe – Warum?

- Verhinderung von “Bore-out” und Abstumpfung von Mitarbeitern
- Optimale Nutzung interner Ressourcen

  → Wirtschaftliche Nutzung von Zeit und Geld

Effiziente Erkennungsmöglichkeiten - Warum?

- Optimale Nutzung von Herstellerprodukten

  → Wirtschaftliche Nutzung von Zeit und Geld

Wie?
Über das strukturierte Beheben von Fehlerzuständen, so dass die Fehler nicht mehr auftreten

finanz informatik

Begriffsdefinition

Operative IT Sicherheit

Laut **Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen**[1]

Aufgaben:

- Auswerten von sicherheitsrelevanten Ereignissen (SRE)
- Protokollierung und Detektion
  - Initiale und Stetige Planung
  - Spezifikation der zentralen Protokollierungsinfrastruktur
  - Kalibrierung/Justierung der Detektoren

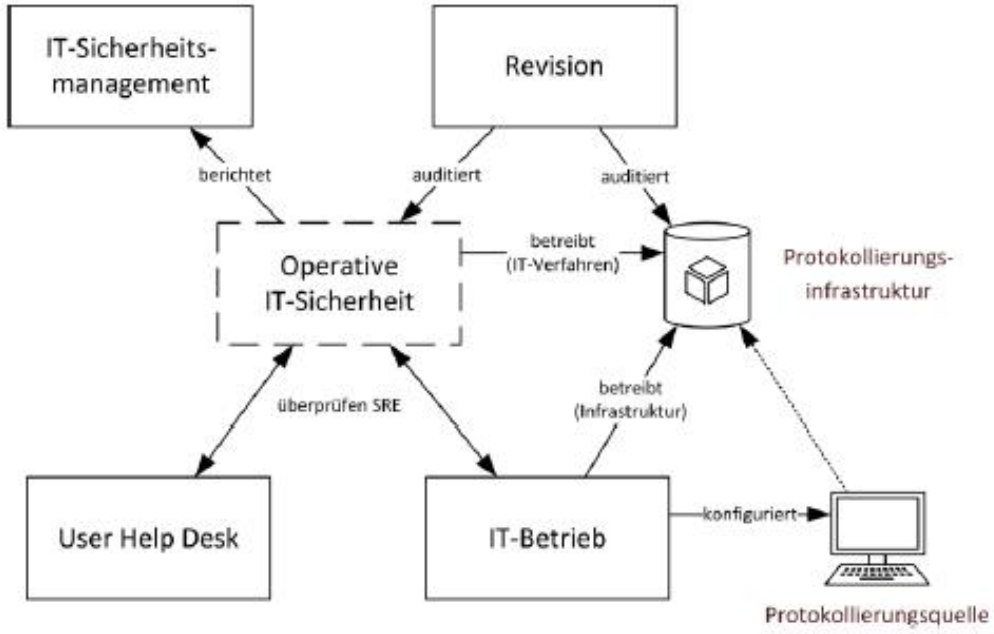


Abbildung 4: Übersicht Aufgabenbereiche

1 Quelle: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/PDCA/PDCA_node.html

Klassische Disziplinen des IT-Betrieb

Beispiele:

1. Active Directory
2. Firewall, Sprungsysteme
3. Identity & Access Management (IAM)
4. VPN Gateways, Router, Switches
5. DNS[1], NTP[2]
6. Herstellerempfehlungen, Sicherheits-Benchmarks, einspielen von Patches
7. IDS[3]/IPS[4]
8. Antivirus

[1] Domain Name System, [2] Network Time Protocol, [3] Intrusion Detection System, [4] Intrusion Prevention System

finanz informatik

Zentrale Disziplinen der Operativen Cyber Sicherheit

Konfigurationsanomalien

Sichere Konfiguration

Wird geprüft über:

- Integritätsmonitoring
- „Compliance Configuration“[1] Monitoring

Schwachstellen-management

Einspielen von „Patches“

Wird geprüft über:

- Schwachstellenscanning
- „Patch Verification“ Scan

Sicherheitsvorfalls-management

Bearbeitung von Sicherheits-ereignissen

Wird geprüft über:

- Auswertung von zentral gesammelten Logs im SIEM
- Anomalie Erkennung auf Systemen (EDR, AV)
- Anomalie Erkennung im Netzwerk (IDS/IPS, NDR)

[1] Überprüfen der Konfigurationen auf Einhaltung der Vorgabe

finanz informatik

Fehlerkategorien der Operativen Cyber Sicherheit

Konfigurationsanomalien

Integrity/Compliance Configuration Monitoring

- Rechtmäßiger Verstoß erlaubt durch dokumentierten „Change“
- Rechtmäßiger Verstoß mit fehlendem dokumentierten „Change“
- Temporäre Konfigurationsabweichung
- Konfigurationsfehler in “Baseline”
- Einschränkung in Überprüfungswerkzeug
- Test Alarm
- Unerlaubter “Change” ohne rechtmäßige Ursache
- Aktivität ohne erforderlichen “Change”

Schwachstellen-management

Verzögungsbegründung bei Patchinstallation

- Ressourcen Problem
- Kompatibilitätsproblem
- Schlechtes SLA
- Support Problem

Fehler in Schwachstellenidentifikation

- Fehlerhafte Schwachstellen-überprüfungskonfiguration
- Kontext für Ausnutzbarkeit ist nicht gegeben

Sicherheitsvorfalls-management

Sicherheitsmonitoring

- Kommunizierte administrative/Benutzer Tätigkeit
- Unangekündigte administrative/Benutzer Tätigkeit
- Log-Management-Regel-Konfigurationsfehler
- Sensor-/Endpunkt-Regel-Konfigurationsfehler
- Schlechter IOC/Regel-Vergleichswert
- Test-Alarm
- Bestätigter Angriff mit IR-Maßnahme
- Bestätigter Angriffsversuch ohne IR-Maßnahme

Ausführliche Beschreibungen sind zu finden unter https://github.com/d3sre/IntelligentProcessLifecycle/ und https://github.com/d3sre/Use_Case_Applicability

Auszug an möglichen Leistungsmesswerten Konfigurationsanomalien

KPI	Beschreibung	Zielwert	Business impact
Anzahl Konfigurationsverstöße welche durch ein “Change Prozess”[1] legitimiert wurde	Dieser Wert reflektiert die Ereignisse, welche normalerweise klassische «False Positives» entsprechen, da offizielle «Change Prozesse» korrekt befolgt wurden aber das Sicherheitsmonitoring Team (CDC/SOC) im Prozess nicht eingebunden wurde.	< 10 %	Governance Risk
Anzahl Konfigurationsfehler in der Referenzkonfiguration pro Quellsystemtyp	Dieser Wert reflektiert welche Systemkonfigurationen (oder Konfigurationsvorgaben) Verbesserungen brauchen.	< 10 %	Change and Compliance Management Risk
Anzahl von Einschränkungen in Überprüfungsprodukt gefunden	Wenn zu viele dieser Alarme ausgelöst werden, sollte das verwendete Werkzeug hinterfragt werden.	< 5 %	SOC operational risk
Anzahl Aktivitäten für welche kein “Change” notwendig war	Wahrscheinlich besteht eine Lücke zwischen dem definierten Sicherheitsverantwortungsbereich und dem Sicherheitsverantwortungsbereich welcher technisch überprüft wird.	< 5 %	Policy-operational mismatch leading to overworked SOC
Anzahl Veränderungen welche ohne formalen “Change” durchgeführt wurden	Dieser Wert dokumentiert, wie oft Änderungen an vorher kritisch definierten Parametern auf Systemen vorgenommen wurden, ohne dass diese formal zuvor in einem Change genehmigt wurden.	< 5 %	Shadow IT Administration Risk
Anzahl ungenehmigter Changes ohne legitimen Auslöser	Sehr hohe Anzahl → Sicherheitsprozesse und IT Prozesse brauchen eine dringende Überarbeitung Sehr tiefe Anzahl → Die vorhandene Konfiguration erkennt nichts oder es geschieht tatsächlich nichts	☺	Potential intrusion/ Prioritise investigation

1 Change Prozesse wie sie unter ITIL zum Beispiel für IT Prozesse empfohlen werden

Auszug an möglichen Leistungsmesswerten

Schwachstellenmanagement

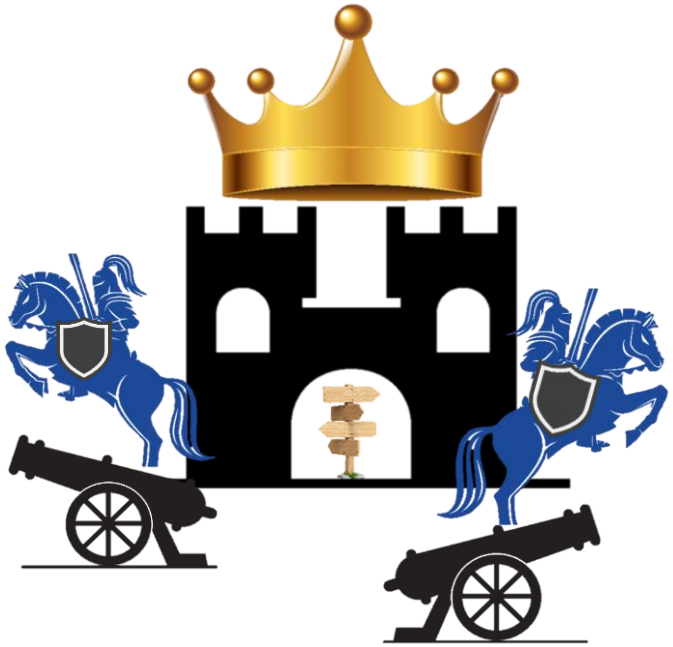
KPI	Beschreibung	Zielwert	Business impact
Anzahl verspätet eingespielter Patches auf Grund von schlechten oder unrealistischen SLAs	Wenn dieser Wert oft sehr hoch ist, kann dies in Verbindung zu spezifischen Dienstleistungen oder Anwendungen verwendet werden um die Vertragssituation anzupassen.	0	Risk Appetite and Contractual Management teams need to match expectations
Anzahl verspätet eingespielter Patches auf Grund von Ressourcenengpässen	Dieser Wert reflektiert welche Teams unterbesetzt oder überpriorisiert sind.	0	Operational Risk Management
Anzahl rechtzeitig (auf Grund der intern geltenden Vorgaben) eingespielter Patches	Dieser Wert sollte natürlich möglichst hoch sein und wird am häufigsten bereits in Berichten verwendet.	> 80 %	Cyber Risk Expectation isn't being met
Anzahl Schwachstellenschliessungen auf Grund von "Kontext für Ausnutzbarkeit ist nicht gegeben"	Eine hohe Anzahl lässt darauf schliessen, dass Sie entweder keine ehrlichen Antworten von den Fachteams kriegen oder dass die aufgesetzte Infrastruktur und die Prozesse zur Identifikation von Bedrohungen fehlerhaft sind	Keine Angabe	Potentially Poor Risk Acceptance Practices

Auszug an möglichen Leistungsmesswerten

Sicherheitsmonitoring/Sicherheitsereignisse

KPI	Beschreibung	Zielwert	Business impact
Anzahl Ereignisse aus Log-Management-Regel-Konfigurationsfehler pro Monat	Dieser Wert reflektiert die Ereignisse, welche aus Konfigurationsfehlern im SIEM ausgelöst werden, welche oft durch Sicherheitsanalysten selber erzeugt werden. Eine hohe Anzahl lässt auf eine schlechte Regelqualität schliessen, für welches mehr Ausbildung und/oder Erfahrung notwendig ist	< 10 %	SOC Operational Risk
Anzahl Ereignisse aus nicht vorher kommunizierten Administrativen Tätigkeiten	Hier zeigt sich, dass Informationsprozesse zum SOC noch nicht funktionieren oder es schwer ist für das SOC, einheitliche Verhaltensmuster im Unternehmen zu identifizieren. Ohne zentrale Steuerung und durchgesetzte einheitliche & verbindliche IT Prozesse ist das SOC hier den Alarmen ausgeliefert.	< 5%	Operational Risk management
Anzahl Ereignisse aus schlechten IOC/Regel-Vergleichswerten pro Monat	Wenn zu viele Ereignisse auf Basis schlechter Bedrohungsindikatoren oder Regelvergleichswerten ausgelöst werden, sollte die Vertrauensermessung in das Quellsystem geprüft werden	< 5%	Operational Risk management
Anzahl von bestätigten Angriffsversuchen ohne IR-Maßnahme (am Besten pro Logquelle)	Anzahl Ereignisse welche erkannt aber verhindert wurden oder für welche die vertiefte Analyse auf Grund einer Risikoabwägung nicht als relevant betrachtet wird	< 50 %	Potentially Poor Risk Acceptance Practices
Anzahl bestätigter Angriffe mit IR-Maßnahmen (am Besten pro Logquelle)	Sehr hohe Anzahl → Die Sicherheitsarchitektur sollte optimiert werden Sehr tiefe Anzahl → Die vorhandenen Regeln scheinen nichts zu erkennen oder Sie sind sicher	☺	Potential intrusion/ Prioritise investigation

Call to Action



Kontakt über Twitter: @d3sre

Mehr Informationen finden Sie unter
https://github.com/d3sre/IntelligentProcessLifecycle und
https://github.com/d3sre/Use_Case_Applicability

Stellen Sie ihrem Dienstleister kritische Fragen ☺

ANHANG

Categories Summary

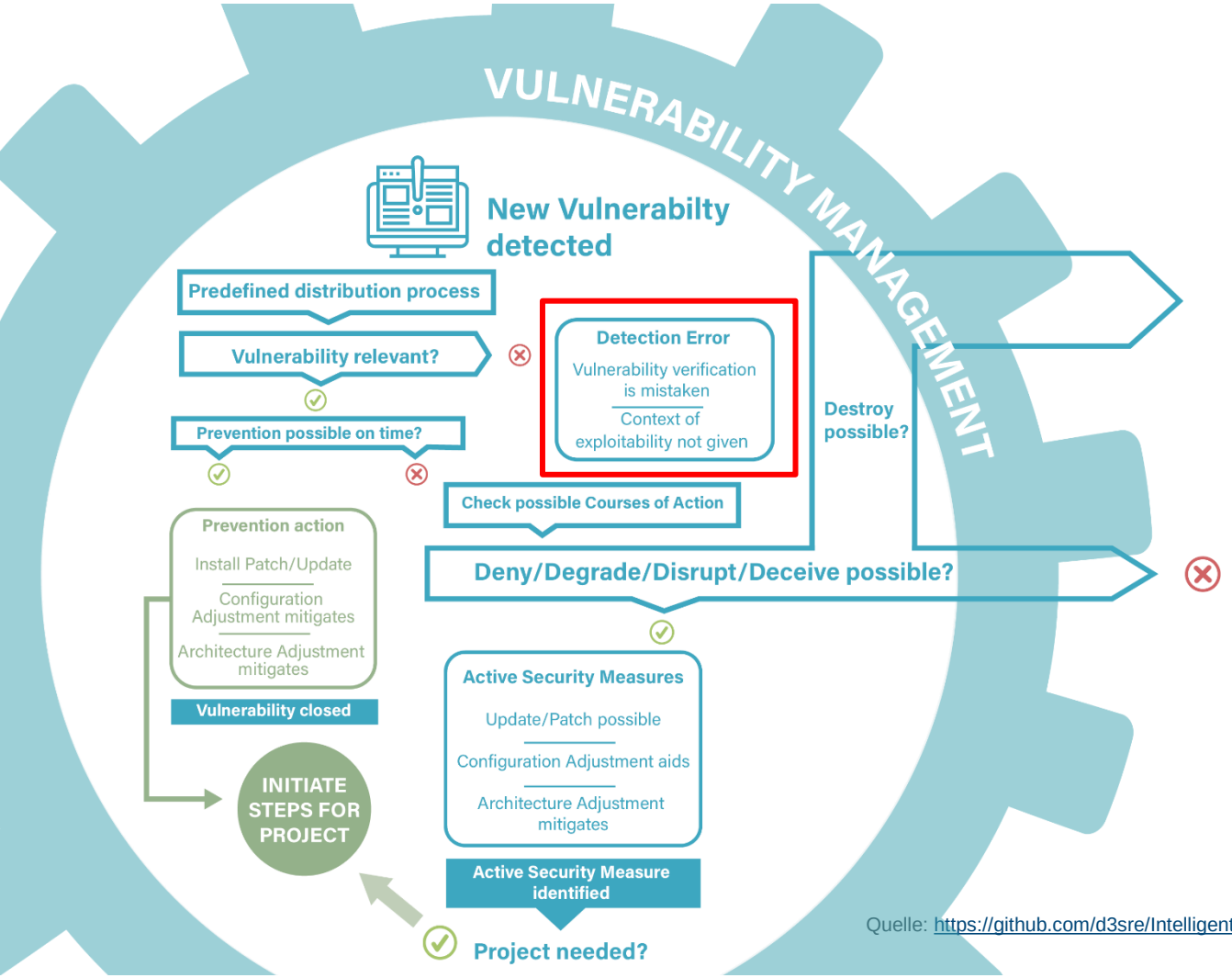
Categories	Solution Type	Alert Cause
a) Announced administrative/user action		
b) Unnannounced administrative/user action		
c) Log management rule configuration error		
d) Detection device/rule configuration error		
e) Bad IOC/rule pattern value		
f) Test alert		
g) Confirmed Attack with IR actions		
h) Confirmed Attack attempt without IR actions		

Quelle: https://github.com/d3sre/Use_Case_Applicability/blob/master/FIRST-Fingerpointing_Falsepositives-Public.pdf

finanz informatik

Category Summary

Vulnerability Management



Follow Up Actions

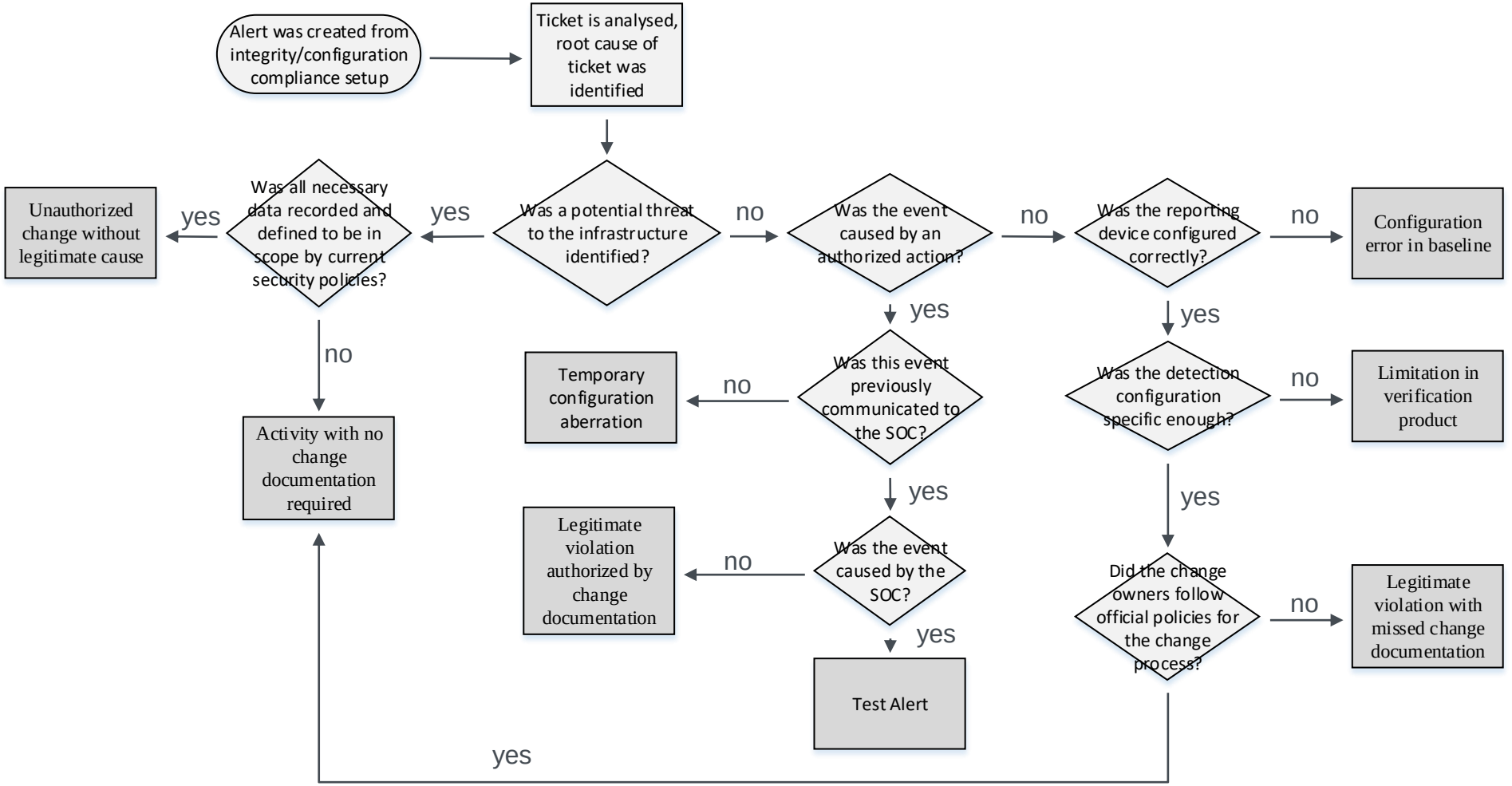
Verify your tool capabilities

Verify your security documention of specific context for threat protection measures

Quelle: https://github.com/d3sre/IntelligentProcessLifecycle/blob/main/FIRST-IntelligentProcessLifecycle-FINAL.pdf

finanz informatik

Analysing Configuration Compliance or Integrity Alerts



Quelle: https://github.com/d3sre/IntelligentProcessLifecycle/blob/main/SCS-CIDailySOCOperations-public.pdf

finanz informatik

Lessons Learned

1

Analysing security events is never a binary thing

For every alert generated there are more dimensions to rate than if this alert was a true or false positive

2

Standardised IT service management processes are the foundation for mature security operations

Change management
Incident management
Asset management
Problem management

3

Scoping of hardening documents and files needs to be regularly reviewed and included in the lifecycle

We need a „normal“ to find the anomaly

Quelle: https://github.com/d3sre/IntelligentProcessLifecycle/blob/main/SCS-CIDailySOCOperations-public.pdf

finanz informatik