How to integrate Continuous Improvement in daily SOC operations

Focus Point: Integrity and Configuration Compliance Monitoring

finanz informatik

About me

Desiree Sacher

- Security Architect @ Finanz Informatik
- 10 years finance industry experience as IT Security Engineer & Security Analyst

Finanz Informatik

- German IT service provider for the German Savings Banks Finance Group
- 32k servers / 324k devices, incl. ATMs

Disclaimer
The opinions and views expressed here are my own and do not represent the opinions of my employer

Goal & why

Sustainable security
by building **intelligent processes**,
and **efficient workflows**
and detection capabilities

Intelligent processes – why?

- guide junior analysts to think the right way to learn to ask the right questions

Efficient workflows – why?

- prevent bore out and blunting of employees
- optimal use of internal resources

→ save time and money

Efficient detection capabilities – why?

- optimal use of vendor capabilities

→ save time and money

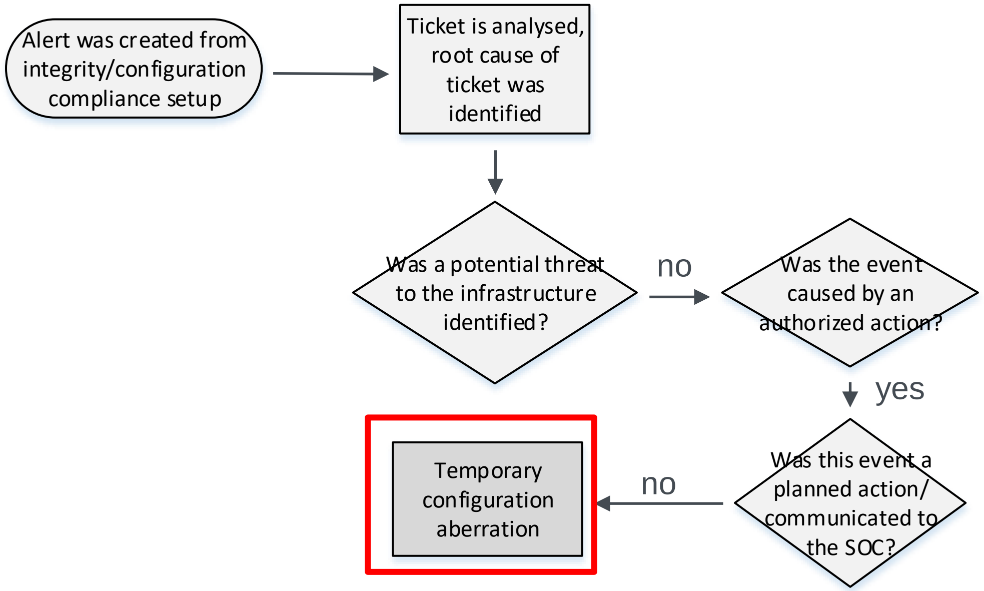
How?
By resolving the source of false alarms in a structured approach so they won´t occur again

Problems of traditional True Positives/ False Positive classification

- **Too simple as focus is "security threat for company or not"**
- **Process most often only focuses on treating symptoms instead of actual activator**
- **SOC needs to rely on accurate company data to work efficiently**

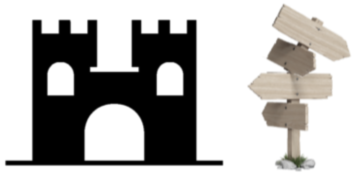
SOC becomes **operational data verification** and **technical security quality assurance center** with **cyber incident investigation & analysis capabilities**

Temporary configuration aberration



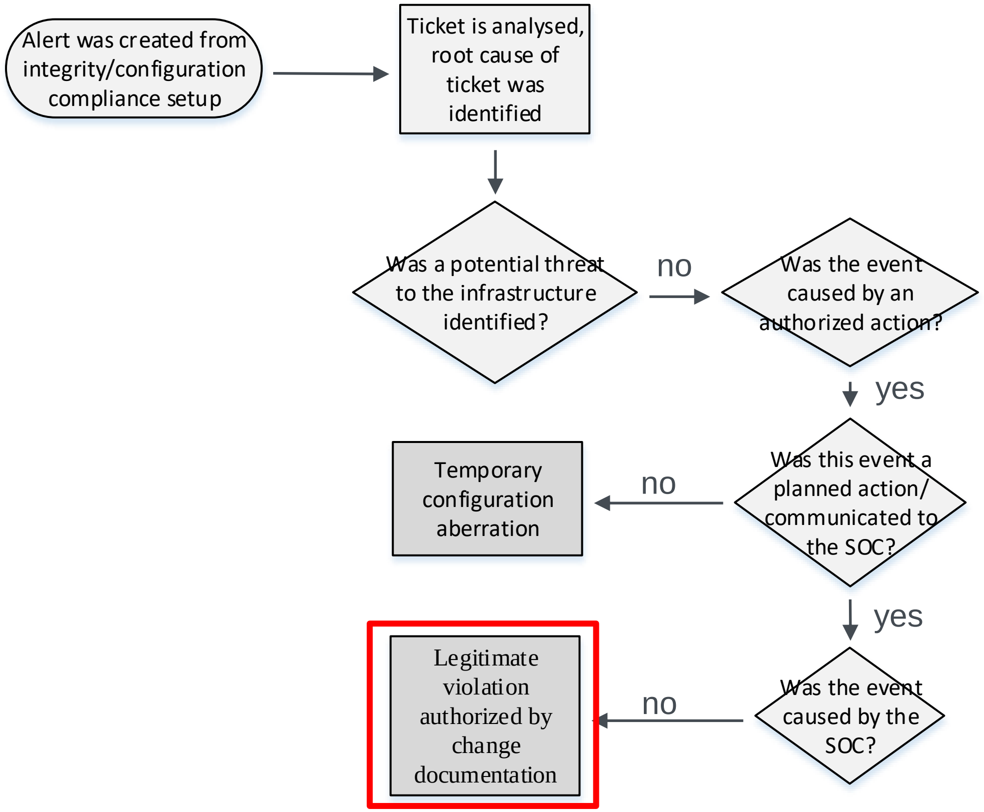
Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
no
Was the event caused by an authorized action?
yes
Was this event a planned action/ communicated to the SOC?
no
Temporary configuration aberration

- ➢ Create temporary suppression or
- ➢ Document blind stop with risk entry



This type of alert is usually unpredictable and important to track as long as the temporary setup is in place. Depending on the amount of time the emergency setup is in place, either the baseline should be adjusted or can be kept.

Legitimate violation authorized by change documentation

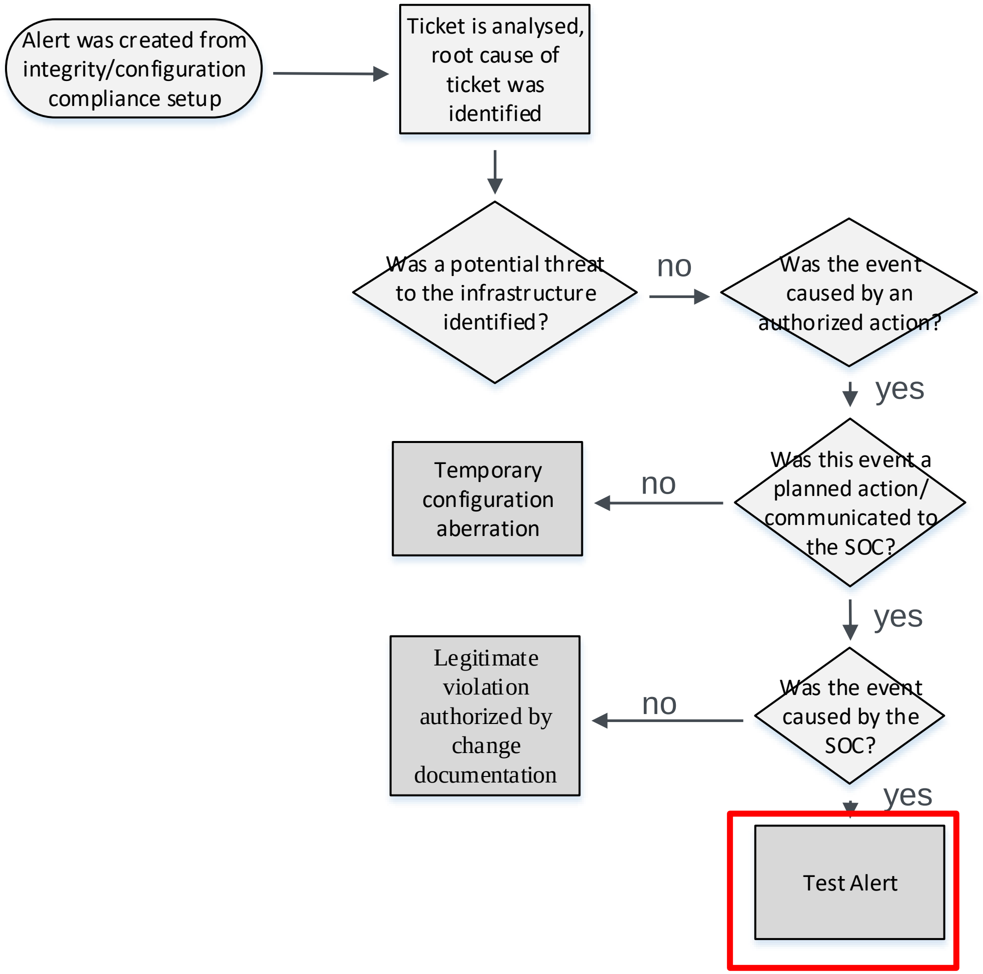


Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
no
Was the event caused by an authorized action?
yes
Was this event a planned action/ communicated to the SOC?
no
Temporary configuration aberration
yes
Was the event caused by the SOC?
no
Legitimate violation authorized by change documentation

- ➢ Adjust baseline configuration
- ➢ Reassess SOC's inclusion in the process

This type of alert is caused by changes in monitored files (on premises or in the cloud) but the SOC did not have a direct suppression associated. The update of the baseline configuration file was either not included in the process or was not possible beforehand.

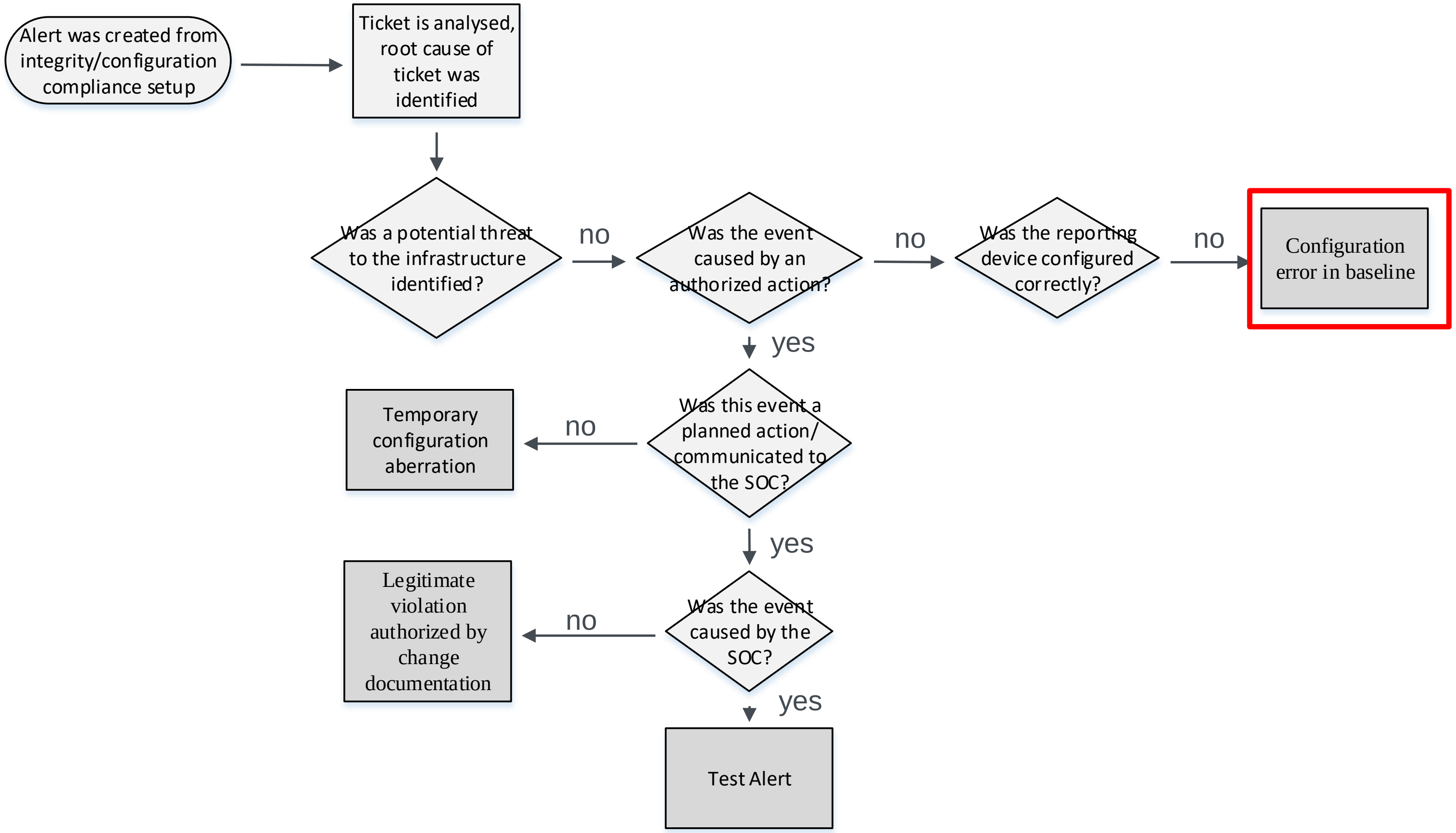
Test Alert


Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
no
Was the event caused by an authorized action?
yes
Was this event a planned action/ communicated to the SOC?
no
Temporary configuration aberration
yes
Was the event caused by the SOC?
no
Legitimate violation authorized by change documentation
yes
Test Alert

- Exclude from reports
- Important for creating trust in established setup

This alert reflects alerts created for testing purposes. This value is important for files or systems that hardly create alerts to proof operational reliability

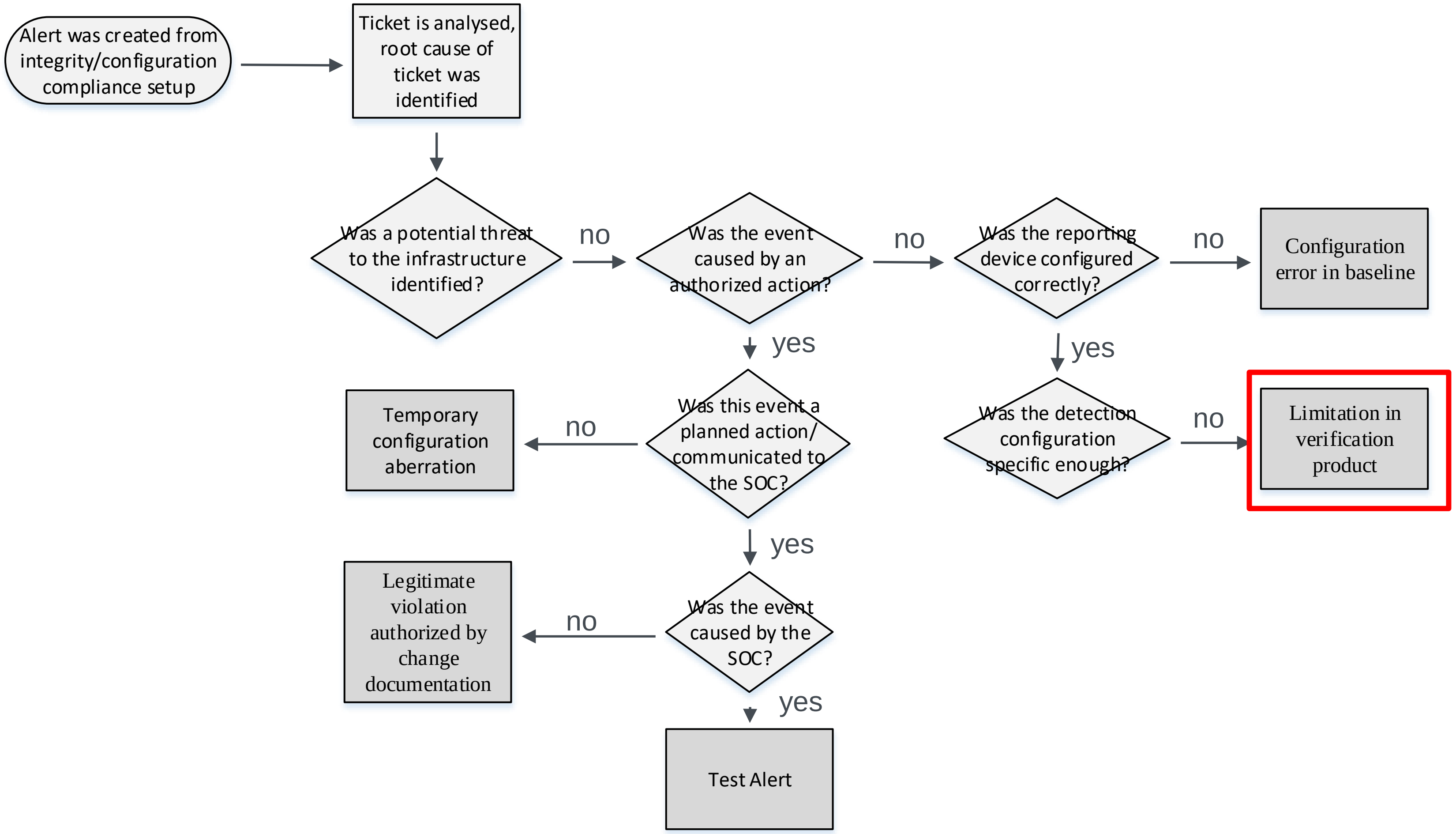
Configuration error in baseline


Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
no
Was the event caused by an authorized action?
no
Was the reporting device configured correctly?
no
Configuration error in baseline
yes
Was this event a planned action/ communicated to the SOC?
no
Temporary configuration aberration
yes
Was the event caused by the SOC?
no
Legitimate violation authorized by change documentation
yes
Test Alert

- ➢ Adjust baseline configuration
- ➢ Don’t use this value to measure SOC performance

This category reflects misconfiguration problems based on bad quality information delivered by the system engineering teams. Often appears when initially rules are configured.

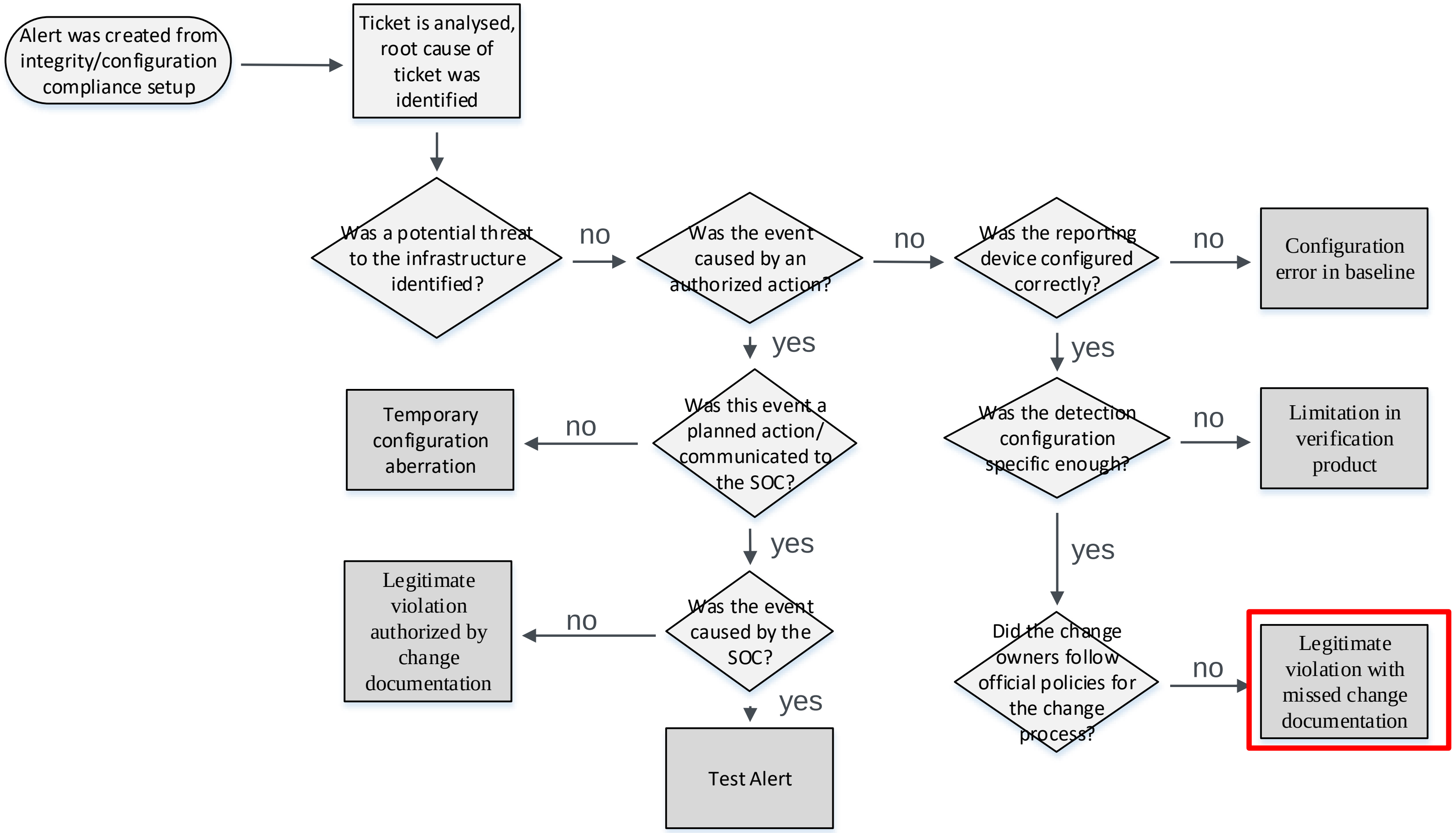
Limitation in verification product


Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
no
Was the event caused by an authorized action?
no
Was the reporting device configured correctly?
no
Configuration error in baseline
yes
yes
Temporary configuration aberration
no
Was this event a planned action/ communicated to the SOC?
Was the detection configuration specific enough?
no
Limitation in verification product
yes
Legitimate violation authorized by change documentation
no
Was the event caused by the SOC?
yes
Test Alert

- ➢ Product should be reviewed

The current product in use for configuration compliance or integrity monitoring is limited in its configuration possibilities and therefore causes bad alerts. This can only be improved by changing the product or applying extensive tricks or workarounds to the setup.

Legitimate violation with missed change documentation



Alert was created from integrity/configuration compliance setup

Ticket is analysed, root cause of ticket was identified

Was a potential threat to the infrastructure identified?

no

Was the event caused by an authorized action?

no

Was the reporting device configured correctly?

no

Configuration error in baseline

yes

Was this event a planned action/ communicated to the SOC?

no

Temporary configuration aberration

yes

Was the event caused by the SOC?

no

Legitimate violation authorized by change documentation

yes

Test Alert

yes

Was the detection configuration specific enough?

no

Limitation in verification product

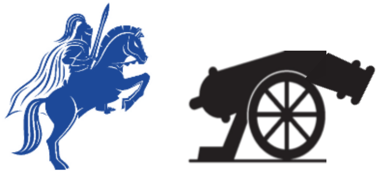
yes

Did the change owners follow official policies for the change process?

no

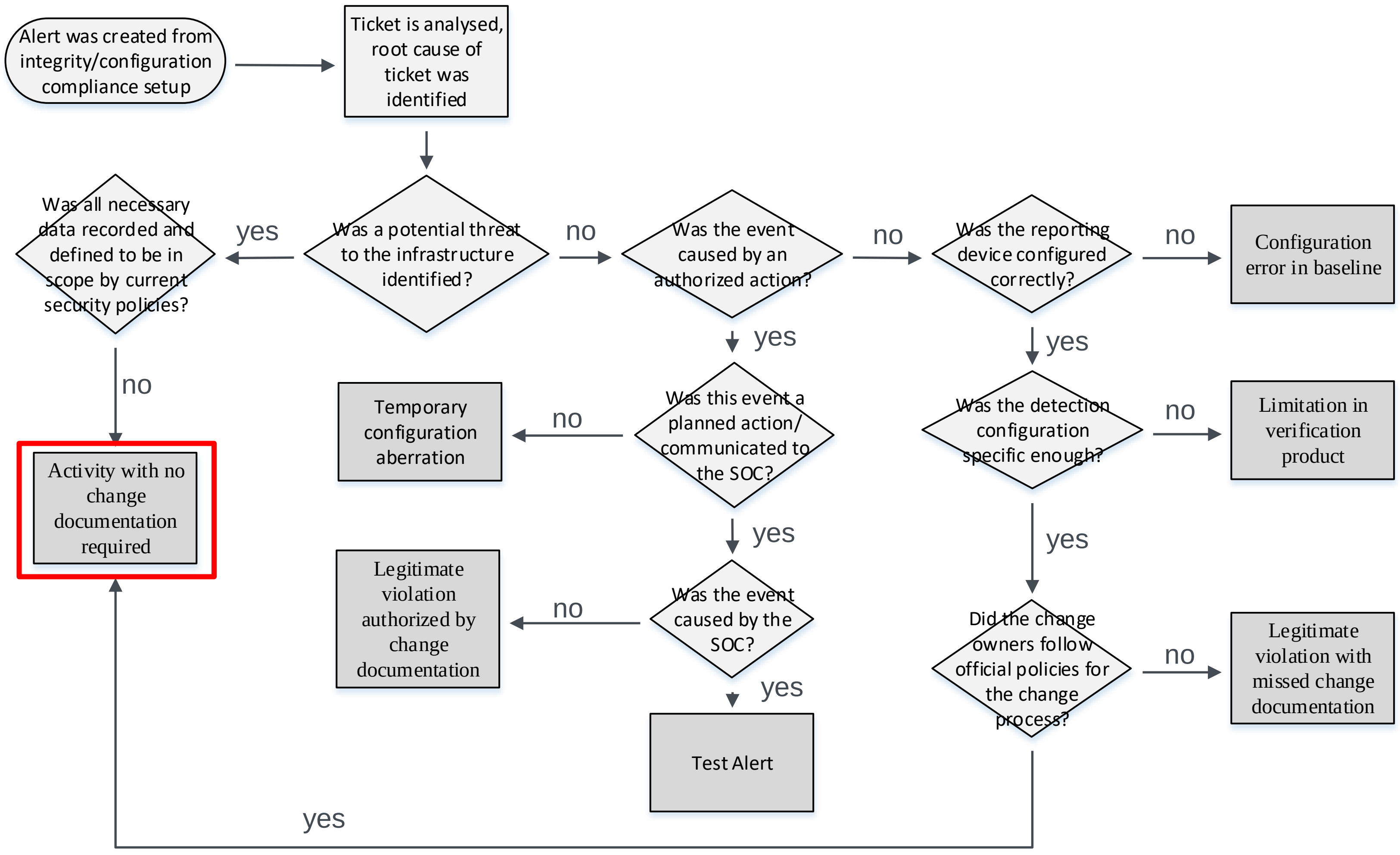
Legitimate violation with missed change documentation

- Adjust baseline configuration
- Identified «black change»



This category of alerts creates statistical values to illustrate when security and IT processes are not being correctly followed (often caused by human error).

Activity with no change documentation required



Alert was created from integrity/configuration compliance setup

Ticket is analysed, root cause of ticket was identified

Was a potential threat to the infrastructure identified?

yes

Was all necessary data recorded and defined to be in scope by current security policies?

no

Activity with no change documentation required

no

Was the event caused by an authorized action?

no

Was the reporting device configured correctly?

no

Configuration error in baseline

yes

Was this event a planned action/ communicated to the SOC?

no

Temporary configuration aberration

yes

Was the event caused by the SOC?

no

Legitimate violation authorized by change documentation

yes

Test Alert

yes

Was the detection configuration specific enough?

no

Limitation in verification product

yes

Did the change owners follow official policies for the change process?

no

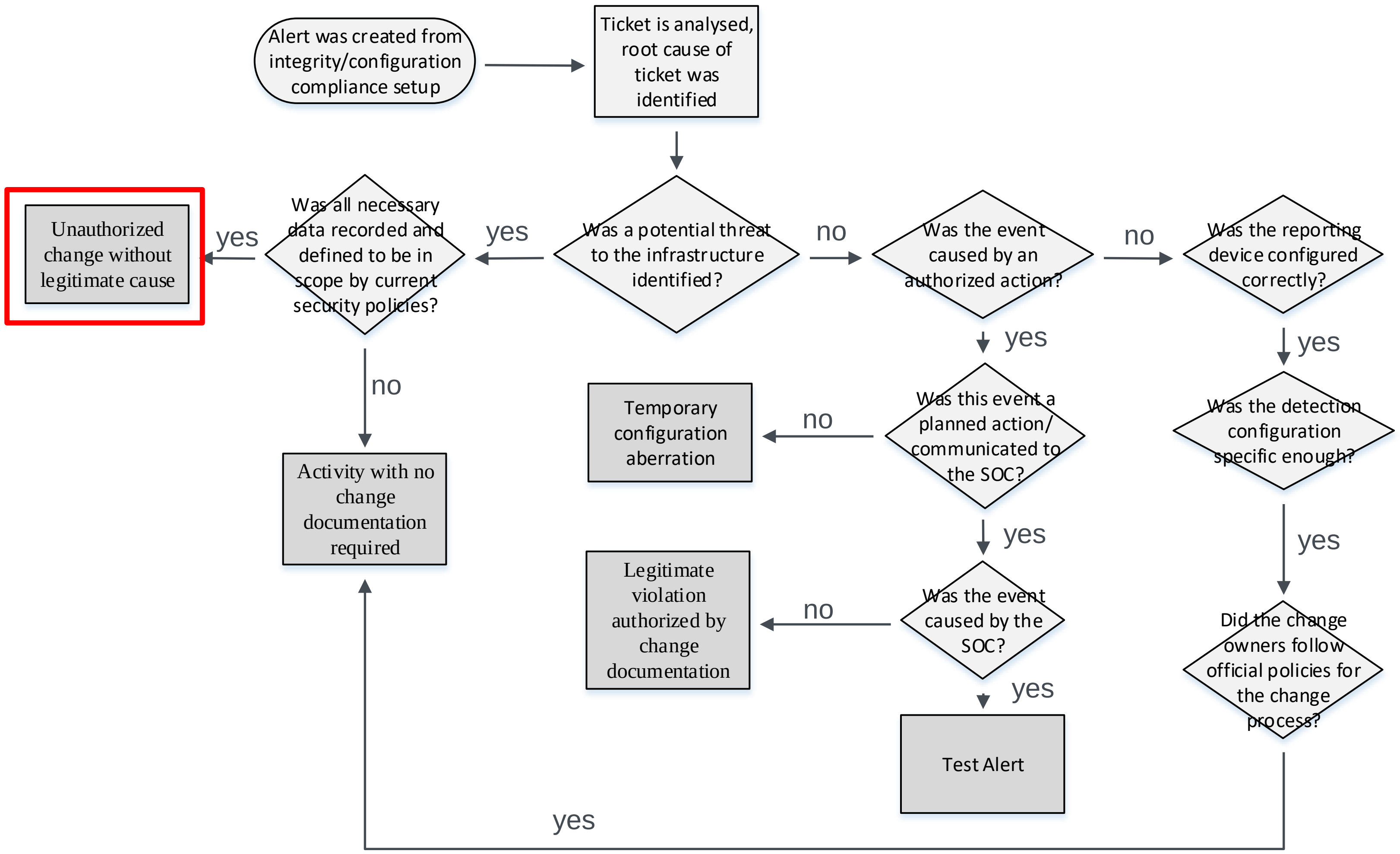
Legitimate violation with missed change documentation

yes

- ➢ Need special review by 2LoD as it reflects where currently the risk is accepted

This category documents alerts that cannot be resolved due to missing documentation and no requirement to document changes on the system or this file type. It can also have resolved alerts, but security policies do not regard these changes as critical.

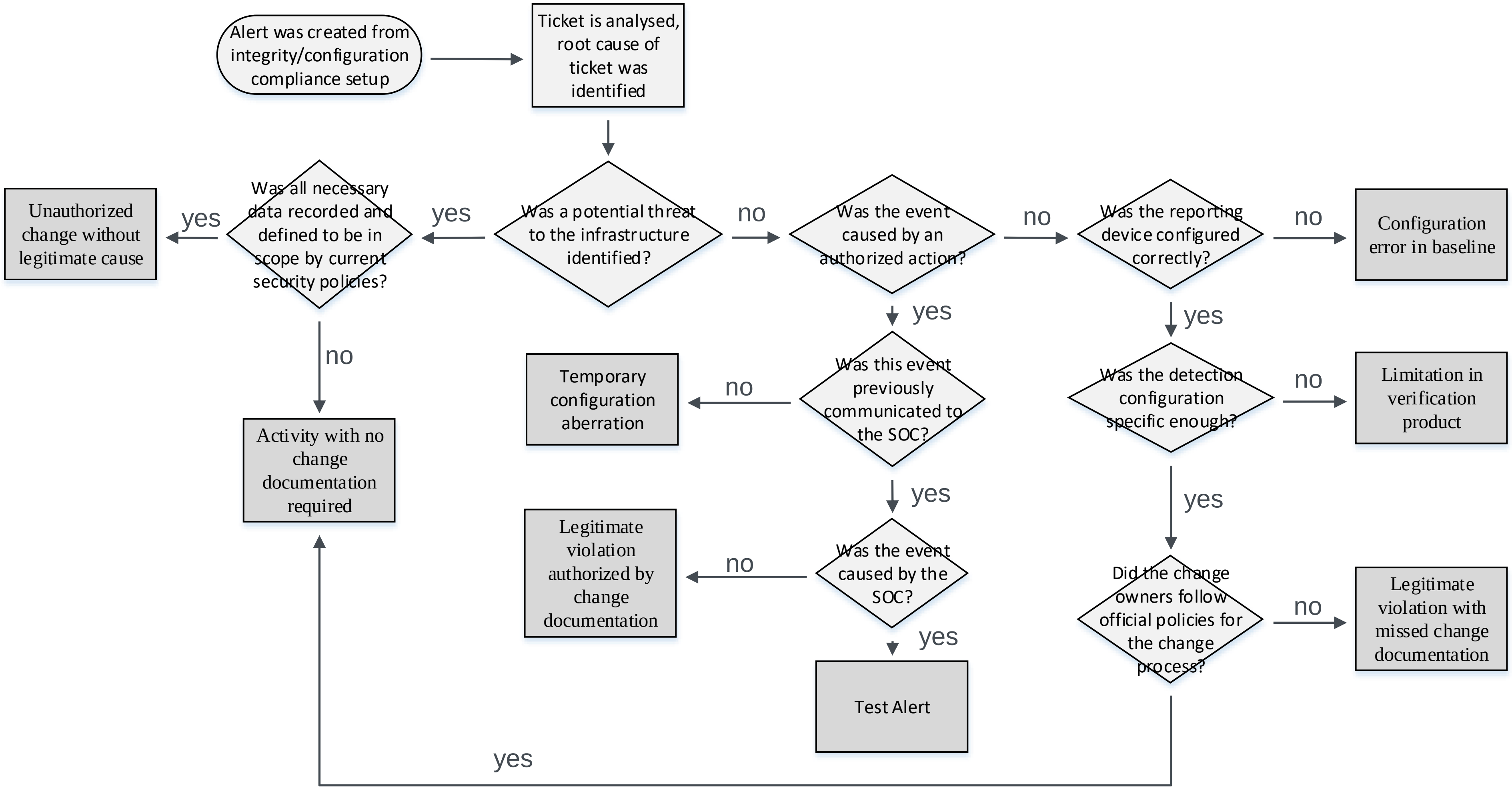
Unauthorized change without legitimate cause


Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
yes
Was all necessary data recorded and defined to be in scope by current security policies?
yes
Unauthorized change without legitimate cause
no
Activity with no change documentation required
no
Was the event caused by an authorized action?
no
Was the reporting device configured correctly?
yes
Was this event a planned action/ communicated to the SOC?
no
Temporary configuration aberration
yes
Was the event caused by the SOC?
no
Legitimate violation authorized by change documentation
yes
Test Alert
yes
Was the detection configuration specific enough?
yes
Did the change owners follow official policies for the change process?
yes

- This must be handed over to the security incident management process

This type of resolution usually causes a security incident analysis. It is of important value for threat and risk estimations. The baseline configuration is not adjusted.

Analysing Configuration Compliance or Integrity Alerts



Alert was created from integrity/configuration compliance setup
Ticket is analysed, root cause of ticket was identified
Was a potential threat to the infrastructure identified?
yes
Was all necessary data recorded and defined to be in scope by current security policies?
yes
Unauthorized change without legitimate cause
no
Activity with no change documentation required
no
Was the event caused by an authorized action?
no
Was the reporting device configured correctly?
no
Configuration error in baseline
yes
Was this event previously communicated to the SOC?
no
Temporary configuration aberration
yes
Was the event caused by the SOC?
no
Legitimate violation authorized by change documentation
yes
Test Alert
yes
Was the detection configuration specific enough?
no
Limitation in verification product
yes
Did the change owners follow official policies for the change process?
no
Legitimate violation with missed change documentation
yes

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

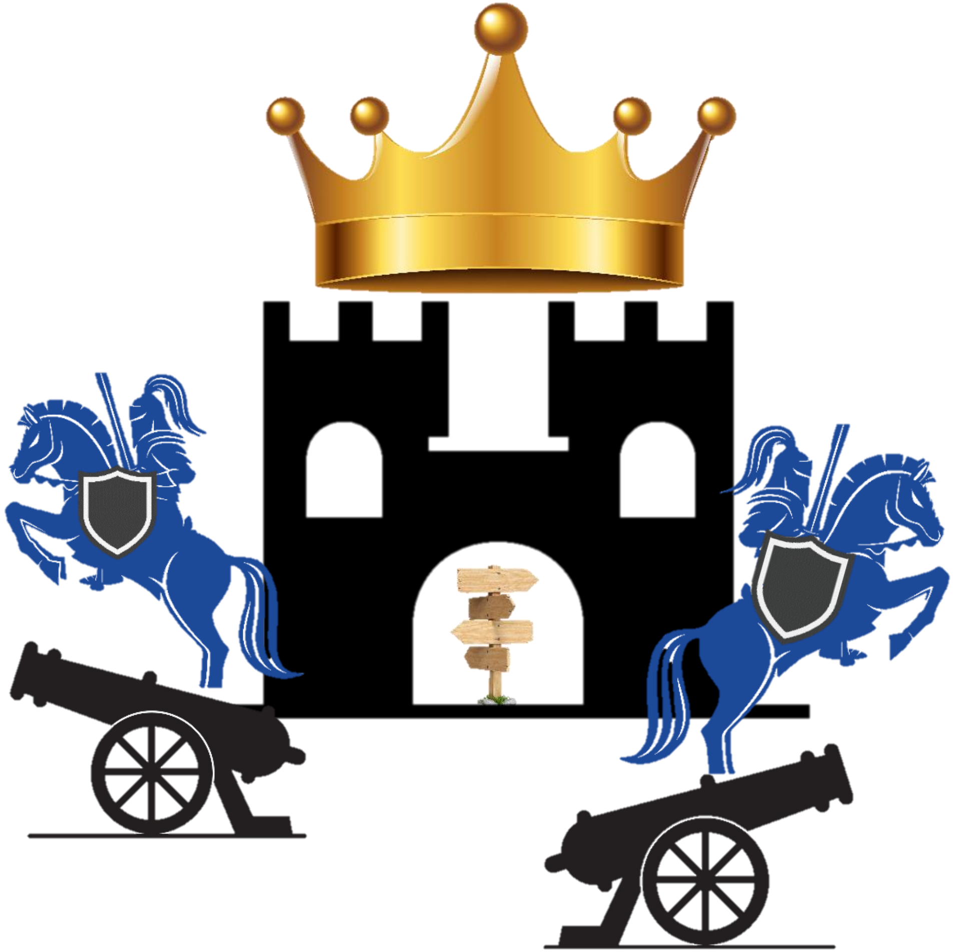
We need a „normal“ to find the anomaly

KPI Suggestions

KPI	Explanation	Target Value	Business impact
Number of legitimate violations authorized by change	This value reflects events which usually are classic false positives, where all official change processes were correctly followed but the SOC was not included in the process and therefore could not prevent the false alarm	< 10 %	Governance Risk
Number of configuration errors in baseline (best matched with Log Source Categories	This value reflects what system configurations (or even configuration templates) needs improvement.	< 10 %	Change and Compliance Management Risk
Number of Limitation in verification products found	If too many of these events were created by configurations, the causing tool should be questioned.	< 5 %	SOC operational risk
Number of activities with no change required	There seems to be a mismatch between the defined security scope and the verified security scope. Gaps should be verified	< 5 %	Policy-operational mismatch leading to overworked SOC
Number of changes without formal documentation	Number of legitimate violation with missed change documentation is highlighting where the SOC had no chance of automating false alerts, as well as where employees are not complying to formal processes.	< 5 %	Shadow IT Administration Risk
Number of unauthorized changes without legitimate cause	Very high numbers → Security process and IT process integration needs rework Very low numbers → The configurations aren‘t detecting or you are safe	☺	Potential intrusion/Prioritise investigation

Call to Action

➢Request field to be added to your workflow platform



- Twitter: @d3sre 🐦
- More information on technical impementation can be found on https://github.com/d3sre/IntelligentProcessLifecycle