31ST ANNUAL FIRST CONFERENCE

EDINBURGH
JUNE 16-21
2019

Finger-pointing False Positives:

How to better integrate Continuous Improvement into Security Monitoring

Desiree Sacher

About me

Desiree Sacher

- SOC 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

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**

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

Categories Summary

Categories	Solution Type	Alert Cause
a) Announced administrative/user action	🐎	🪧
b) Unannounced 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	👑	🛡

SOC internal optimizable incidents

Announced administrative/user action

- The process to communicate administrative activities or special user actions was in place and working correctly. Internal sensors are working and detecting privileged or irregular behaviour. No suppressions were added by the SOC.

Examples:

- Detected port scan can be correlated to a previously communicated penetration test.
- Support connection with administrative privileges was detected on a user device with default privilege.

Process/knowledge problem

- Update suppressions for announced actions
- Verify if rule is actually meaningful

Problems that might indicate lack of knowledge/education in a SOC or organisational structure difficulties

SOC internal optimizable incidents

Log management rule configuration error

- This category reflects false alerts that were raised due to configuration errors in the central log management system, often a SIEM, rule.

Example:

- Analysis of alerts for command and control traffic IPs shows connection to a multihoster system, where the actual URL accessed was not compromised.

Configuration problem

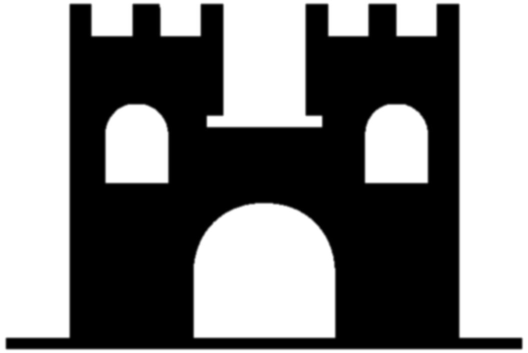
- SIEM rule correction needed

Problems that might indicate lack of knowledge/education in a SOC or organisational structure difficulties

Company optimizable incidents

Unannounced administrative/user action

- Internal sensors have detected privileged or user activity, which was not previously communicated. It can also reflect improper usage behavior. This illustrates a problem with internal communication channels or processes.



Example:

- A network scan was performed by a network engineer, while troubleshooting a problem.

Process/knowledge problem

- Update information process
- Verify if rule is actually meaningful

Problems that should be addressed with company security architecture key employees

Company optimizable incidents

Detection device/rule configuration error

- This category reflects rules on detection devices, which are usually passive or active components of network security. In bigger organisations these tools are often maintained by for example the network team.

Example:

- The IDS sends an alert to the SIEM for a suspicious pattern detected within application traffic in a subnet, where this application is actually not located.

Configuration problem

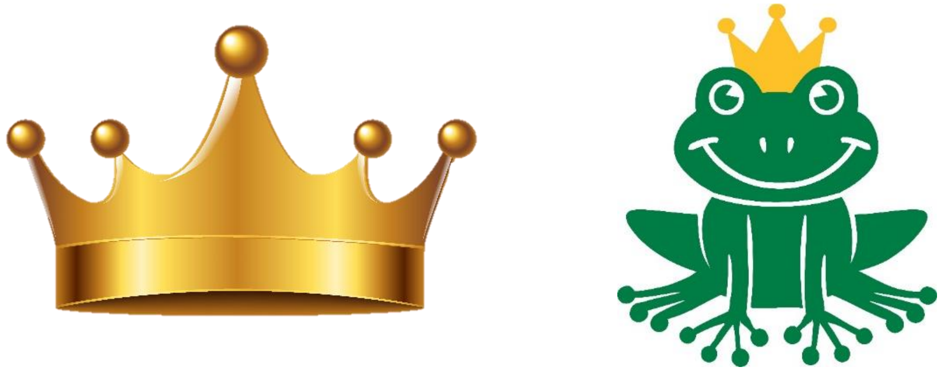
- Detection device/rule configuration correction needed

Problems that should be addressed with company security architecture key employees

Key business process artifacts

Bad IOC/Rule Pattern Value

- Products often require external indicator information or security feeds to be applied on active or passive infrastructure components to create alerts. This information can be outdated or wrong, which should be measured separately.



Example:

- An alert for an IP address categorized as Command and Control connection can upon analysis be classified as an obsolete indicator, which no longer hosts malicious services.

Knowledge/Strategy problem

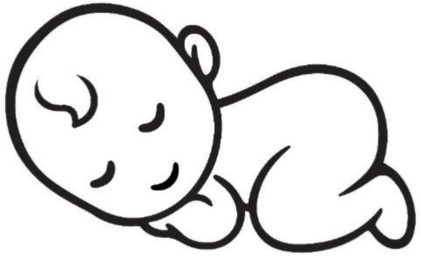
- IOC provider should be reviewed

Helpful incidents for strategic decision making & regulatory requirements

Key business process artifacts

Test Alert

- This alert reflects alerts created for testing purposes. This can be caused by regular unit tests, if such processes are in place, or single tests performed when baselining or fine tuning a rule.



Example:

- The alert was created for testing purposes by the SOC team

Quality Assurance

- Should be excluded from reporting

Helpful incidents for strategic decision making & regulatory requirements

Key business process artifacts

Confirmed Attack with IR Actions

- This alert represents the classic true positives, where all security controls in place were circumvented, a security control was lacking or a misconfiguration of a security element occurred.

Example:

- An alert for an outgoing connection to a URL provided by an IOC reveals an infection. Further host analysis is performed.

Service confirmation

- Lesson learned should point out needed infrastructure improvement

Helpful incidents for strategic decision making & regulatory requirements

Key business process artifacts

Confirmed Attack Attempt without IR Actions

- This category reflects an attempt by a threat actor, which in the end could be prevented by in place security measures but passed security controls associated with the delivery phase of the Cyber Kill Chain.

Example:

- An Antivirus alert is raised on a client device for detection of a malicious software. Infection was prevented.

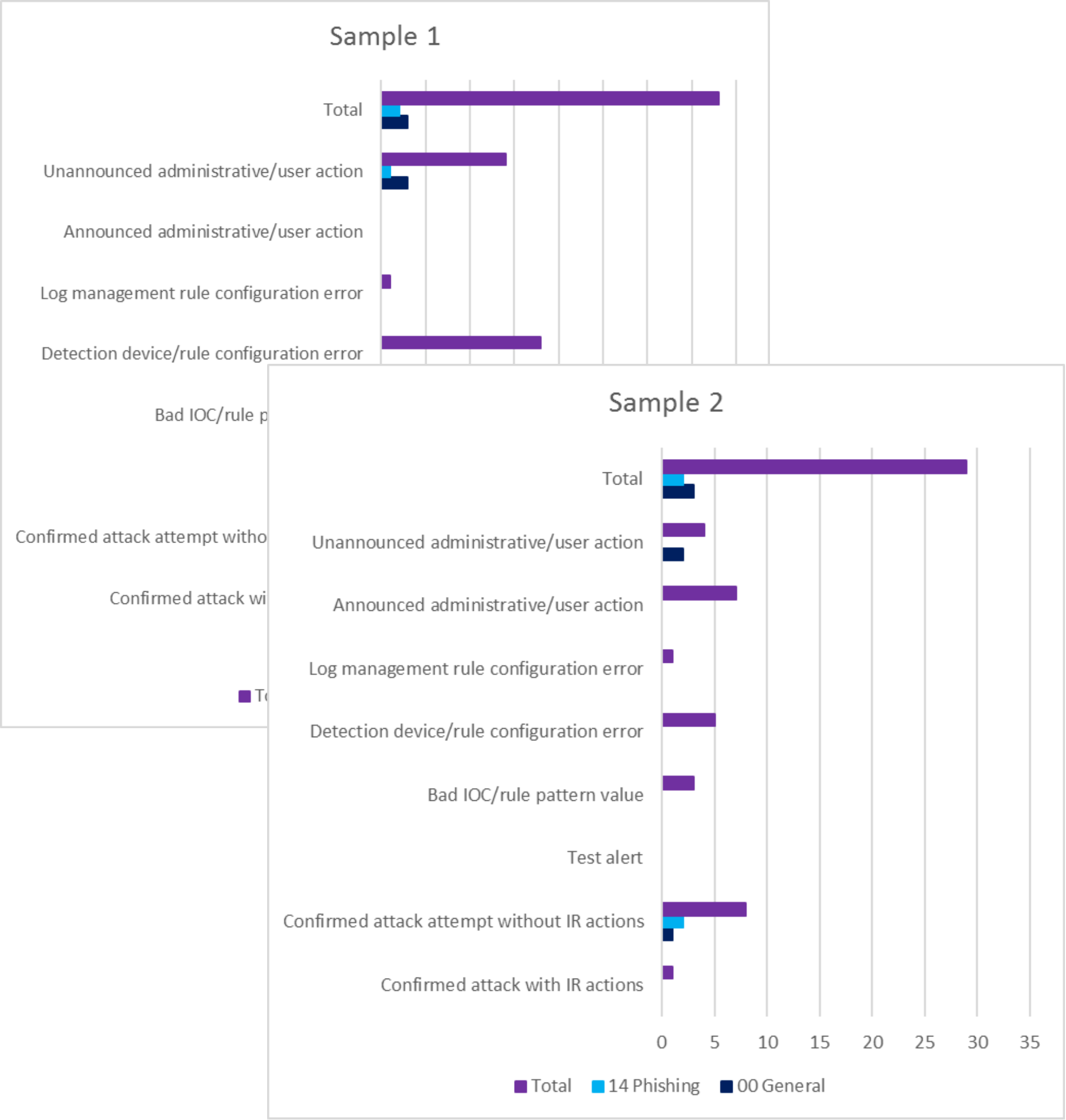
Architecture confirmation

- To be included in SOC report to reflect well spent budget

Helpful incidents for strategic decision making & regulatory requirements

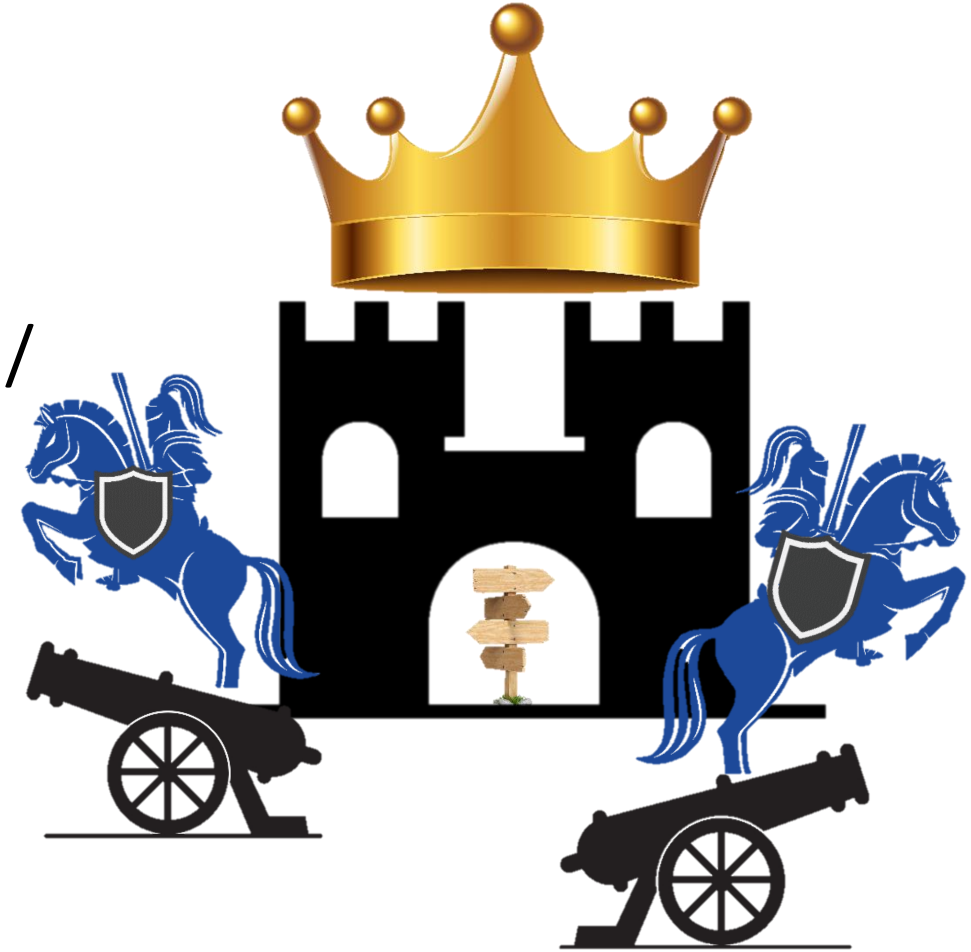
Benefits

- Identify where time is actually being spent
- Statistics for effectiveness of internal security measures & architecture
- Process possibility for directly initiating continuous improvement



Call to Action

- ➢Request field to be added to your SIEM tool/ Security incident platform



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