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

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) 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		

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.

Process/knowledge problem

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

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.

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.

Process/knowledge problem

- Update information process
- Verify if rule is actually meaningful

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.

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.

Knowledge/Strategy problem

- IOC provider should be reviewed

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.

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.

Service confirmation

- Lesson learned should point out needed infrastructure improvement

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 or an accepted risk.

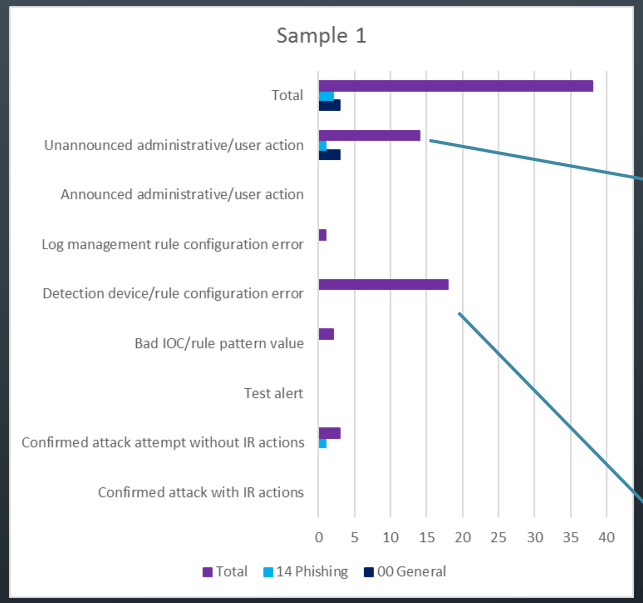
Architecture confirmation

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

Helpful incidents for strategic decision making & regulatory requirements

BENEFITS

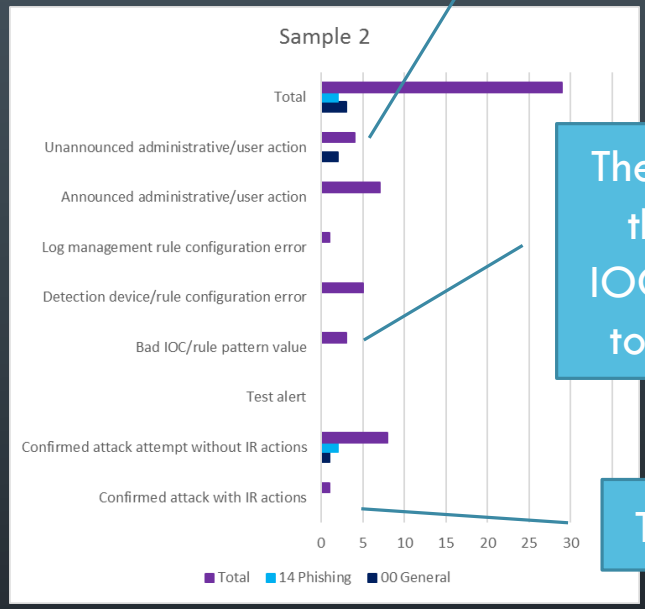
- Identify where time is actually being spent
- Statistics for effectiveness of internal security measures & architecture → new KPI possibility



Employees don't follow best security practices or policies

Company systems need better configuration verification

The SOC can improve the suppressions



The trust level of the alarming IOCs might need to be updated

True Positive \o/

BENEFITS

- Statistics for effectiveness of internal security measures & architecture → new KPI possibility

KPI	Explanation	Target Value
Number of Log Management Rule Configuration Error events per month	This value reflects the rules configured in the SIEM by the SOC Analysts. A high number suspects bad quality of rules, more training or experience needed.	< 10 %
Number of Announced Administrative/User Action events per month	This value reflects suppressions that should be improved.	< 10 %
Number of Bad IOC/rule pattern value events per month	If too many events were created by bad IOCs or rule pattern values, the source or the trust in it should be questioned.	< 5 %
Number of Confirmed Attack attempt without IR actions (best matched with Log Source Category)	Number of events detected but prevented by measures in place or where the alert isn't viewed as a high risk.	> 50 %
Number of Confirmed Attack attempt with IR actions (best matched with Log Source Category)	Very high numbers → Security Architecture should be updated Very low numbers → The rules aren't detecting or you are safe	☺

BENEFITS

- Process possibility for directly initiating continuous improvement

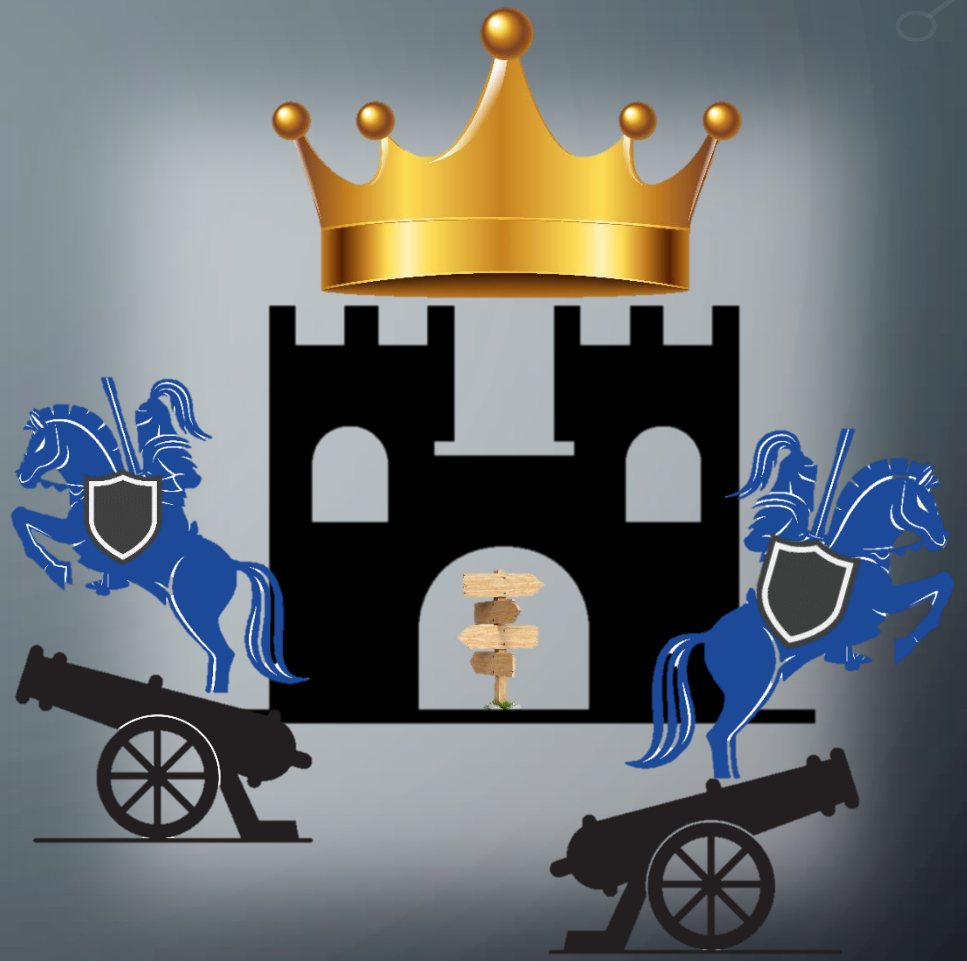
Disclaimer: this might break snake oil AI

Case	C-Level Perspective	SOC Perspective	Follow Up Action
Key driver	Does this alert inform me about an actual threat to the company?	Are our SIEM rules/detection capabilities working correctly?	What lesson can be learned from this event?
Announced administrative/user action	No – False Positive	Yes – True Positive	Update suppressions for announced actions
Unannounced administrative/user action	No – False Positive	Yes – True Positive	Update information process
Log management rule configuration error	No – False Positive	No – False Positive	SIEM rule correction needed
Detection device/rule configuration error	No – False Positive	No – False Positive	Detection device/rule configuration correction needed
Bad IOC/rule pattern value	No – False Positive	No – False Positive	IOC provider should be accredited
Test alert	No – False Positive	Yes – True Positive	Should be excluded from reporting
Confirmed attack with IR actions	Yes – True Positive	Yes – True Positive	Lesson learned should point out needed infrastructure improvement
Confirmed attack attempt without IR actions	No – False Positive	Yes – True Positive	To be included in SOC report to reflect well spent budget

Source: Paper - Table 2: False Positive - True Positive Comparison by Perspective

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/