Improving Security Incident Quality in SOCs with Resolution Categories

Desiree Sacher

Twitter: d3sre

Security incidents created during the security continuous monitoring process (ISCM, NIST 800-137,[1]), can be a valuable source for improving company processes and an efficient reference for budget planning if used right. The idea presented in this paper was created from years of experience in monitoring NIST 800-53 [2] controls, amongst others, where often the processes in place did not address the root cause of the problem but rather add suppressions to the detection rule. This paper discusses how security incidents can be tracked to focus on company improvements and strategically create statistical values. It is a suggestion for a structured resolution approach, inspired by the Post-Incident Activity – Lessons Learned phase by NIST 800-61 [3].

I. Introduction

For a long time, security related incidents have been categorized into true positives, when an alert actually detected a malicious event, and false positives, when no malicious activity could be identified. False positive is the term most often used to express that all of the safety measures have worked and no harm was done to the entrusted infrastructure. When reminded of what our current security measures have grown out of, a company lifecycle of policies, specifications, and configuration guidelines, this view makes sense. In today's world, where security processes need constant improvement as attack scenarios change faster than ever, this view is obsolete.

When looking at security measures through the SOC perspective, it becomes clear that false positives become an antiquated measure, not supporting technical changes often needed in companies. At worst the statistics created from security incident tracking even ensure management that everything is well and no improvements need to be done. Usually at this stage, the security professionals turned to penetration tests, to illustrate technical gaps in the security of products and services. Penetration tests are still a helpful instrument, but they don't always show cultural barriers or give well investigated basis for discussion. Also they can be very expensive and not every company can afford them.

What this paper suggests is to use security incidents as a means to track and illustrate improvements and adjustments of the security infrastructure. SOCs are most efficient, when every incident or event can be turned into a specific action to improve overall security of a company, therefore all events should be categorized as such.

II. Materials and Methods

Throughout my work in the last 3 years, where I was part of new SOCs that were built up, I've promoted tracking of security incidents and implemented the resolution categories displayed in Table 1: Overview resolution categories. Every category is illustrated with an example. The description/significance section explains what this category in numbers can tell the reader and why it is of importance. The benefit section is a quick outlook on what positive changes can be introduced when interpreting the numbers of such a statistic.

The resolution categories were defined for SOC monitoring rulesets, also called "Use Cases", usually configured in a SIEM. Security incidents created by use cases defined as part of the Information Security Continuous Monitoring process, often are the primary source of information for SOCs as generally this process is best documented and visible to the company. This value is not intended to

replace other categorisation but should be instead used as an additional field to improve SOC quality by focusing on what caused the wrong alert instead of just suppressing part of the detection rule. Figure 1: Decision Matrix for Applicability Categorization can assist in finding the right categorization. They should be applied after successful analysis of the Incident where identification of root cause for the event has been finished, along with diagnosed actual impact of the event.

	ENGLISH VERSION	DEUTSCHE VERSION
A)	Announced administrative/user action	Kommunizierte administrative/Benutzer Tätigkeit
B)	Unannounced administrative/user action	Unangekündigte administrative/Benutzer Tätigkeit
C)	Log management rule configuration error	Log-Management-Regel-Konfigurationsfehler
D)	Detection device/rule configuration error	Sensor-/Endpunkt-Regel-Konfigurationsfehler
E)	Bad IOC/rule pattern value	Schlechter IOC/Regel-Vergleichswert
F)	Test alert	Test-Alarm
G)	Confirmed Attack with IR actions	Bestätigter Angriff mit IR-Massnahme
H)	Confirmed Attack attempt without IR actions	Bestätigter Angriffsversuch ohne IR-Massnahme

Table 1: Overview resolution categories

a) Announced Administrative/User Actions

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.

Description/significance:

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.

Benefits:

Regular statistics can be created about tested security measures and processes. Log settings or suppressions for known activities can be optimized.

b) Unannounced Administrative/User Actions

Example:

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

Description/significance:

Internal sensors have detected privileged or user activity, which was not previously communicated. It can also reflect improper usage behaviour. This illustrates a problem with internal communication channels or processes. This category, when evaluated, illustrates time and effort by the SOC that was spent on following up on issues, that actually were not a problem. With growing maturity of a SOC, as much time as possible should be spent on actual technical analysis or the optimization of the detection capabilities.

Benefits:

This category reflects how well the SOC is included in surrounding IT processes. It can also be used as an indicator for awareness throughout the company, as reaction from the SOC emphasises that such behaviour is monitored, which might before not have been well known yet.

c) Log Management Rule Configuration Error

Example:

- Analysis of alerts for failed logins shows a misconfiguration in the central log management system rule, where the algorithm for counting the failed attempts is wrong.
- Analysis of alerts for command and control traffic IPs shows connection to a multihoster system, where the actual URL accessed was not compromised.

Description/significance:

This category reflects false alerts that were raised due to configuration errors in the central log management system, often a SIEM, rule. These errors in the detection algorithm should be corrected as fast as possible to prevent further false alarms. Following false alarms by this rule can lead to threat alert fatigue, which can occur if alarms are not taken serious anymore by analysts as they already expect it to

be a false alarm. Threat alert fatigue should be avoided at all cost to keep up analyst motivation and considering appropriation of analyst's resources is the simplest form of respect that can also prevent bore out.

Benefits:

Analyst's motivation can be kept on a higher level as the trust in the ruleset can be sustained. This category can reflect the quality of the rules, as especially rules that were properly vetted in the baselining phase and were moved to a productive state should not raise false positives by the algorithm anymore. If false positives by SIEM rule configuration error persist, skills of the SIEM engineers might need to be improved or the rule logic might need to be adjusted. As SIEM rules are usually maintained by the SOC, SOC analysts can directly influence this category. This category can be a valuable key performance indicator (KPI) as too many SIEM rule errors reflect basic SOC skill or understanding infrastructure problems.

d) Detection Device/Rule Configuration Error

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.
- The IDS rule pattern has created false positives as the rule is not specific enough.

Description/significance:

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. By the defined nature and scope of the teams, needed adjustments of these rulesets can often not be visible to the responsible maintaining teams, as they rarely are focused on processing security alerts. Therefore a close and trusted interaction with the SOC is essential. As both teams are met by different type of KPIs (usually network- and firewall teams are measured by operation related KPIs like uptime, SOCs are measured by the response time and completion/quality of analysis reports), adjustments to the rulesets and configuration can oblige to SLAs or might only be performed with a lower priority. To create KPIs for the SOC on this category would therefore not be fair.

This value can also be important in a SOC as a Service/MSSP relationship, as these devices are often not controlled by the SOC company and therefore bringing visibility into customer configuration ruleset quality might be needed to support changes.

Benefits:

Direct visibility into device configurations and rulesets to support the need for configuration adjustments. If no improvements to the ruleset can be performed by the responsible team, this can indicate the need for a different product or structural adjustments to the responsibilities of the involved teams or the company processes.

e) Bad IOC/Rule Pattern Value

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.

Description/significance:

Products often require external indicator information or security feeds to be applied on active or passive infrastructure components to create alerts. The quality of these indicators should be measured in a separate category as the used tool might actually fulfil SOC requirements, but the additional security feed might not uphold to the requested standards. This category can directly support needed changes in the SOC supply chain.

Benefits:

The source of the false positive can be clearly identified and proves that the SOC performance is better than superficial results might suggest. With this information adjustments to the SOC supply chain can be initiated.

f) Test Alert

Example:

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

Description/significance: 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. It should be counted in a separate category to not confuse it with other measures. No direct improvement suggestions can be derived from this category, but they might be a seal of quality as it supports a working SIEM rule configuration process. These incidents should also always be excluded when number of attacks are calculated for managers or customers.

Benefits:

Direct visibility into business relevant amount of security incidents.

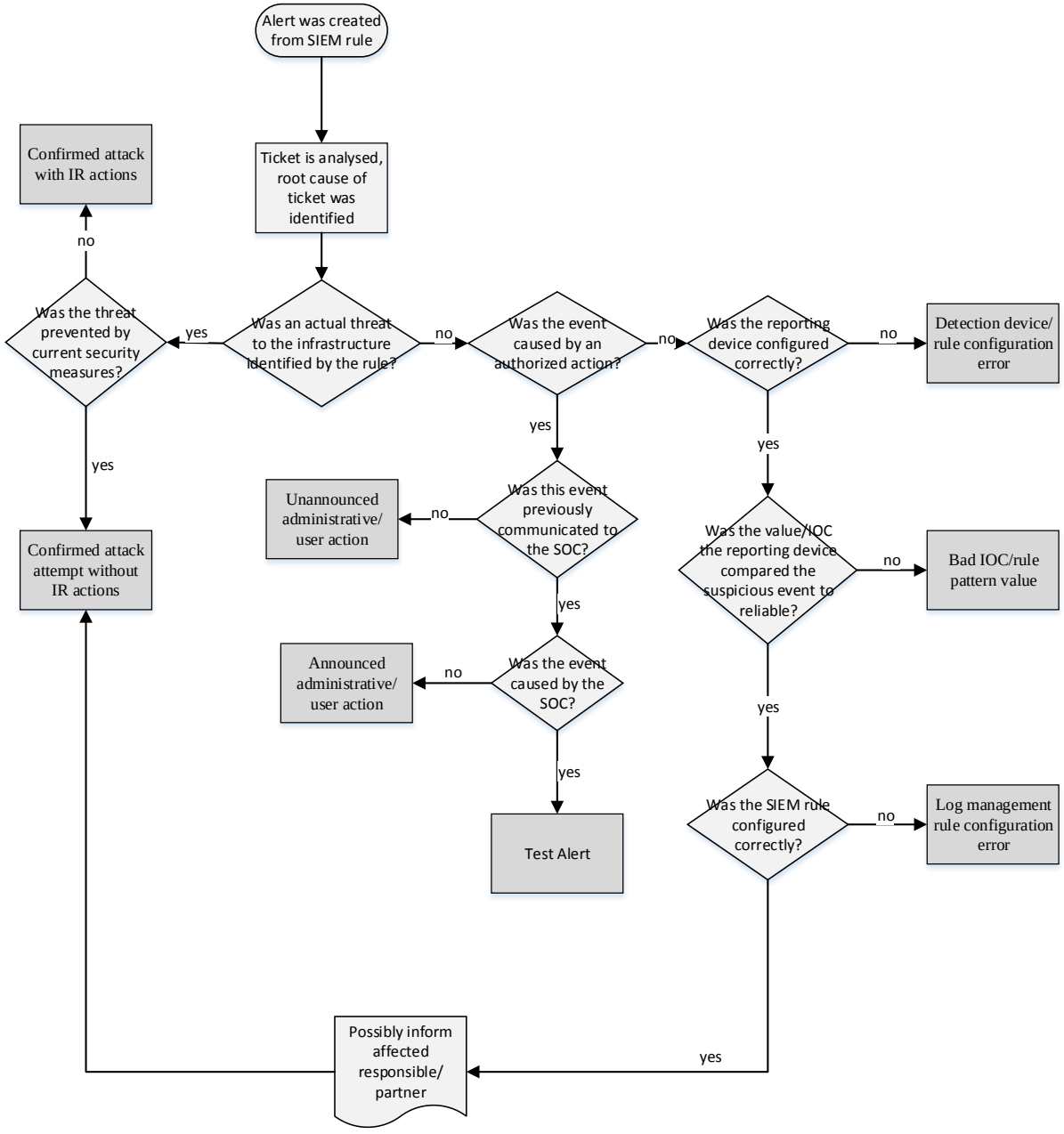

Figure 1: Decision Matrix for Applicability Categorization

g) Confirmed Attack with IR Actions

Example:

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

Description/significance:

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. In any way a throughout Incident Response had to be started (according to NIST 800-61) and an in-depth analysis needs to be performed to identify prospective needed prevention measures during the lesson learned phase.

Benefits:

This value represents the classic true positives, which is often the number managers or MSSP customers are most interested in. They represent a direct risk for the confidentiality and integrity of company data and should therefore be processed with cautious steps, possibly involving external specialists where needed.

h) Confirmed Attack Attempt without IR Actions

Example:

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

Description/significance:

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 [4]. It's the desired state of a security incident, as it proves current measures to be sufficient. Confirmation for prevented infection should always come from active infrastructure components. Mapping this resolution category to passive infrastructure components most likely indicates handling errors. If the number of these category incidents is low, infrastructure improvements earlier in the Cyber Kill Chain (Phase: Delivery, Installation, and Exploitation) should be prioritized as it may indicate lack of successful detection capabilities [5].

Benefits:

This value management and MSSP customers are most interested in in the general security monitoring process, as it represents actual attack attempts and can be used to illustrate and support security spending.

Case	**C-Level Perspective**	**SOC Perspective**	**MSSP Account Manager 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?*	*Were the MSSP service systems configured correctly to detect a threat to my company?*	*What lesson can be learned from this event?*
Announced administrative/user action	No – False Positive	Yes – True Positive	No– False Positive	Update suppressions for announced actions
Unannounced administrative/user action	No – False Positive	Yes – True Positive	Yes – True Positive	Update information process
Log management rule configuration error	No – False Positive	No – False Positive	No – False Positive	SIEM rule correction needed
Detection device/rule configuration error	No – False Positive	No – False Positive	No – False Positive	Detection device/rule configuration correction needed
Bad IOC/rule pattern value	No – False Positive	No – False Positive	No – False Positive	IOC provider should be accredited
Test alert	No – False Positive	Yes – True Positive	Yes – True Positive	Should be excluded from reporting
Confirmed attack with IR actions	Yes – True Positive	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	No – False Positive	To be included in SOC report to reflect well spent budget

Table 2: False Positive - True Positive Comparison by Perspective

III. Results

These categories allow a more granular definition of false positives, as false positive is actually subjective to the decision maker. For example from the perspective of a CSO, every alert except those belonging to the category "Confirmed attack with IR actions" should be seen as false positives, as they represent actions performed by the SOC, where no harm to the infrastructure was done so all current security measures were sufficient. If these numbers are evaluated well they can already today present a great image of where budget was spent well. From a SOC perspective though an alert categorised as "Unannounced administrative actions" and "Confirmed attack attempt without IR actions" represents a well working ruleset which actually detected suspicious behaviour and is therefore rather a true positive. Even "Announced administrative actions" can represent a well working ruleset, although the process for suppressing such alerts might want to be improved, in case the rules have been extensively proofed to be working well in the past. Of course CSO/CRO would not want this value to be counted in the number of attacks represented to the board of managers to indicate additional budget needs.

A SOC manager or architect on the other hand can use these values to see on what the team is most spending it's time on. The values become indispensable for basing strategic decisions for further needed infrastructure components, partners, or resources on. The Table 2: False Positive - True Positive Comparison by Perspective highlights the main differences in perspective and what action should be followed up with after classification of the event.

IV. Discussion

Other methods to categorize incidents usually relate to the type of event that was analysed e.g. Denial of Service, Forensics, Compromised Asset, etc [6] or related to other activity or criticality. The MISP project [7] created a great overview of known taxonomies for such cases. This categorization method though rather focuses on what lesson can be learned from each monitoring event by identifying the real root cause for the rule to trigger, so it actually reflects considerations usually done at the post-incident activity phase by NIST 800-61 which might not be already applied by the standard continuous monitoring process. It should therefore also be done at the end of a security incident.

This method of categorizing security incidents created by continuous security monitoring rulesets, have been proven valuable in the business context of an MSSP, but also within bigger companies succumbing to standards by NIST, PCI DSS, Swift, etc.

V. Acknowledgment

I originally came up with the dislike for false positives when maintaining security device rulesets of a former employer. Thank you to Christoph Weber and Michael Kurth for supporting and vetting this idea and successfully implementing it at our shared former employer. Thank you to Raphaël Vinot, Corsin Camichel, Eireann Leverett, Florian Roth, Ian Amit, Meline Sieber, Frank Boldewin, Jochen Raymaekers, Francesco Picasso and Amanda Berlin to further vet and correct this paper.

VI. Literature Cited

The following information was referenced during this paper:

[1]NIST Information Security Continuous Monitoring (ISCM): https://csrc.nist.gov/publications/detail/sp/800-137/final

[2] NIST Security and Privacy Controls: https://nvd.nist.gov/800-53

[3] NIST Computer Security Incident Handling Guide 800-61: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[4] Lockheed Martin Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[5] Lockheed Martin Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[6] Incident Categories by FIRST CSIRT: https://github.com/MISP/misp-taxonomies/tree/master/csirt_case_classification

[7] MISP Taxonomy Overview: https://github.com/MISP/misp-taxonomies