КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE

№ 2 (14), 2021

ISSN 2663 - 4023

DOI 10.28925/2663-4023.2021.14.614
UDK 004.056.53

Drahuntsov Roman
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-1781-7530
draguntsow@yahoo.com

Rabchun Dmytro
PhD, Associate Professor at the Department of Information and Cyber Security
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

POTENTIAL DISGUISING ATTACK VECTORS ON SECURITY OPERATION CENTERS AND SIEM SYSTEMS

Abstract. In this article we highlight several potential vectors of attacks that can be carried out on a monitoring capacities powered by SOC SIEM using its common features and misconfigurations. Widely spread problems like excessive amounts of false positive alerts or not absolutely accurate configuration of the correlation rules may lead to situation where an attacker is able to trigger an undesired state of the monitoring system. We've find three potential vectors for evasion the SIEM powered SOCs monitoring. The first vector grounds on mechanisms used to collect event data – log collectors: the malfunctioning SIEM state can be achieved with generating and submitting the bogus event data to the processing party like SIEM. Fake data flow may cause generation of mistaken alerts which can confuse the analytics stuff. The second vector employs some of the attacker's knowledge about actual SIEM configuration – exploitation of correlation rule flaws. Taking into account the fact that correlation rules are mostly hand-written, they are prone to some logic flaws – certain detection rules may not be triggered by all of the malicious attack indicators. An attacker with knowledge about that feature may fulfill the unrecorded conditions and trick the SIEM to treat the attack flow as benign activity. The last researched vector is based on redundantly sensitive detection rules which produce a lot of false positive alarms but are not removed. An attacker may trigger the malfunctioning alarm continuously to distract the analytics stuff and perform its actions under the cover of noise. Those discussed vectors are derived from analysis of the actual SIEM installations and SOC processes used as best practices. We have no actual indicators that those attacks are carried out "in wild" at the moment of issuing of this article, but it is highly probable that those tactics may be used in the future. The purpose of this research is to highlight the possible risks for the security operation centers connected with actual processes and practices used in industry and to develop the remediation strategy in perspective.

Keywords: Security Operation Center; SIEM; Evasion; Disguise; Monitoring; Defense evasion; Adversary tactics.

1. INTRODUCTION

In this paper we discuss the original proposal about the new potential attack vectors on the security operation center – we call it "disguise" attacks because of actual purpose to carry out one – to hide the malicious activity under the hood of "noise" of false positive alarms or other monitoring malfunctions.

As the complicatedness of the composite and distributed enterprise environments rises, security operation centers equipped with SIEM become much more spread in protection measures in use. As well attackers are about to evade those controls applied in much more sophisticated ways [1]. Potential threat agent may use the described below vectors in order to cover some complicated companies in the sophisticated and distributed enterprise environment protected with SOC SIEM. In this paper we are about to set up a conception that is a result of practical exploration of several SIEM systems used in production environments. All of three vectors highlighted below may be applicable for the most common SOC SIEM architectures and procedures. Remediation steps that can be carried out in order to eliminate risks connected with those attack scenarios should be applied to all of three major SOC components – technologies, people and processes. The highlighted problems don't belong only to configuration issues of the implemented software solutions – it touches as well multiple procedures like SLA implemented in security center.

There are couple of related works were found in the field of exploration of the SIEM false positive alarms and their impact on security posture and business flow [2] [3] [4]. The high false positive alarms rate problem's outcomes are fully described in [2] and the possible remediation strategy is proposed in [4]. As statistical reports say, most of the company with currently implemented SIEMs still experience security breaches and suffer from exceptional noise in the reports [5]. Those aspects are important in context of hardening the security operation center – which is succinctly set out in NSA Report [6]. The common points for building or architectural design of SOCs are highlighted in [7] and [8]. In all of the researched papers on the discussed topic arises the question of false positive alarms reduction and sharpening of a SIEM rules in use in order to prevent overloading. Paper [9] contains valuable notices on how human factor impacts the overall SIEM efficiency – from planning and setting up the correlation rules to close-end exploitation and incidents analysis. In our work we set up the question of possible new attack vectors based on the SOC SIEM misconfigurations. The scenarios of willing logic flaw exploitation by threat agents were not covered in the available sources at the moment of this research execution.

Main purpose for this article is to describe possible disguise attack abilities that can be used by threat agents in order to evade current security monitoring and controls. Those descriptions should be used to develop the remediation strategies against possible threats.

2. SOC SIEM: ACTUAL POPULARITY AND STATUS OVERVIEW

Popularity of the security operation centers with the SIEM solution as a core of detection capabilities is growing over last years. The main reason for it lies in the exceptionally fast growth of the IT infrastructure in all of the economics realms. As the assets evolves, the risks connected with it don't fall behind. To adopt the principle of counteraction on all of the killchain steps business requires the comprehensive detection and response solution. Implementation of SOC may respond to the raised challenges, however it may face several problems – as well as common ones and those not widely described. For instance, according to the study [10], 65% of modern SOCs faces the problem of an opaque IT infrastructure, especially the network traffic inspection. Lack of the relevant and comprehensive information about the current operations and network state may render the overall organizational SOC completely ineffective. As said in [11], the SOC consists of three main building blocks – people, technologies and processes. The potential problem covered in the following sections based on all of those components.

3. SIEM MONITORING AND ALERTING FUNDAMENTALS

Proposed conception of the correlation logic flaws scenarios bases on the fundamental principles used in SIEM solutions. The main idea of those systems may be defined as collection of data from the various non-homogenous sources, normalization, categorization and correlation based on the defined rules and criteria. To reduce the amount of time needed for analytics to process the collected data, SIEM performs automated analytics of that data (so called “events”). When some events in their group responds the criteria of a security incident, an appropriate alert is elevated for an investigation – depending on the SIEM realization this event is called “offense”, “incident”. Investigating only the raised incidents saves significant amount of time for appropriate stuff – and that is one of the biggest challenges in SOC implementation [9]. In most SIEM realizations incident alerts have some attributes defining its common parameters. For example, the definition of the similar incidents number – if there are more than one incident of this type at the time, all instances will be grouped in a one reducing the number of times the same instance will be processed. Depending on the SOC`s organizational structure process of incident investigation may differ. The most common [11] process involves an incident “pipeline” operated by the 1st SOC line and an SLA definition for each incident revealed. Time for an investigation – and false positive alerts detection respectively – may be explicitly defined, so an analyst should not skip any alert raised. This behavior is mostly intended to reduce the false positive detection mistake probability [2].

4. ATTACK VECTOR 1: FAKE LOG GENERATION

This kind of attack was described here [12], simultaneously as we researched this approach. The essence of that tactic is generation of enormous amounts of fake thought plausible log files and entries in a format understandable for the actual SIEM system and corresponding the actual event source format. This data is being sent to the SIEM log collector endpoint, then aggregated, and processed, producing the irregular volumes of new events which may lead to correlation halting, overloading the computing capacities, irrelevant incident alerts. As the best practices say, SIEM systems must constrain the scope of systems from where the event data is accepted [3], this attack requires from threat agent either misconfigured SIEM system either compromised trusted host. An actual result may depend on the specific payload, type of SIEM in use, datacenter computing capabilities, list of the configured correlation rules and policies, etc. As vast majority of SIEM implementations suffers from superfluous noise in their reports [5], this attack vector hits a nerve of most SOCs.

Fake log generation attack is possible when the following statements are satisfied:

1) Attacker has an access to the internal corporative network;
2) Attacker knows and has access to the SIEM log collector endpoint;
3) Attacker knows the input event data format;
4) Attacker has an approximate understanding of the SIEM correlation rules applied.

An access to the target`s internal network is required for an adversary in perspective of direct communication with SIEM log collector endpoint which are not commonly configured to be accessible from external network. The attack flow from the adversary point of view can be divided into the following steps:

1) Gaining access to the internal network, abusing certain connected device;
2) Analysis of the local device configuration or sniffing the internal traffic, or applying any other way to figure out log collector endpoint`s location and input logs format.
3) Analysis of the log format and crafting the performant rogue log source.
4) Redirection the fake log source to the log collector`s endpoint.

Some attack phases require additional explanation. On the second step attackers purpose is to figure out the way event data flows reaches the SIEM log collector. That purpose can be accomplished in various ways, the straightest one is to capture and analyze actual log data flow from one of the SIEM connected endpoints. Consider the following example. An adversary gains control over one of the legitimate log sources – server powering the rsyslog service – and is able to review the local configuration, live connections, etc. In this situation, an attacker may inspect the syslog configuration and some of the log files. On Unix-like systems with common configuration this can be accomplished with the following commands:

```
less /etc/rsyslog.conf
less /var/auth.log
less /var/kern.log
```

rsyslog.conf file with high confidence may contain the location of the SIEM entrypoint in a similar format:

```
# SIEM
*.* @10.10.10.10
```

This configuration example is interpreted as sending all the log files connected monitored by rsyslog service to the remote syslog server listening on the default 514 TCP port. From the adversary’s position, it is not possible to know which logs are processed by SIEM and which are not, however it can be assumed from the common best practices. For instance, security monitoring is extremely likely configured to supervise the SSH authentication attempts in order to detect possible bruteforce attacks or to reveal non-legitimate authorizations. This behavior can be abused by the attacker with fake SSH authentication logs. The fact the logs of this kind can’t be generated by the system from the external attacker activities may lead the monitoring team to treat it as legit. To achieve the massive scale of the attack, logs can be generated automatically with a pattern. After achieving the fake log’s generation and delivery process automation an adversary may launch it from the compromised device or from the extraneous network device.

Possible outcomes of the described fake log generation attack may be the following security issues:

1) SIEM is overflowed with fake events, licensed EPS volume is exceeded, new actual events will not be accepted in full scale – the simultaneous security incidents may be missed by the software and overlooked by the security team;
2) The hardware powering the SIEM is overloaded with an increased correlation load, the system is out of normal workflow and may not properly handle incoming event data;
3) Security team devotes too much time to handle the abnormal log source missing the actual attack workflow which may be much quieter than the distraction activity is.

5. ATTACK VECTOR 2: CORRELATION LOGIC FLAW EXPLOITATION

As a best practice most of the SOCs are obliged with SLAs on handling and investigation of the SIEM generated incident alerts [3]. That means each incident will consume the security team’s time resources and attention to handle the offence either prove it wrong (mark as false positive). That behavior may be treated as a possible security drawback, because of probable overloading of the SOC human resources [9] – it is not allowed to neglect the incident alert without proper time consuming investigation. Most of cases where this vector may present are stated in [4].

Any security incident alert (offence) produced by the SIEM system is a product of the certain logical function – correlation rule, which has some pre-requisites for alert generation. Those pre-requisites may be treated as function arguments and the produced alert as function's positive result. An adversary may reverse engineer the logical function of the correlation rule, line up the incoming arguments – as an events, flows and other SIEM incoming data – and try to fit the outlined criterias. As a result, SIEM will generate an incident alert based on those rogue pre-requisites. The attack's essence is in the fact that there were no actual incident but the alert still raised. Significant amount of such "fake" incidents may consume too much SOC specialists' time and reduce the overall efficiency. Therefore, an adversary has more chances to stay undetected or underestimated in its real malicious activity. The balance between data value and amount of data processed is perfectly displayed in [7]. As detection mechanisms have their blind spots they have malfunctions connected with excessive attention to some details [3].

The reason why the emphasized attack may exist is the logical flows in the SIEM correlation rules. Namely, an array of criteria used to indicate the incident is redundant and thus is not exclusively represents an actual incident. An ideal configuration of the SIEM correlation engine generates zero false positive results and alerts about any actual incident occurred – this behavior may be considered as ideal model, which is not possible to achieve in real environment. Considering the array of actual incidents and array of situations the SIEM estimates as incidents, in ideal model those arrays are not equal. In real conditions, they may overlap, intersect or not, but the purpose of correlation rules tuning is to approach the ideal configuration by transforming the array of SIEM alert indicators. The closer it is to the actual incident array, the less false positive amounts generates SIEM. Zone which is not in the actual incident array but is covered by SIEM correlation rules is represented by false positive alerts. Provocation of the excess amount of false positive alerts is a purpose of an adversary in the delineated attack scenario.

The principal challenge an adversary faces while performing correlation logic flaw exploitation is guessing the SIEM configuration in use. The ways to figure out are not observed in this article. Assuming the common configuration and being able to trace SOC's reaction adversary can suggest the correlation rules in use and required events to produce alerts.

As an example of such an attack can be fetched the following situation. SOC drives the detection of common security issues exploitation as IDS rule. Consider the MS17-010 exploitation attempt as an attack requiring investigation. However, it is not enough to handle single IDS signature alert of common exploit attempt as an actual exploitation evidence. It is much more probable that appropriate correlation rule uses another required signature as an identifier of successful exploitation – establishing of the command&control channel. There is a common practice to configure the IDS rule for searching the malicious patterns in the incoming traffic to meet that requirement. Such pattern can be just a piece of shell commands, such as "cat /etc/passwd". Hence the exploitation attempt of MS-17-010 vulnerability and attempt to remotely execute shell command are different kinds of alerts interconnected in an attack flow, the correlation rule may combine them as an identifier of the successful exploitation. As a result, SIEM will raise the high-value incident alert and analysts will be obliged to investigate it. Needless to say, such indicators are not obviously indicate actual incidents and are extremely prone to fall short in detecting the actual attack. Exploitation attempt is NOT yet a successful compromise, as shell command signature in intercepted traffic may not reflect the C2 channel. Such configuration is strongly prone to false negatives in detection the actual exploitation, but in the observed scenario the adversary`s target is not the staying undetected, but actually do in noisy fashion.

Assuming that an attacker may guess the constituents of the correlation rule logical parts, he can easily trigger the alert by starting sequenced attempts of exploitation and command&control channel establishing from the side infrastructure, which is not intended to carry out the actual attack flow. In the described case, SIEM will fall short in differing the actual successful attack from sequenced imitations of malicious activity.

Guessing certain array of misconfigured rules an adversary may trigger heterogeneous scope of alerts on the analysts' consoles. Concentrated in short time period they may trick the security personnel to think of a massive and complex incident. Well camouflaged actual attack workflow on different targets scope may remain under the radar in the period of the diversion attack, even leaving some minor evidences.

6. ATTACK VECTOR 3: "THE SHEPHERD'S BOY AND THE WOLF"

This type of attack is based on the similar basis as the previously described correlation logic flaws exploitation. The key point and the main difference is the purpose of its execution – in this case, triggering the security team to disable the annoying and false alerts rising rule – as most of the SIEM alerts are false positives [2].

Consider the correlation rule which is well configured to hunt the actual threat, unlike the example rule mentioned in the previous section, but prone to some false positive alerts. If the false positive alert pre-requisites for such rule can be accomplished with benign activity, the attack is possible. An adversary fills out the correlation requirements and triggers single or a couple of incidents. Security team investigates the alerts and closes them as false positives. Then the adversary triggers the rule again. If SOC team stands down in investigation of actual reasons of such behavior, it is highly probable, that "annoying" detector will be disabled till redesign, or further investigations will not be performed deeply – in ideal conditions that tests should be conducted on pre-deployment stage [4]. Such behavior of the security analyst`s may be triggered by incorrect efficiency metric (count of closed incidents, investigation timings, etc), lack of practical of experience or just negligence which is easily explained with excessive workload [10]. The adversary is able to detect the start of ignorance observing the side-channels – for example, blocking of the alerting node by the security team. When the monitoring is disabled on the stricken vector, the adversary may start the activity on it completely undetected – even if the monitoring rule is not turned off, the security personnel will not pay attention to its alerts.

There are some significant challenges an attacker faces before accomplishing this attack`s results. The first obstacle is the suggestion of detection method in use. As for previously discussed kinds of diversion attacks, the way to achieve this target may differ in common infrastructures – analyzing of the security team`s activity, attacking the SIEM, hunting for a security detection samples, etc. The second obstacle is to find reasonable vector to trick monitoring turning off – it should be useful for an adversary in performing the scheduled attacks. It is not obvious that such a misconfigured detection rule will be faced on the desirable for an adversary vector.

7. CONCLUSIONS AND PERSPECTIVES

As a result of conducted study we have described three possible ways that threat agents may use to evade the implemented security controls. Current best practices in SOC building do not obviously prevent the realization of those attacks as they are targeting the essential parts of principles on which security operation centers are built and SIEMs are configured. Despite we have no data about usage of those tactics in actual security incidents we are aware of that in future. We are looking forward to have experimental proof-of-concept for or against described conception and now working on remediation strategy principles.

REFERENCES

1 Butler, M. (2009). *Benchmarking Security Information Event Management (SIEM).* SANS.
2 (2019). *The impact of security alert overload*. CriticalStart.
3 Swift, D. (2010). *Successful SIEM and log management strategies for audit and compliance*. SANS.
4 Sacher, D. (2020). Fingerpointing false positives. Digital Threats: Research and Practice, 1(1), 1–7. https://doi.org/10.1145/3370084
5 *2014 SIEM Efficiency Report*. (2014). Netwrix.
6 *Hardening siem solutions*. (2019). NSA
7 *The critical elements of improving the effectiveness of a security operation center.* (2021). SecureOps.
8 Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford.
9 Bojana Vilendečić, Ratko Dejanović & Predrag Ćurić. (2017). The impact of human factors in the implementation of SIEM systems. *J. Of Electrical Engineering*, *5*(4). https://doi.org/10.17265/2328-2223/2017.04.004
10 *Improving the Effectiveness of the Security Operations Center*. (2019). Ponemon Institute LLC.
11 Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/access.2020.3045514
12 *Attacking SIEM with Fake Logs* -. (2020). LetsDefend Blog. https://letsdefend.io/blog/attacking-siem-with-fake-logs/

УДК 004.056.53

Драгунцов Роман Ігорович
Державний Університет Телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-1781-7530
draguntsow@yahoo.com

Рабчун Дмитро Ігорович
кандидат технічних наук, доцент кафедри управління інформаційною безпекою
Державний Університет Телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

ПОТЕНЦІЙНІ ВІДВОЛІКАЮЧІ АТАКИ НА ОПЕРАЦІЙНІ ЦЕНТРИ БЕЗПЕКИ ТА SIEM СИСТЕМИ

Аннотація. В даній статі розглянуто деякі потенційні вектори атак, що можуть бути здійснені на системи моніторингу операційних центрів безпеки (SOC), зокрема системи SIEM. Широко розповсюджені проблеми таких центрів, такі як великі обсяги хибних позитивних спрацювань, або не абсолютно точна конфігурація кореляційних правил, можуть призводити до ситуацій в яких порушник має змогу спровокувати небажаний стан системи моніторингу. Ми виявили три потенційні вектори подолання моніторингу SOC, що здійснюється через SIEM. Перший вектор ґрунтується на механізмі, що використовується для збору даних про події - log collector: Некоректний стан роботи SIEM може бути досягнутий за допомогою генерації сторонніх беззмістовних даних про події та спрямування їх на SIEM. Потік підроблених даних може спровокувати появу помилкових інцидентів, який витрачає час та можливості для реагування відповідного персоналу. Другий вектор вимагає від агенту загрози певних знань про фактичну конфігурацію SIEM - експлуатація проблем кореляційний правил. Беручи до уваги той факт, що кореляційні правила SIEM створюються вручну, вони можуть містити логічні помилки - певні правила детектування можуть не спрацьовувати на всі необхідні індикатори шкідливої активності. Агент загрози, що знає про такі особливості, може задовольнити критерії не-детектування та таким чином замаскувати процес атаки під легітимну активність. Останній досліджений вектор базується на надлишково чутливих правилах детектування, що генерують істотний обсяг хибно позитивних повідомлень, але все одно залишаються активними. Агент загрози може провокувати хибні тривоги на постійній основі для відволікання аналітиків та проведення атак під "шумовим маскуванням". Усі три вектори були досліджені нами в ході аналізу практичних інсталяцій SIEM та процесів SOC, що визнані стандартами індустрії. На даний момент ми не маємо інформації про те, що дані атаки вже відбувались в реальному середовищі, але існує висока вірогідність появи таких тактик в майбутньому. Мета даного дослідження полягає у висвітленні можливих ризиків для операційних центрів безпеки, пов'язаних з поточними процесами та практиками, що використовуються в індустрії, та розробити стратегії подолання даних проблем у перспективі.

Ключові слова: Security Operation Center; SIEM; Обхід; Маскування; Моніторинг; Defense evasion; Тактики супротивника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Butler, M. (2009). *Benchmarking Security Information Event Management (SIEM).* SANS.
2 (2019). *The impact of security alert overload*. CriticalStart.
3 Swift, D. (2010). *Successful SIEM and log management strategies for audit and compliance*. SANS.
4 Sacher, D. (2020). Fingerpointing false positives. Digital Threats: Research and Practice, 1(1), 1–7. https://doi.org/10.1145/3370084
5 *2014 SIEM Efficiency Report*. (2014). Netwrix.
6 *Hardening siem solutions*. (2019). NSA

7 *The critical elements of improving the effectiveness of a security operation center.* (2021). SecureOps.

8 Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford.

9 Bojana Vilendečić, Ratko Dejanović & Predrag Ćurić. (2017). The impact of human factors in the implementation of SIEM systems. *J. Of Electrical Engineering*, *5*(4). https://doi.org/10.17265/2328-2223/2017.04.004

10 *Improving the Effectiveness of the Security Operations Center*. (2019). Ponemon Institute LLC.

11 Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8,* 227756–227779. https://doi.org/10.1109/access.2020.3045514

12 *Attacking SIEM with Fake Logs* -. (2020). LetsDefend Blog. https://letsdefend.io/blog/attacking-siem-with-fake-logs/