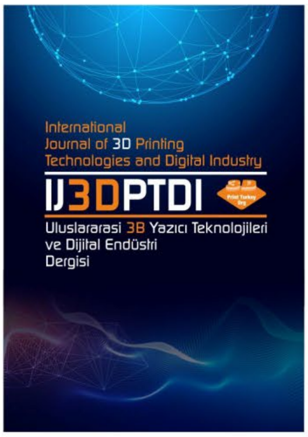
International
Journal of 3D Printing
Technologies and Digital Industry
IJ3DPTDI
Uluslararası 3B Yazıcı Teknolojileri
ve Dijital Endüstri
Dergisi

ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING
TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)

URL: https://dergipark.org.tr/ij3dptdi

# DETECTION OF ADVANCED PERSISTENT THREATS USING SIEM RULESETS

**Yazarlar (Authors):** Adem ŞİMŞEK*, Ahmet Hasan KOLTUKSUZ

***Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article):*** *Şimşek A., Koltuksuz A. H., "Detection of Advanced Persistent Threats Using Siem Rulesets" Int. J. of 3D Printing Tech. Dig. Ind., 7(3): 471-477, (2023).*

**DOI:** 10.46519/ij3dptdi.1353341

**Araştırma Makale/ Research Article**

**Erişim Linki:** (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

# DETECTION OF ADVANCED PERSISTENT THREATS USING SIEM RULESETS

Adem ŞİMŞEK[a]*, Ahmet Hasan KOLTUKSUZ[b]

[a]Antalya Belek University, Faculty of Engineering, Department of Software Engineering, TÜRKİYE
[b]Yaşar University, Faculty of Engineering, Department of Computer Engineering, TÜRKİYE

* *Corresponding Author: ademsim@gmail.com*

(**Received:** 31.08.23; **Revised:** 24.11.23; **Accepted:** 13.12.23)

## ABSTRACT

Cyber-attacks move towards a sophisticated, destructive, and persistent position, as in the case of Stuxnet, Dark Hotel, Poseidon, and Carbanak. These attacks are called Advanced Persistent Threats (APTs), in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period. APT attacks threaten the main critical areas of today's digitalized life. This threat covers critical infrastructures, finance, energy, and aviation agencies. One of the most significant APT attacks was Stuxnet, which targeted the software controlling the programmable logic controllers (PLCs) that are, in turn, used to automate machine processes. The other one was the Deep Panda attack discovered in 2015, which compromised over 4 million US personnel records because of the ongoing cyberwar between China and the US. This paper explains the difficulties of detecting APTs and examines some of the research in this area. In addition, we also present a new approach to detecting APTs using the Security Information and Event Management (SIEM) solution. In this approach, we recommend establishing APT rulesets in SIEM solutions using the indicators left behind by the attacks. The three basic indicator types are considered in the rulesets and are examined in detail.

**Keywords:** Cyber Security, APT, SIEM, Rule Based Warning, Rule Sets.

## 1. INTRODUCTION

Transforming the manufacturing industry to the further generation or evolution to cyber-physical systems, namely Industry 4.0, is a new trend in world computerization [1]. On the other hand, according to some estimates, cybercrime's global cost is $1 trillion annually [2]. Cybersecurity is becoming increasingly important as private sector companies, the military, national institutions, and even retail shoppers shift their operations to the Internet. [3].

Developing an industrial environment and critical infrastructures, the basis of vital activities, and innovative national solutions, makes life easier. However, this well-designed life brings insufficient security measures. Sophisticated and stealthy attacks exploiting these vulnerabilities can lead to many national and international cyber wars, such as Stuxnet, Dark Hotel, Poseidon, and Carbanak [4-7]. These attacks are called Advanced Persistent Threats (APT).

This paper looks at Security Information and Event Management (SIEM) and proposes a new approach to detect APTs using SIEM solutions based on event analysis. While Section II highlights the motivations and contributions of the paper, Section III presents an overview of APTs and their features, as well as a summary of the related works as a methodology. Section IV discusses security defense systems and explains why SIEM solutions are essential to remedy the APT attacks. Section V defines indicators of compromises (IOCs) and rule-based approach in SIEM, selected indicators of APTs, and implementation in an open-source platform. In this section, the applied rulesets are evaluated, and the detection of the early phases of some APTs is described. The discussion and the achieved results are in Section VI. Finally, Section VII delineates the conclusion and planned future work.

## 2. MOTIVATION AND CONTRIBUTION

As the problem of APTs grows more prominent, there seems to be no clear-cut solution other than early warning systems. The SIEM equipped with rules for a rule-based alarm system looks very promising; hence, our primary motivation is to create new rules so that a typical SIEM would be much more potent in the fight against the APTs.

As shown in the sections, the various rules can be produced for all APTs and positioned in the SIEM environment. And that is precisely the accomplishment of this study. Moreover, 30 different rules have already been created, which is a leading contribution to the struggle with APTs

## 3. METHODOLOGY: A GENERAL LOOK INTO THE APTs

### 3.1. APT Features

The reason for APT creation can be many-fold. Political, economic, personal ego-boosting, or even a game can be a motivational factor. The basic structural features of APTs may not change, even at simple or advanced targets. It has an attack plan. The plan's objective is clarified, and the methods used to achieve this goal are determined. So, the attack is carried out in an organized manner. During the attack, the primary objective is to get clean access to the inside of a cyber system. To that end, many vulnerabilities of any given cyber system can be utilized from the simplest to the most difficult, including 0-day exploits for the applications or systems used. Once attackers enter, they stay insidiously and silently until they reach the primary goal. At this stage, the methods to increase the resistance to penetration into the system can be used as a solution for the APT attack. The termination of the attack is the choice of the attacker. They may also choose to move away for a while, leaving a path they can take again. Thus, the life of an APT has started in the victim system.

### 3.2. The Life Cycle of APTs

The life cycle of APTs can be described in 5 distinctive phases:

Phase #1 - Intelligence Gathering: APTs conduct detailed research on their targets to identify particular avenues of attack.

Phase 2 - Initial Exploitation: The initial attack targets individuals through some form of social engineering. Initial foothold into the target environment and Malware beacon home and download additional functionality.

Phase 3 - Command and Control (C2) means control of the compromised virtual environment. In most cases, this persistence is only possible with new services. Usually, APTs perform corporate reconnaissance to locate computers, servers, or storage areas where the information instructed to steal is located.

Phase 4 - Privilege Escalation: Intruders move laterally to new systems to explore their contents. They inevitably seek to escalate from local users to local Administrators to higher levels of privilege in the environment.

Phase 5 - Data Exfiltration: Finding data that interests them, APT systematically collects the data in an archive, compressing and encrypting it. The primary purpose of an APT attack is to steal something valuable. APT can also use traditional methods to transfer files. Finally, APTs attempt to do what their controllers have assigned to them and maintain access to the target environment. [8].

### 3.3. Why Hard to Detect?

APTs are target-specific attacks. For this reason, the tools and methods used can be specific to the target. According to researchers at Dell, the defense tools, procedures, and other controls commonly applied to address commodity security threats are primarily ineffective against targeted APT-style attacks [9]. This is because the actors behind the attack are focused on a specific target and can customize and tailor their tactics.

### 3.4. Summary of the Related Works

Sekharan and Kandasamy express and profile an abstraction of SIEM tools and event correlation engines by describing their technical comparative work focusing on the most popular SIEM tools and open-source rule-based correlation engines [10]. Raja and Vasudevan emphasize that the SIEM solution can be used in TCP SYN Flood attacks [11]. Russ Anthony used a diary collection exercise as an example [12]. Anthony notes that some log rules can be used to catch APTs. Bryant and Saedian found a solution suitable for the chain-of-kill model [13]. Their study deduced how many log sources can be obtained from each APT stage data. By presenting an output-oriented strategy, Chuvakin says, you will only collect a particular event if you know what to do with that event in advance and only if that event will be generated towards some known output, such as an alert or report measure. [14]. Industrial Control Systems (ICS) are vital components of many critical infrastructures. Alladi discusses case studies of significant cybersecurity attacks on ICS infrastructures in the last 20 years [15]. Mohammed examines usable indicators against cyber-attacks [16]. Atluri and Horne propose a framework for network traffic indicators in ICS [17]. NIST presents and compares commercial and open-source solutions [18]. Toker uses Wazuh HIDS for the intrusion detection system for the SCADA system [19]. Zahid proposes an agentless module for the Wazuh security information and event management (SIEM) solution [20].

## 4. A SOLUTION ATTEMPT: SIEM

Many security solutions are used to detect and prevent APTs. A firewall is used to block known IP addresses and suspicious ports used for attacks. An e-mail security solution effectively protects users from black-listed mailers and suspicious IP addresses from being redirected to users. Using IDS / IPS to detect suspicious movements in network traffic and analyze network behavior is vital. An anti-virus system is a critical security measure in end-user machines and critical systems in case of malware behavior. This understanding of security defense is the leading security solution for analyzing immediate movements and preventing possible attacks. However, in the case of unknown types of attack, log management is an element that reinforces this security system in the post-analysis of unimpeded attack behaviors.

### 4.1. Position of SIEM

SIEM tools collect, analyze, normalize, and correlate all files, analyze data from various devices, and give a centralized view of logs.

It is essential to send log records of all systems to SIEM to clarify security events. The rules in SIEM allow deep examination of the events that fall into the log pool. Generating rule alarms can resolve a critical event for the security operation center.

Placing the SIEM solution at the heart of the defense system against APTs can give some advantages, such as:

- Ensures a 360° view of a company's IT ecosystem and allows for correlating heterogeneous security events,
- Guarantees a quicker and better-automated analysis of all security events within a single location,
- It allows companies to flexibly tailor their defenses to specific needs, creating a unique security posture that complies with corporate security policies and best practices. [21].

### 4.2. The Commercial SIEM Solutions

SIEM solutions are used effectively in today's IT environment. One of the leading products is IBM Qradar [22]. It has basic rulesets for detecting malware infections and spear-phishing campaigns, scanning network traffic for suspicious communications, and privilege escalation methods. HP ArcSight is another powerful solution [23]. It has essential features, which include identifying suspicious event patterns and detecting misconfigurations of network devices, systems, and applications. Another most popular product is Wazuh [24]. It is an open-source solution. The main capabilities are creating rulesets for specific attacks, checking file integrity, and monitoring the Windows registry. It also has an OSSEC HIDS that runs on most operating systems.

## 5. DETECTION OF APTs USING SIEM RULESETS

### 5.1. Indicators of Compromises (IOCs)

SIEM is not an active attack detection solution such as firewall, e-mail security, and IDS / IPS systems. However, it can generate alarms through event records received from active defense systems. In the case of an information breach, IOCs might include a variety of electronic evidence left behind, such as an MD5 hash, a C2 domain or hardcoded IP address, a registry key, a filename, etc [25].

This paper describes creating rules through three fundamental indicators: (i) monitoring the file movements, (ii) registry changes, and (iii) the privilege escalations. Modifying existing files or creating files or new file types on the target machine is the essential malware feature while carrying out the second stage of the attack. Each APT attack can use different file names and paths at this stage. These file names and paths are sufficient IOCs for SIEM. Similarly, the intruders may create new keys or values in the registry or modify existing ones to make a point of resistance. Current SIEM solutions do not have specific rules for each APT. Thus, the anti-virus or SIEM solution may not detect changes in keys and values. Another type of behavior is privilege escalation, which is vital in all APTs. This attempt is monitored in most SIEM products. However, it will give more meaningful results when it is combined with file and registry changes. So, privilege escalations become meaningful when and if evaluated as a whole.

### 5.2. Rule-Based approach

The main feature of the APT attacks is that each attack has a unique structure. The tools and modules they use from beginning to end of the attack can be specific to that attack. For this reason, traditional security methods are not enough to provide a complete solution. At this point, this article proposes the creation of an APT ruleset with special rules for each APT. This approach, which we call the rule-based approach, can determine the files each attack uses, the registry records it modifies, and the user accounts it provides access to. Rules are created on SIEM using these indicators. When these indicators are generated in the logs collected, an alarm is sent to the administrators. Sample rules are:

File Match (FM.) Rule:

- Alert on <file_name> created in <folder_path>

Registry Match (RM.) Rule:

- Alert on <registry_value> modified in <registry_location>

Privilege Escalation Match (PEM) Rule:

- Alert on <standard_account> is added to <Administrators_Group>
-

Table 1 refers to mapping the above-identified alarms to the APT phases. The rules for each APT can be determined by which attack phase coincides.

**Table 1.** Phase/Rule Match Table.

| Phase /APT | Ph.1 | Ph.2 | Ph.3 | Ph.4 | Ph.5 |
|---|---|---|---|---|---|
| APT Name | - | FM | RM | PEM | - |

### 5.3. Implementation in Wazuh

In 2023, there were 101 APTs, both active and passive, in the world [29]. This number is increasing every year. When we examine these APTs, we can see that they have many indicators; thus, special rules can be produced for almost all of them. This paper gives three Wazuh rules or, in other words, three basic indicators below.

Indicator Example #1: The APT-28 targets insider information related to governments, militaries, and security organizations that would likely benefit the Russian government. [26] In this attack, intruders create a hidden file that can be named as
%ALLUSERSPROFILE%\edg6EF885E2.tmp

For temporary storage. So, this can be a good indicator for the File Match (FM) rule. The following rule states that the APT 28 may have started on this indicator:

```
<rule id="60001" level="12">
<if_sid>512</if_sid>
<match>edg6EF885E2.tmp</match>
<description>A suspicious file has been
detected, </description>
<description>APT28 Phase 1 may have
begun.</description>
<group>win_apt,rootcheck,pci_dss_11.5,gpg1
3_4.11,gdpr_II_5.1.f</group>
</rule>
```

Indicator Example #2: The Duqu, yet another APT, is a precursor to a future Stuxnet-like attack. Cyber threats were written by the same people or coders with access to Stuxnet source code, and recovered instances were created after the last discovered version of Stuxnet. [27]. In this attack, attackers make a registry key to give the information that the computer has been compromised. The following rule can report the existence of APT when there is a registry operation:

```
<rule id="60002" level="12">
<if_sid>550</if_sid>
<match>\SOFTWARE\Microsoft\Windows\C
urrentVersion\Internet
Settings\Zones\4</match>
<description>A registry change has been
detected, </description>
<description>Duqu APT Phase 3 may have
begun.</description>
<group>win_apt,syscheck,pci_dss_11.5,gpg13
_4.11,gdpr_II_5.1.f</group>
</rule>
```

Indicator Example #3: Black Energy is a popular crimeware that is sold in the Russian cyber underground and targets Ukrainian government institutions [28]. The malware bypasses the default Windows User Account Control (UAC) settings. It exploits a backward compatibility feature found in newer versions of Windows. The following rule can notify when a user with standard rights is added to the Administrator's group:

```
<rule id="60003" level="10">
<if_sid>18203,18217</if_sid>
<match>A member was added to a security-enabled local group.</match>
<description>A user has been added to Administrators Group, </description>
<description>Black Energy APT Phase 4 may have begun.</description>
<group>windows,pci_dss_8.1.2,pci_dss_10.2.5,group_changed,win_group_changed</group
>
</rule>
```

## 6. DISCUSSION and RESULTS

APTs are sophisticated and prolonged attacks. Traditional security solutions may not always be effective in special APT attacks. Due to the nature of an APT attack, intruders may be able to bypass existing security systems. SIEM's contribution to existing security solutions can boost the defense in such an environment. The position of SIEM cannot be instant monitoring or prevention but can provide meaningful data to those who follow its process.

- This paper introduced SIEM rules to strengthen the security defense line.
- The rule-based approach allows for the creation of alerts when file movements, registry changes, and privilege escalations occur.
- Rules on these three different types of behavior were created on the Wazuh platform and examined in the section above.
- The proposed WAZUH rulesets have been successfully tested in the SIEM project of one of the metropolitan city municipalities of Türkiye for the last five years. So far, no APT attacks that could have been detected by the rulesets defined in this paper were detected. That result shows that the APTs our rulesets can see were not tried in that specific municipality, for they would have been caught up otherwise.
- So far, we have created 30 new rules that can be integrated into the WAZUH environment.

## 7. CONCLUSION and FUTURE WORK

The three examples above show that similar rules can be produced for all APTs and positioned under the APT heading in the SIEM environment.

The 30 new rules we have created will be introduced in a subsequent paper.

The currently available rulesets are in GITHUB; access is provided in the "data availability statement" below.

However, future research will focus on network movements, memory moves, and e-mail behaviors within each APT attack. The specific rules will be created for specific APT attacks over other indicators. This scheme will allow early feedback on many indicators when an APT attack occurs.

## DATA AVAILABILITY STATEMENT

The rulesets associated with this study have been deposited in GITHUB at the address **https://github.com/ademsim/ossec-apt-rules**

## ACKNOWLEDGMENTS

The early version of this manuscript was prepared from a doctoral dissertation titled "Detection of APT Attacks Using SIEM Rules," defended at Yasar University, Department of Computer Engineering, in 2018. Additionally, it was presented at "the 3rd International Scientific-Practical Conference on Modern Information, Measurement, And Control Systems: Problems, Applications And Perspectives 2022 (MIMCS'2022)" on November 04-05, 2022, Antalya, Turkey.

The authors wish to thank the anonymous referees for their valuable contributions in making this research paper precise & presented in superior quality.

## REFERENCES

1. J. Lee, B. Bagheri, H. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems", Manufacturing Letters, Vol. 3, January 2015, Pages 18-23.

2. C. Tankard, "Advanced Persistent threats and how to monitor and deter them", Network Security, Vol. 2011, Issue 8, 2011, Pages 16-19.

3. Harknett, R. J. and Stever, J. A., "The New Policy World of Cybersecurity", Public Administration Review, Vol. 71, 2011, Pages 455-460.
4. M. Kenney, "Cyber-terrorism in a post-stuxnet world," Orbis, Vol. 59, Issue 1, Pages. 111–128, 2015.

5. Kaspersky Lab, "The Darkhotel Apt - A Story Of Unusual Hospitality", Version 1.1, November 2014.

6. Kaspersky Lab, "Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage", https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/, October 1, 2018.

7. Group IB and Fox It, "Anunak: APT Against Financial Institutions". https://www.group-ib.com/resources/research-hub/anunak-apt/, October 2, 2018.

8. P. S. Radzikowski, "CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation", http://drshem.com/2016/02/11/cybersecurity-expanded-look-apt-life-cycle-mitigation/#footnote-dsp-5061.2, October 10, 2018.

9. Dell, "Lifecycle of an Advanced Persistent Threat", 2012, http://www.redteamusa.com/PDF/Lifecycle%20of%20an%20Advanced%20Persistent%20Threat.pdf, October 10, 2018.

10. Sekharan, S. S., & Kandasamy, K., "Profiling SIEM Tools and Correlation Engines for Security Analytics", WiSPNET 2017 Conference, 2017, Pages 717-721.

11. Raja, N. M., & Vasudevan, R. A., "Rule Generation for TCP SYN Flood attack in SIEM Environment", 7th International Conference on Advances in Computing & Communications, 2017, Pages 580-587.

12. Anthony, R., "Detecting Security Incidents Using Windows Workstation Event Logs", SANS Institute, 2013, Pages 8-15.

13. Bryant, Blake D. and Hossein Saiedian. "A novel kill-chain framework for remote security log analysis with SIEM software." Computers & Security Vol. 67, 2017, Pages 198-210.

14. Chuvakin, A., "On "Output-driven" SIEM", http://blogs.gartner.co (Alladi, Chamola, & Zeadally, 2020)m/anton-chuvakin/2012/09/24/on-output-driven-siem/, September 8, 2018.

15. Alladi T., Chamola V., Zeadally S., "Industrial Control Systems: Cyberattack trends and countermeasures", Computer Communications, Vol. 155, 2020, Pages 1-8.

16. Mohammed A., Neetesh S., Peter B., "Investigating Ssable Indicators Against Cyber-Attacks in Industrial Control Systems", Proceedings of the 17th Symposium on Usable Privacy and Security, 2021.

17. Atluri V., Horne J., "A Machine Learning based Threat Intelligence Framework for Industrial Control System Network Traffic Indicators of Compromise", SoutheastCon 2021, Atlanta, GA, USA, 2021, Pages 1-5.

18. Powell M., Brule J., Pease M., StoufferK., Tang C., Zimmerman T., ... & Zopf M., "Protecting Information and System Integrity in Industrial Control System Environments", NIST, 2022.

19. Toker F.S., Ovaz Akpinar K., ÖZÇELİK İ., "MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, Pages 1-6.

20. Zahid H., Hina S., Hayat M. F., Shah G. A., "Agentless Approach for Security Information and Event Management in Industrial IoT", Electronics, 2023, Pages 1831.

21. ScienceSoft, "Siem-Based Apt Protection", https://www.scnsoft.com/services/security/siem/apt-protection retrieved October 12, 2018.

22. IBM Qradar, "IBM Security Qradar Suite", https://www.ibm.com/qradar, May 12, 2023.

23. HP ArcSight, "ArcSight Enterprise Security Manager", https://www.hpe.com/psnow/doc/c05100164.pdf?jumpid=in_lit-psnow-getpdf, May 12, 2023.

24. Wazuh, "The Open Source Security Platform", https://wazuh.com/, May 12, 2023.

25. Crowd Strike, "Indicators Of Attack Versus Indicators Of Compromise", https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperIOAvsIOC.pdf, October 13, 2018.

26. FireEye, "APT 28: A Window into Russia's Cyber Espionage Operations?", https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, March 13, 2017.

27. Symantec, "W32.Duqu The precursor to the next Stuxnet", Version 1.4, 2011, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/w32-duqu-11-en.pdf, April 14, 2017.

28. F-Secure," Blackenergy & Quedagh - The Convergence Of Crimeware and APT Attacks", https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf, January 23, 2017.

29. Kaspersky," Targeted Cyberattacks Logbook", https://apt.securelist.com/, May 17, 2023.