Security Solutions – Investigating Alerts in Digital Enterprises

Alexandra IOANID
University Politehnica of Bucharest
Academy of Romanian Scientists
alexandra.ioanid@upb.ro

Mihai-Andrei BACIU
University Politehnica of Bucharest
mihai_andrei.baciu@stud.aero.upb.ro

Abstract: During the last couple of years, cybersecurity attacks have continued to increase, not only in terms of vectors and numbers, but also in terms of their impact. Although the COVID-19 pandemic has also affected the threat landscape, with the shift to a hybrid office model, the attacks have begun to target companies through home offices as well. Due to the increase of their online presence, the transition of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity, and the use of new features of emerging technologies such as Artificial Intelligence (AI), cybersecurity threats are also growing. The paper presents how a security information and event management solution provides the necessary information to detect whether an attack or an unusual activity occurred inside the network of an organization. The tests were conducted following the MITRE ATT&CK tactics, techniques and procedures, in an isolated environment replicating an enterprise information system.
Keywords: Security solution, cyber security, digital enterprise.

INTRODUCTION

Security is one of the most important fields in information technology and communication. Everybody, from an individual to a large corporation, is concerned about securing their data, software and information. One short definition for cybersecurity is „The protection of software, hardware and data resources connected and stored on the Internet" (Thakur & Al-Sakib, 2020).

In general, cybersecurity deals with protecting personal financial data, commercial data, business-critical information, data integrity, business continuity, and the availability of online software services. The components of cybersecurity regulate physical access and control the malicious intrusion, allow authorized access, encrypt, and protect valuable information.

Cybersecurity relates to the technological processes and procedures to keep valuable data and software resources safe and secure from being tampered with, but physical security is a big component that affects cybersecurity both directly and indirectly.

https://doi.org/10.54851/v4i2y202209

In the modern digital environments, software resources are the core components for almost all businesses, public activities, governmental organizations, defense systems, and many other fields. Nowadays, physical security is also becoming a part of the information security issue.

Because of the automation of homes, factories, commercial areas, buildings, places, and the integration of Internet of Things (IoT) technologies, the entire physical security of any installation will also be influenced by cybersecurity threats through the Internet. Any minor breach in the physical layer of security can also pose a great threat to information security (Thakur & Al-Sakib, 2020).

Cybersecurity is classified into multiple elements:

- Network Security (NS)
- Information Security (IS)
- Application Security (AS)
- Disaster Recovery (DR) or Business continuity
- Leadership commitment
- Operational security (OPSEC)
- End-user education

It is important to say that cybersecurity is a continuous process of security awareness, strategic planning, implementation, monitorization, and evaluation. This means that cybersecurity is a vast field in the information technology environment, covering from human behaviors to technological procedures that impact the security of valuable resources stored and connected to the network, directly or indirectly.

INVESTIGATING ALERTS

The scope of the laboratory environment is to test TTP (techniques, tactics, and procedures) and generate IoCs (indicators of compromise) so we can better understand how an attack works and what kind of noise it generates, in order to be able to detect that attack.

Building an environment replicating an enterprise information system requires resources and it can be done on a hardware, physically (namely, on servers, switches, firewalls, routers etc.) or on a host machine, virtually (namely, on virtual machines used to simulate a corporate network). We created this environment via virtualization because it is easier to set up and backup and cheaper than buying the required hardware needed to set up a physical environment.

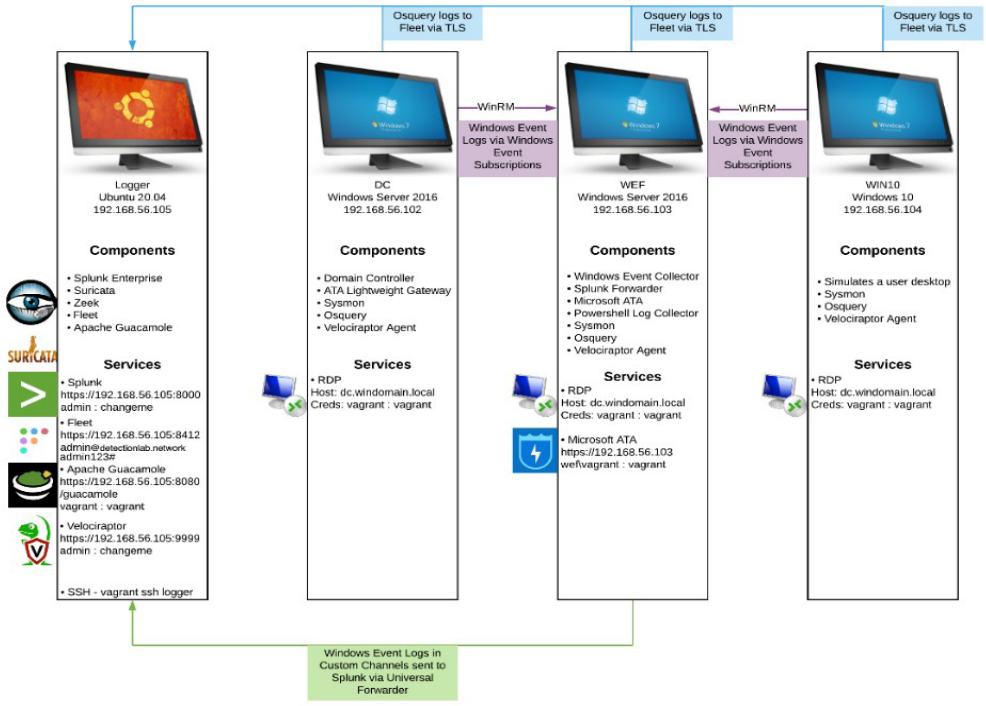

Fig. 1: *Environment Diagram (DetectionLab, n.d.)*

It is important to know the requirements used by an enterprise environment, in terms of operating systems, tools, and applications uses, in order to replicate it for the tests. The idea for this environment is to be easy to set up, but also to be easy to replicate a corporate information system.

DetectionLab is a repository containing various scripts that allow the automation of the process which creates an Active Directory environment online, with logging and security tools, using a variety of platforms that can also be found in enterprise data centers.

Environment Architecture

Because the scope of this environment is to mimic a real-world information system, Windows Active Directory (AD) will be used. Figure 1 displays a diagram of the environment that will be set up using DetectionLab repository.

Table 1: *Virtual machines roles*

Hostname	Operating System	Role
Logger	Ubuntu 20.04	Centralized logging with Splunk Enterprise (Free License), Fleet (Osquery manager), Suricata, Zeek, Velociraptor EDR and Apache Guacamole for remote access
DC	Windows 2016 Server (180 days evaluation)	Domain Controller with ATA lightweight gateway, Osquery, Velociraptor agent, Sysmon
WEF	Windows 2016 Server (180 days evaluation)	Windows Server with Event Collector, Splunk Forwarder, Microsoft ATA, Powershell Log Collector, Osquery, Sysmon, Velociraptor agent
WIN10	Windows 10 (180 days evaluation)	Windows workstation with agents (Sysmon, Osquery, Velociraptor)

All of the tools provided by the DetectionLab package are used in enterprise environments. Besides the Active Directory and Windows Advanced Threat Analytics, there are also Splunk SIEM and Suricata used for intrusion detection, and Zeek used for network traffic analysis. Table 1 presents the four virtual machines and their role.

Using those operating systems and tools, we can replicate a real-world environment in which we can perform various tests, in order to understand how an attack is performed and what artifacts are left in the form of system logs and events. Using those artifacts, we can set rules and develop the IoCs employed by security solutions to generate alerts.

Testing SIEM Capabilities

Generating Alerts Using MITRE ATT&CK TTP

MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures referred to as TTP that advanced persistent threats against enterprise networks. In addition, ATT&CK was created to document about adversaries' behaviors, information which was used within a research project called FMX. The objective of FMX was to investigate the use of endpoint telemetry data and analytics to improve post-compromise detection of adversaries operating within enterprise networks.

ATT&CK is a knowledge base of adversarial techniques – a breakdown and classification of offensively oriented actions that can be used against particular platforms. ATT&CK does not focus on the tools and malware that attackers use, but on how they interact with systems, during an operation. The relationships between tactics and techniques can be visualized in the ATT&CK Matrix.

The ATT&CK Matrix is one of the most recognizable aspects of ATT&CK because it is commonly used to show defensive coverage of an environment, detection capabilities in security products, and results of an incident or red team engagement (Don Murdoch, 2019). One of the tools used to emulate adversary attacks on an environment is „Atomic Red Team". It is an open-

source tool which uses individual tests that can be manually executed directly on a system or through the PowerShell command line. This tool allows us to test over 200 attack techniques mapped to the MITRE ATT&CK framework.

Because there are many TTP to test, a selection was made based on the techniques utilized by ATPs to get control of a compromised host and further access inside the network. The techniques that will be used for this test are:

- T1003.001 – OS Credential Dumping: LSASS Memory: This technique is used by attackers to access credentials stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores various credential materials in LSASS process memory. These credentials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement.
- T1047 – Windows Management Instrumentation: Attackers may abuse WMI to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access. An adversary can use WMI to interact with local and remote systems and to execute various activities such as gathering information for Discovery and remote Execution of files, as part of Lateral Movement.
- T1136.001 – Create Account Local Account: Adversaries may create an account to maintain access to the victim systems. Local accounts are those configured by an organization in order to be employed by users, remote support, services, or administration, on a single system or service. With sufficient access, the creation of such accounts may be used to establish secondary credentialed access that does not require persistent remote access tools to be deployed on the system.
- T1055.001 – Process Injection Dynamic-link Library Injection: Attackers use this technique to inject dynamic-link libraries (DLLs) into processes, in order to evade process-based defenses and, possibly, to elevate privileges. DLL injection is a method of executing arbitrary code in the address space of a separate process.

Those tests will be done using the Atomic Red Team tool from the WIN10 machine. Each test should be logged into the logger machine, and alerts should be generated to see what happened on the respective machine. Although we only ran tests for those techniques, there may be alerts triggered for different techniques based on what the test does to trigger an alert. In order to run a test, we have to import the Atomic Red Team module in PowerShell on our „victim" machine. To do this, we run the following command in PowerShell on the WIN10 machine: Import-Module „C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" - Force.

After the import of the module, AtomicRedTeam can be invoked to run the selected TTPs. To do this we simply run the Invoke-AtomicTest <Test_ID> command. For some tests there are also sub-techniques, so we must specify the sub-technique we want to use, by providing a number after the Test_ID in the command. The commands used to run the tests for the techniques described above are mentioned in Table 2.

Table 2: *Atomic Red Team Test invocation*

Technique	Atomic Red Team Command
T1003.001	Invoke-AtomicTest T1003.001
T1047	Invoke-AtomicTest T1047
T1136.001	Invoke-AtomicTest T1136.001
T1055.001	Invoke-AtomicTest T1055.001

Each command outputs some details regarding what is happening behind the scenes (see, for example, the output of the T1003 sub-technique 1 illustrated in Figure 2). As it can be seen, LSASS is used to create a credential dump in a temporary folder, under the user that runs the command; then the script invokes Mimikatz, an open-source software that allows users to view and save authentication credentials. In Figure 3, the output of Mimikatz shows the cleartext passwords for the Vagrant users and Administrator.

```
Done executing test: T1003.001-7 LSASS read with pypykatz
Executing test: T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1


    Directory: C:\Users\vagrant\AppData\Local\Temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/8/2022  11:50 AM       47071786 lsass_672.dmp


Done executing test: T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1
Executing test: T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
The system cannot find the path specified.
Done executing test: T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
Executing test: T1003.001-10 Powershell Mimikatz
```

Fig. 2: *Output of T1003.001 test*

```
  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 167418 (00000000:00028dfa)
Session           : Interactive from 1
User Name         : vagrant
Domain            : WIN10
Logon Server      : WIN10
Logon Time        : 5/8/2022 8:50:03 AM
SID               : S-1-5-21-4089106852-1179389713-3053946134-1000
        msv :
         [00000003] Primary
         * Username : vagrant
         * Domain   : WIN10
         * NTLM     : e02bc503339d51f71d913c245d35b50b
         * SHA1     : c805f88436bcd9ff534ee86c59ed230437505ecf
        tspkg :
        wdigest :
         * Username : vagrant
         * Domain   : WIN10
         * Password : (null)
        kerberos :
         * Username : vagrant
         * Domain   : WIN10
         * Password : (null)
        ssp :
        credman :
         [00000000]
         * Username : WIN10\vagrant
         * Domain   : TERMSRV/WIN10
         * Password : 1password2!
         [00000001]
         * Username : Administrator
         * Domain   : TERMSRV/WIN-DC
         * Password : 1password2!
```

Fig. 3: *Output of Mimikatza*

Showcasing Splunk SIEM

Splunk Enterprise Security is a security information and event management (SIEM) solution that detects internal and external attacks and offers threat management capabilities and intelligence. With applications developed by various security vendors, Splunk can also be integrated with the MITRE ATT&CK framework and display alerts generated using various TTP. This SIEM was chosen as it is used in many organizations and offers a free enterprise license with a limit regarding the number of logs it can take in a day.

After logging into the SIEM of our environment, the first image that appears is the one of the Dashboard that shows the number of events per hour, top events for Suricata, Zeek Network traffic, PowerShell events, and a lot of other useful information gathered from our systems. Figure 4 describes the dashboard of Splunk Enterprise.

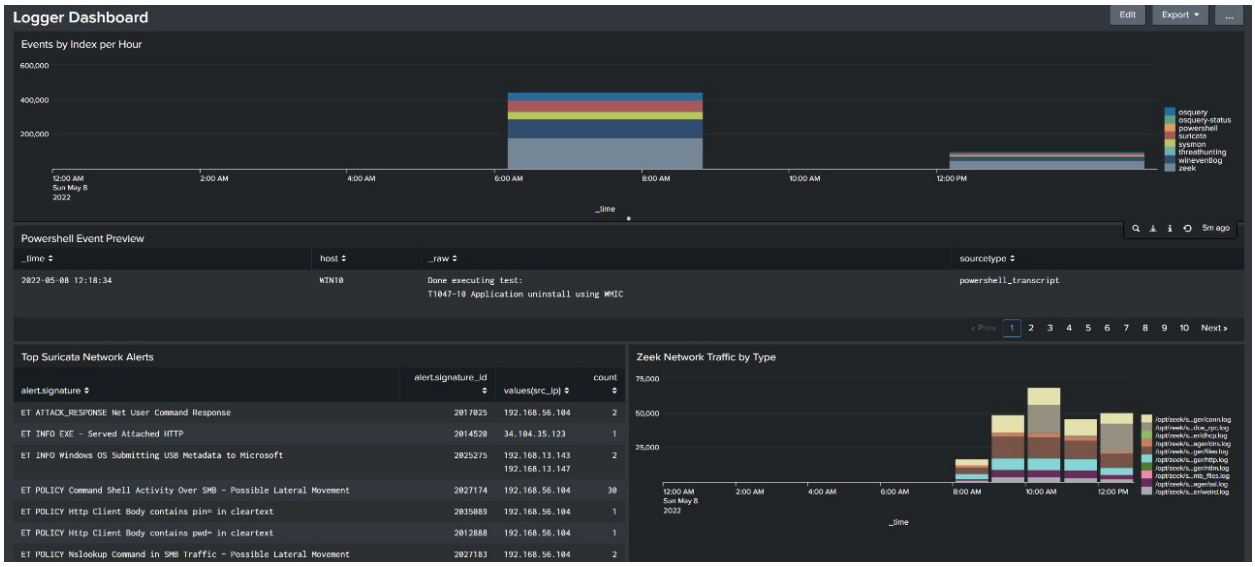

Fig. 4: *Splunk Enterprise Dashboard*

With the Threat Hunting app installed and configured in Splunk, the events that the SIEM catches are correlated with MITRE TTP, and alerts are generated based on the observed techniques. Figure 5 illustrates the Threat Hunting app dashboard that shows alerts regarding the tests done on WIN10 machine.

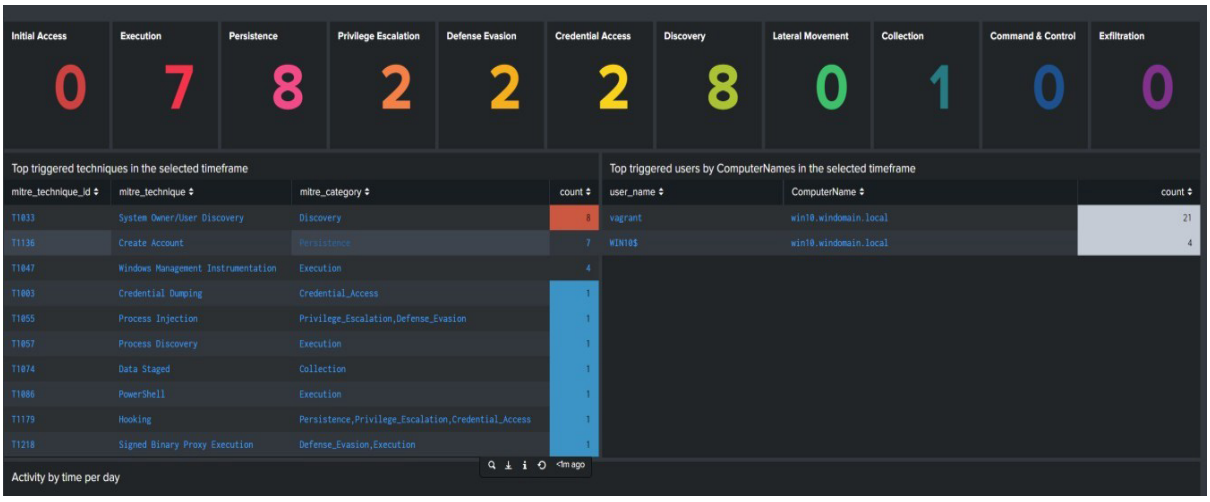

Fig. 5: *Threat Hunting Dashboard*

This dashboard shows us what MITRE TTP was triggered on our system. The Figure demonstrates that the tests triggered Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Collection TTP successfully.

By looking further into the Execution pane, you can see more information on what events triggered those alerts, as shown in Figure 6. Splunk also offers information regarding the computer name, the user that started the process which generated the event and the process command line. All this information is helpful to show what happened on the system that sent those events and generated alerts in the SIEM.

Fig. 6: *Events that triggered Execution TTPs*

Investigating logs

Using Splunk to Investigate Alerts

As an analytics-driven SIEM tool, Splunk collects, analyzes, and correlates high network volumes, logs, events, and other machine data in real-time. It continuously monitors all network resources and activities to detect anomalous behavior. Using the information provided by Splunk, we obtain get a detailed, data-driven view of the performance, health, and vulnerabilities of the network. Malicious or high-risk activities are automatically reported with contextual information regarding the threat.

System Compromise and Highest Priority alerts should always receive attention as soon as they arrive. They usually warrant an investigation ticket, meaning the alert should flow through a defined workflow and record-keeping process to mark them as false positive or true positive. Some alerts can be handled easily, while other will require investigation. For every data source that can provide information to help validate or close the alert, the supporting data from the system that caused the alert must be checked.

Because the logs are forwarded in the Splunk SIEM, we can see them clearly within the web application. For example, for the Credential Access TTP, we can see the log provided by the machine to SIEM in Figure 7, and we can also see that the Mimikatz tool was used to dump the credentials stored on the system.

Fig. 7: *Log indexed in Splunk*

Searching for PowerSploit will give us more information about this repository, as the creators' state is a „collection of Microsoft PowerShell modules that can be used to aid penetration testers" (GitHub, 2017). With all this information, we can assume that in a real-world scenario, this was most likely a positive alert, and the host that triggered it is most likely to be compromised. If we investigate what happened after the credential dumping, we can see the log in Figure 8 showing that the Vagrant user created a local account named T1136.001 and added it to the local administrators' group. This is an unusual behavior, and the security team should flag the workstation as compromised and investigate it further.

05/08/2022 12:10:48 +0000, search_name="[T1136] Create Account", search_now=1652012580.000, info_min_time=1652011680.000, info_max_time=1652012580.000, info_search_time=1652012581.349, indextime="05/08/2022 12:10:49", user_name=vagrant, process_parent_path="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe", event_description="Process Creation", process_parent_id=0x1ad8, mitre_category=Persistence, mitre_technique="Create Account", process_id=0x14f0, process_command_line="\"C:\\Windows\\system32\\cmd.exe\" /c \"net user /add \"T1136.001_Admin\" \"T1136_pass\" & net localgroup administrators \"T1136.001_Admin\" /add\"", mitre_technique_id=T1136, ComputerName="win10.windomain.local", process_path="C:\\Windows\\System32\\cmd.exe"

Fig. 8: *New user created log*

Threat hunting

Threat hunting can be defined as leveraging information to proactively search out and identify if an attacker successfully compromised a network, applications, data sources, or systems on an iterative basis. Threat hunting begins by establishing a hypothesis or a testable condition used to find a compromise (Don Murdoch, 2019).

When it comes to making use of data sources, security professionals can use as many as they can and work to determine the current network and system state as a known baseline.

For example, if we establish a baseline that users don't need to create local accounts in the administrator group on their workstations, it should be investigated when we see an event regarding this behavior.

Once a baseline and the data are understood, models, tests, and other hypotheses about the detection measures that can initiate a threat hunting effort can be developed. After defining the hunt activities, various tools can search for threat indicators.

These tools allow for a comprehensive analysis of the operating environment on the Windows platform: registry changes, file system changes, IP addresses communication patterns, and binary comparisons by hash to known malware databases. If the hunt team finds something, an incident should be triggered, and, afterward, the appropriate processes to clean up the network should be found.

Threat hunting benefits the organization in multiple ways. Firstly, hunting maximizes the security spent through data mining, analysis, reporting, and improved alerting. Secondly, it can also detect deviations against normal system operations, and error conditions can be detected through summary data review.

Thirdly, by keeping a close eye on the environment, adversaries can be detected earlier, while damage control can be more effective, with the specific objective of reducing dwell time. Finally, human review and analysis can define baselines for traffic volume, traffic velocity, commonly used sites, and data flow patterns which can then be used to define automation and to improve the alerts.

CONCLUSIONS

The concept of cybersecurity is an essential matter in the era of digitalization. In the first part, we revised the structural elements of cybersecurity, how the CIA triad represents the fundamental objective in information security, and how adversaries are using different types of cyberattacks to exploit and disrupt the normal flow of data.

Security is about protecting business goals and assets. It means providing a set of controls and policies matched to the organization's needs, derived from an assessment and analysis of risks. The ocean of change is constantly battering organizations with many ups and downs to disrupt their risk profile. Security professionals must proactively head off the risks introduced by changes, as per requirements of security policies.

This research paper reviews the basics behind cyber threats and vulnerabilities and focuses on the security solutions and how they can aid a security professional in identifying and responding to cyber threats. It also covers threat models and frameworks that help understand

cyber threat behavior and describes how an organization can defend against cyber threats using standards, guidelines and procedures. The last part focuses on how a SIEM solution works and how it can be used in a real-world scenario to determine if an alert is positive and if an actual event occurred within the system of an organization.

REFERENCE LIST

DetectionLab (n.d.). *Network.* Retrieved from https://detectionlab.network/images/lab.png?width=1200

Don Murdoch, B. M. (2019). Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: Notes from the field. *A condensed field guide for the Security Operations team*, *2*(2). CreateSpace Independent Publishing Platform.

Thakur, K., & Al-Sakib, K. P. (2020). *Cybersecurity Fundamentals - A Real-World Perspective* (1st ed.). Boca Raton: CRC Press.

GitHub. (2017). *PowerShellMafia*. Retrieved from https://github.com/