

Research Focused on Threat Detection Rule Development utilising the Splunk Attack Range to fortify Cybersecurity Analysis.

School of Computing - National College of Ireland

MSc Cybersecurity – Research Project

Rajuaravind Sankar

Student ID: X22250042

Supervisor: Mark Monaghan

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name: Rajuaravind Sankar

Student ID: X22250042

Programme: Cybersecurity **Year:** 2023-2024

Module: Research Project

Supervisor: Mark Monaghan

Submission Due Date: September 2024

Project Title: Research Focused on Threat Detection Rule Development utilising the Splunk Attack Range to fortify Cybersecurity Analysis.

Word Count: 6347 words **Page count:** 22 pages

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rajuaravind Sankar
.....

Date: July 2024
.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Table of Contents

1 Introduction.....	4
1.1 Research Question (RQ).....	5
1.2 Importance of the research.....	5
1.3 Objectives of the research	5
2 Literature Review	5
3 Research Methodology	7
4 Utilized Resources and Technologies.....	8
5 Research Background	9
5.1 SIEM Tools.....	9
5.2 Threat Detection Rule.....	10
5.3 MITRE ATT&CK Framework.....	10
6 Splunk Attack Range Tool	11
6.1 Attack Simulation Engines	12
6.2 Splunk Attack Range Deployment Options.....	12
6.3 Terraform and Ansible with the Splunk Attack Range	12
6.4 Splunk Attack Range Command Actions.....	13
7 Implementation	13
7.1 Selection of Deployment	14
7.2 Splunk Attack Range Environment Setup	14
7.3 Attack Simulation – OS Credential Dumping	16
7.5 Attack data Built-in analysis with Splunk Enterprise	18
7.6 Threat detection rule development Phase	19
8 Evaluation	20
9 Future Work.....	21
10 Conclusion	22

Research Focused on Threat Detection Rule Development utilising the Splunk Attack Range to fortify Cybersecurity Analysis.

Rajuaravind Sankar - X22250042

Abstract

The research focused on the developing threat detection rule using the Splunk Attack Range tool to enhance the organization infrastructure security. In this research work, the key challenge of replicating production environment to simulate attack data is tackled with the Splunk Attack Range tool, which is a vital for effective threat detection rule development. This study delves into strategies to overcome the time-consuming nature of this replication process. By optimizing the simulation, organizations can efficiently create threat detection rules tailored to their specific environments. The development of efficient threat detection rule plays a vital role in identifying and eliminating the malicious actor in the network, therefore strengthening the organization infrastructure. The ultimate goal of the research aims in the improvement of defence security by enabling the development of accurate and robust threat detection alerts to counter the evolving cyber threats in the modern IT world.

Keywords: Threat Detection Rule, Splunk Enterprise, Splunk Attack Range, Security Analysis, SIEM, Attack Data.

1 Introduction

The deployment of an effective threat defence system in an organization's infrastructure have become crucial due to the escalating and advancing malicious threats in the recent years. An organization's IT Security Operations Center (SOC) team, which oversees monitoring potential threats, faces many challenges in deploying optimal threat detection rules within the organization's infrastructure. How to develop an efficient threat detection alert? - With the help of attack data, an optimal threat detection rule can be created by SOC team professionals, protecting the organization from malicious threats. The data dataset is a set of information collected from various cyber incidents and security attacks. It helps the Security Operational centre team to understand and analysis the nature of the attacks, tactics and techniques used and as well as the impact of the attacks. Although attack data can be found on the internet, it is still challenging to write an effective threat detection rule as the attack data is not simulated which may leads to missing of some important field artefact in the attack data. In some case, the attack data doesn't match the organisation's environment, as each organisation's environment infrastructure varies, for example, the attack data on windows 2016 server can't help effectively to deploy a potential threat detection rule windows 2019 server. To simulate the attack data on their own based on their infrastructure, organizations have to do a lot, and it will be quite challenging and time-consuming. The Splunk threat research team brought forth a plan to address the complex, time-consuming challenges with the Splunk Attack Range tool, which will be utilized in this research on fortifying the organization's IT security defence. This research also focused on addressing the limitation

identified by Korving and Vaarandi (2023) in simulating attack data within production-like environments for Windows domain controllers, Windows servers, and Windows workstations, as well as enhancing the analysis of the simulated attack data.

1.1 Research Question (RQ)

Developing a threat detection rule using the security incident attack data available on the internet may not be very effective, as it has a possibility to lead false negatives threat alerts with the developed threat detection rule. Since each organization's environment is unique, attack data must be simulated in a test environment that closely mirrors the production environment. Given that replicating the production environment is both challenging and time-consuming, what can be done to address the issues of time consumption and high resource usage when simulating attack data and creating an effective threat detection rule?

RQ: “How does the utilization of Splunk Attack Range assist in the development of Threat Detection Rules?”

Based on my research, the potential features of Splunk Attack Range for developing threat detection rules will be explored. Therefore, Contributing to the Security Operational Centre (SOC) team with an optimal threat detection rule.

1.2 Importance of the research

Implementing threat detection rules is a crucial defence mechanism against cyber threats and attacks in an organization. Developing and deploying effective threat detection alerts are vital for organizational security. This research explores the capabilities of the Splunk Attack Range, a publicly available tool, which allows organizations to simulate attacks and create robust threat detection rules to prevent malicious activity within their network.

1.3 Objectives of the research

The objectives of my research on the utilization of Splunk Attack Range in the development of threat detection rules are listed below.

1. To evaluate the Effectiveness of Splunk Attack Range Tool.
2. To identify Key Features of Splunk Attack Range Tool.
3. To develop Optimal Threat Detection Rules and enhance the organization’s defense mechanisms against cyber threats.

2 Literature Review

This literature overview provides a comprehensive review of past research on the utilization of scenario-based Attack Datasets, highlighting the contributions, challenges, and potential future

directions in this field. Utilizing these attack dataset resources plays a crucial role in enhancing an organization's defense systems.

A significant contribution to the cybersecurity analysis field using Attack Datasets is the study by Korving and Vaarandi (2023). Their research is particularly valuable for this review. The primary achievement of their work is the development of a publicly accessible toolkit that generates security datasets and aids in creating Intrusion Detection System (IDS) rules using these datasets. This effort is concentrated on an open-source, customizable tool named DACA, which facilitates the execution of automated attack scenarios. DACA operates as a Command Line Interface (CLI) tool, built in Python, using configuration files to produce attack scenario datasets.

The study also compares other tools such as Splunk Attack Range, Deter, Cloudlab, and Detectionlab. However, it provides limited information on data analysis derived from the generated attack scenario datasets, as it does not utilize any data analysis tools. The paper discusses and validates a DNS tunneling scenario. Notably, DACA is designed solely for local VM-based scenarios, making it unsuitable for setting up attack data simulation labs in cloud environments. The tool, initially developed by Korving (2022), was noted to be underdeveloped and not user-friendly in its original form. Furthermore, it lacks full automation for lab environment setup, complicating the simulation of attack data.

Both studies by Korving (2022) and Korving and Vaarandi (2023) exhibit inefficiencies in validating simulated attack data. Additionally, the predominant focus on generating attack data in these papers overshadows the advancement and implementation of Threat Detection Rules.

The research paper by Mustafa, H.M. et al. (2023) presents a reconfigurable Cyber-Power Grid Operation designed to simulate cyber-physical attacks on systems. It highlights two primary use cases: implementing cyberattacks similar to the GridEx exercises and validating the CP-TRAM and SyncAD tools. The study employs the Splunk tool as a standard Security Information and Event Management (SIEM) system for collecting, indexing, and analyzing data from the created testbed. Splunk also plays a crucial role in detecting and analyzing events, supporting incident response, and developing defense strategies.

In their 2022 research, Ananthapadmanabhan and Achuthan propose an approach to enhancing cloud security through the integration of threat modeling with Splunk. This study addresses the increasing cyber threats faced by cloud platforms by combining threat modeling with real-time threat intelligence to create a robust defensive model. Splunk Dashboards are used for visualizing and analyzing threats, enabling effective monitoring and response to security incidents.

The research by Su, T. et al. (2016) focuses on detecting Denial-of-Service (DOS) attacks using the Splunk SIEM tool. After capturing the attack data, it is transferred to the Splunk environment for analysis. The study involves analyzing TCP SYN attack patterns and identifying malicious TCP flag combinations in XMAS attacks. A case study is presented where packet data collected from a FortiGate firewall is uploaded to Splunk for analysis, demonstrating how Splunk can detect

anomalies in network traffic and identify potential DDoS attacks. Visualization techniques, such as mapping source and destination IPs, are utilized to understand attack origins and targets.

Similarly, the research by Selvaganesh, M. et al. (2022) showcases how Splunk can be used to detect malicious events through custom search queries and alerts. It validates the effectiveness of the Splunk SIEM tool in identifying brute force attack scenarios. The paper by Korving and Vaarandi (2023) also mentions the notable aspect of the Splunk Attack Range tool, providing an overview of its capabilities in setting up lab environments and comparing attack dataset simulations with other available tools. However, this paper primarily focuses on utilizing the DACA tool for the implementation and development of alert rules, but it lacks detailed information on the development process, implementation, and validation.

3 Research Methodology

In this section, the methodologies and procedures utilized to achieve the research objective are outlined.

The research methodology for Threat Detection Rule Development utilising the Splunk Attack Range to fortify Cybersecurity Analysis will be the combination of qualitative and quantitative methods. This mixed methods approach enables a comprehensive analysis of the effectiveness of Splunk attack range tool in developing optimal threat detection rules. The research methodology begins with an extensive literature review to collect existing information on threat detection rule development, attack datasets, and Splunk capabilities. The key research by Korving and Vaarandi (2023), Mustafa, H.M. et al. (2023), Ananthapadmanabhan and Achuthan (2022), Su, T. et al. (2016), and Selvaganesh, M. et al. (2022) will be critically analysed to understand the current state of research in this field.

In the implementation phase, an experimental setup will be created to simulate various attack scenarios using Splunk Attack Range. This controlled test environment will mimic a production environment, allowing for the generation and analysis of data from simulated attacks such as DNS tunnelling, DDoS attacks, and brute force attacks. The data analysis will focus on evaluating the key features of Splunk Attack Range that facilitate the development of threat detection rules. This includes assessing how these features contribute to reducing time consumption and resource usage in attack simulation and rule creation. Developed threat detection rules will be tested for their effectiveness in detecting and responding to simulated attacks.

For validation, the developed threat detection rules will be tested in a production-like environment to ensure their accuracy in detecting real-world threats without generating false negatives. The research process, including the experimental setup, attack scenario simulations, and rule development, will be meticulously documented. Recommendations for organizations on effectively utilizing Splunk Attack Range for developing threat detection rules will be offered, along with best practices and strategies for optimizing the use of attack simulation tools to enhance cybersecurity defenses. This research methodology aims to deliver a thorough evaluation of the

Splunk Attack Range tool and its potential in improving the development of threat detection rules, thereby contributing significantly to the overall security posture of organizations.

4 Utilized Resources and Technologies

In this section provide a comprehensive overview of the technologies and resources used in the research. The section also includes the detailed description of each tool, software, platform and service employed during the research.

Resource\Technology Name	Description
Amazon Web Services	Cloud computing platform offering a wide range of services including computing, storage, and databases.
Amazon Elastic Compute Cloud (EC2)	Provides resizable compute capacity in the cloud, allowing users to run virtual servers (instances) with various configurations.
Virtual Private Cloud (VPC)	Allows users to create isolated networks within the AWS cloud, providing control over IP address ranges, subnets, route tables, and network gateways.
Elastic IP Address	A static, public IP address designed for dynamic cloud computing, which can be associated with instances
Identity and Access Management (IAM)	Enables users to manage access to AWS services and resources securely, providing fine-grained control over user permissions and roles.
Docker	A platform that automates the deployment, scaling, and management of applications using containerization technology, allowing applications to run consistently across different environments.
Python Programming Language	Interpreted programming language known for its readability, simplicity, and versatility, widely used.
Terraform	Allows users to define and provision infrastructure using a declarative configuration language.
Ansible	An open-source automation tool used for configuration management, application deployment, and task automation, utilizing simple, human-readable YAML files for its playbooks.
Splunk Enterprise	A platform for searching, monitoring, and analyzing machine-generated big data via a web-style interface, used for log management, security monitoring, and operational intelligence.
Splunk Machine learning Toolkit App	An app for Splunk Enterprise that provides a suite of tools and algorithms for applying machine learning techniques to data analysis and predictive modeling within the Splunk environment.
Enterprise Security Content Update App	An app for Splunk that offers regularly updated security content and use cases, helping organizations enhance their security monitoring and incident response capabilities.
MITTRE ATT&CK Framework	Acknowledged resource that catalogs the tactics, techniques, and procedures (TTPs) employed by adversaries in cyber-attacks.

Atomic Red Team Attack Simulation	A library of pre-built attack simulation tests designed to help organizations assess their security posture by emulating tactics and techniques used by real-world adversaries.
Purple Sharp Attack Simulation	An open-source tool that integrates with existing security infrastructures to perform adversarial simulations, helping organizations identify gaps in their defenses and improve detection and response capabilities.

5 Research Background

5.1 SIEM Tools

Security Information and Event Management (SIEM) tools play a prominent role in preventing organizations by providing live analysis of security events and alerts generated from the machine-generated data like web application and network devices. The SIEM tools are capable of collecting and normalizing data from a wide variety of sources across the organization infrastructure. This data collection mechanism enables the SIEM tools to achieve a consolidated view of an organization's security posture. By combining the data from different sources, SIEM tools understand the pattern of the events, therefore providing an efficient view to detect and respond to the security threats.

The combination of advanced analytics and machine learning features in SIEM tools provides effectiveness in working with data to detect and respond to security threats. The machine learning algorithms analyze the historical data to understand how normal behaviour looks like for the users and the systems in an organization. The SIEM tools provide a proactive approach to monitor the machine-generated data from the organization's network to detect and respond to the potential threats and prevent damage to the organization network. SIEM Tools are capable of ranking the threat detection alerts by their seriousness and possible effect, allowing security teams to tackle the most urgent concerns initially. Tools such as QRadar, Splunk, Sentinel, Graylog, among others, are utilized within the IT sector for identifying threats to aid in the prevention of cyber-attacks.

The SIEM tools play a vital role in Security Operation Centres (SOCs) monitoring for the security analysts. When the threat detection alert is triggered, the security analysts investigate the root cause of the alert, it may be true positive or false negative, if the triggered alert is true positive the actions needed to resolve the issue is taken by the SOC Team. This may involve isolating affected systems, blocking malicious IP addresses, or applying patches to vulnerable systems. Through continuous monitoring and analysis, SIEM tools enable organizations to maintain a robust security posture by promptly identifying and addressing potential threats.

This research explores the Splunk SIEM and Splunk attack range tool capabilities for the development of effective threat detection rules. By utilizing these tools, organizations can strengthen their security infrastructure, predict potential threats, and protect their essential assets while ensuring the integrity of their IT systems.

5.2 Threat Detection Rule

Threat detection method involves monitoring infrastructure to identify attacks that bypass the traditional security measures in an organization. The detection method leverages various techniques including endpoint monitoring, behaviour-based detection, signature-based detection and user-based detection. The goal of threat detection is to identify and neutralize the attacks proactively, preventing them from escalating into breaches. The threat detection rule minimizes the number and severity of security compromises, enhancing the overall security of the organization environment. Integrating Optimal threat detection rule into an organization's security program is crucial for data protection.

The threat detection rules come in various forms, including scheduled rules, near-real-time (NRT) rules, and anomaly rules, each serving unique functions and offering specific benefits. Scheduled threat detection rules operate on a fixed timetable, running at regular intervals to check for specific patterns or indicators of compromise. For instance, a rule might be configured to scan logs for unauthorized access attempts every hour. These rules are useful for ensuring consistent monitoring without overwhelming the system's resources, balancing thorough analysis with efficiency. Scheduled rules in Splunk can be set up using its alerting feature, running predefined searches at specified intervals.

The real time threat detection rules enable continuous monitoring of the machine generated data from the organization network. The real time detection rule is deployed in the cases where the threat severity is high and need to response the threat incident as soon as they occur, significantly reducing potential damage from cyber-attacks. For example, a real time threat detection rule from, a Splunk Enterprise is triggered as there an unusual high number of failed login attempts are made by a user in the network, indicating real time potential brute force attack.

Anomaly rules focus on identifying deviations from normal behaviour within the network. These rules are based on baseline behaviour patterns established over time, flagging activities that significantly differ from these norms. Anomaly detection is particularly useful for uncovering sophisticated threats that may not match known attack patterns but still represent a risk due to their abnormal nature. For example, an anomaly rule might alert administrators if an internal user suddenly starts accessing sensitive data at odd hours, suggesting a potential insider threat. Anomaly detection in Splunk often utilizes its machine learning toolkit to establish baselines and identify deviations, enabling proactive threat identification and mitigation.

5.3 MITRE ATT&CK Framework

MITRE ATT&CK Framework is a detailed matrix that categories the various tactics and techniques used by cyber experts throughout different attack stages. The framework helps the organization in understanding the specific behaviours and methods employed by attackers, allowing them to develop targeted threat detection rules. Mapping these techniques, the framework provides a structural approach to identifying and mitigating potential threats. The Framework helps

the organization move beyond signature-based detection to behaviour-based detection approaches, enhancing their security posture by detecting threats at various attack points.

By regularly updating detection rules according to the evolving techniques documented in the framework, organizations can stay ahead of emerging threats. The MITRE ATT&CK Framework also provides context around each technique, helping fine-tune detection rules for greater accuracy and reduced false positives. The MITRE ATT&CK Framework enables organization to enhance their ability to detect, respond, and mitigate advanced threats effectively.

The Splunk Attack range tool's attack simulation engines such as Atomic Red Team and PurpleSharp are aligned with the MITRE ATT&CK framework, therefore providing an efficient method to detect and response to the potential cyber threats. This alignment enables security professionals to create robust threat detection rules using the tactics and techniques from the MITRE ATT&CK framework.

6 Splunk Attack Range Tool

The Splunk Threat research Team, came up with the idea of developing a tool to enhance the attack data simulation and to support in the development of efficient Threat detection rule. The Splunk Attack range tool is an open source project available for both cloud and local environment. The tool spins up the attack simulation environment, simulates attacks and forward the data to the Splunk SIEM in the attack simulation environment. The created simulation environment by the Splunk attack range tool can be used to build an optimal threat detection rule.

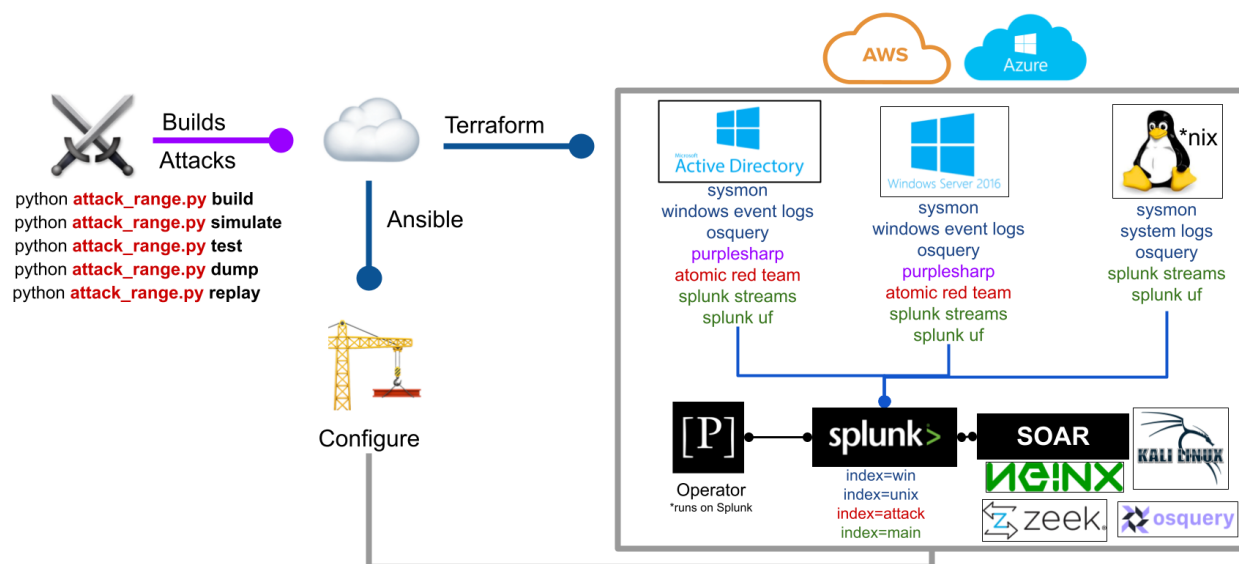


Figure 1.1 – Splunk Attack Range Architecture

The Splunk Attack Range is a platform designed for threat detection development, addressing three key challenges in threat detection engineering. It enables users to swiftly construct a small lab environment that closely mimics a production setting. It facilitates attack simulations using various

engines, including Atomic Red Team and Caldera, to produce authentic attack data. It fits perfectly into any CI/CD pipeline, making it easy to automate the testing of detection rules.

6.1 Attack Simulation Engines

The Splunk attack range uses various simulation engines to simulate attacks and generate realistic attack data. The attack simulation engines including atomic red team, Purple Sharp and prelude Operator. The Atomic red team is an open-source library of tests aligned with the MITRE ATT&CK framework, enabling security teams to test their environment quickly and consistently. Purple Sharp, another open-source tool written in C#, simulates adversary techniques specifically within Windows Active Directory environments. Purple Sharp provides a valuable telemetry to assess and enhance the effectiveness of detection engineering programs.

6.2 Splunk Attack Range Deployment Options

The Splunk Attack Range tool provides several deployment options to suit different needs. Users can set up simulation environments locally with VirtualBox and Vagrant or deploy it on cloud platforms like AWS and Azure for enhanced scalability. Additionally, a Docker image is available for those who prefer containerized setups. These diverse options allow organizations to seamlessly integrate the Splunk Attack Range into their infrastructure, whether they are using on-premises or cloud-based systems.

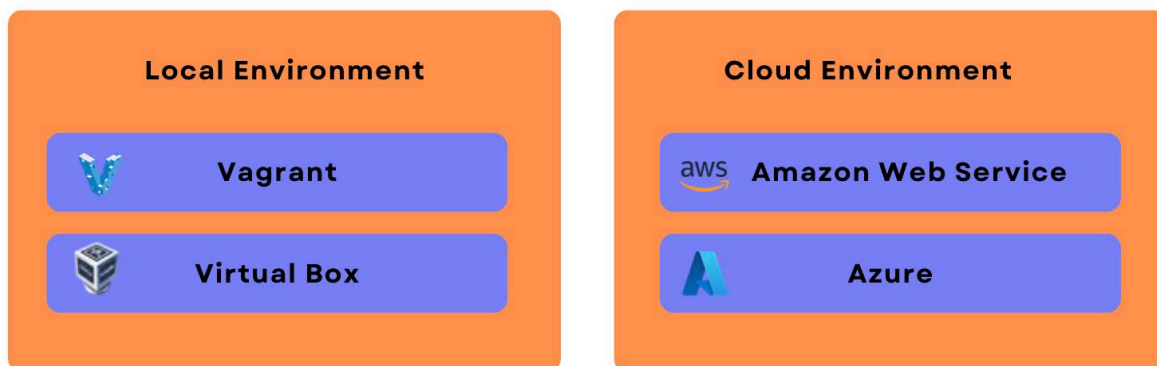


Figure 1.2 – Splunk Attack Range Deployment options

6.3 Terraform and Ansible with the Splunk Attack Range

In Splunk attack range tool, Terraform and ansible plays a crucial role in automating the setup environment and configuration of attack simulation. Terraform automates the provisioning of the necessary infrastructure with the servers configured in Splunk attack range configuration file on the AWS platform. It ensures the consistent and reliable environment for attack simulation. Once Terraform has established the infrastructure, Ansible takes over to configure and deploy the simulation on the infrastructure. Together, these tools simplify and automate the process, making the setup of the attack range more efficient and reliable.

```

● rajuaravindsankar@Rajuaravinds-MacBook-Pro aws % pwd
/Volumes/aravindx/Attack range repo/attack_range/terraform/aws
○ rajuaravindsankar@Rajuaravinds-MacBook-Pro aws %
● rajuaravindsankar@Rajuaravinds-MacBook-Pro aws % tree
.
├── backend.tf.tmp
├── main.tf
├── modules
│   ├── kali-server
│   │   ├── resources.tf
│   │   └── variable.tf
│   ├── linux-server
│   │   ├── outputs.tf
│   │   ├── resources.tf
│   │   └── variable.tf
│   ├── network
│   │   ├── output.tf
│   │   ├── resources.tf
│   │   └── variable.tf
│   ├── nginx-server
│   │   ├── resources.tf
│   │   ├── variable.tf
│   ├── phantom-server
│   │   ├── outputs.tf
│   │   ├── resources.tf
│   │   └── variable.tf
│   ├── splunk-server
│   │   ├── resources.tf
│   │   └── variable.tf
│   └── windows
│       ├── outputs.tf
│       ├── resources.tf
│       └── variables.tf
└── zeek-server
    ├── resources.tf
    └── variables.tf

```

Figure 1.3 – Terraform Configuration files tree view

```

○ rajuaravindsankar@Rajuaravinds-MacBook-Pro ansible %
● rajuaravindsankar@Rajuaravinds-MacBook-Pro ansible % pwd
/Volumes/aravindx/Attack range repo/attack_range/terraform/ansible
○ rajuaravindsankar@Rajuaravinds-MacBook-Pro ansible %
● rajuaravindsankar@Rajuaravinds-MacBook-Pro ansible % tree
.
├── linux_server_post.yml
├── nginx_server_post.yml
├── phantom_server.yml
├── roles
│   ├── azure_logging
│   │   ├── tasks
│   │   │   ├── azure_logging.yml
│   │   │   └── main.yml
│   │   └── templates
│   │       ├── inputs.conf.j2
│   │       ├── mscs_azure_accounts.conf.j2
│   │       └── mscs_azure_audit_inputs.conf.j2
│   ├── bad_blood
│   │   ├── tasks
│   │   │   ├── install_badblood.yml
│   │   │   ├── main.yml
│   │   │   └── run_badblood.yml
│   ├── carbon_black_cloud_agent
│   │   ├── tasks
│   │   │   ├── install.yml
│   │   │   └── main.yml
│   ├── carbon_black_cloud_logs
│   │   ├── files
│   │   │   └── local.meta
│   │   ├── tasks
│   │   │   ├── config.yml
│   │   │   └── main.yml
│   │   └── templates
│   │       └── inputs.conf.j2
│   ├── cloudtrail_logs
│   │   ├── tasks
│   │   │   ├── configure_inputs.yml
│   │   │   ├── main.yml
│   │   └── templates
│   │       ├── aws_account_ext.conf.j2
│   │       └── aws_inputs.conf.j2

```

Figure 1.4 – Ansible Configuration files tree view

6.4 Splunk Attack Range Command Actions

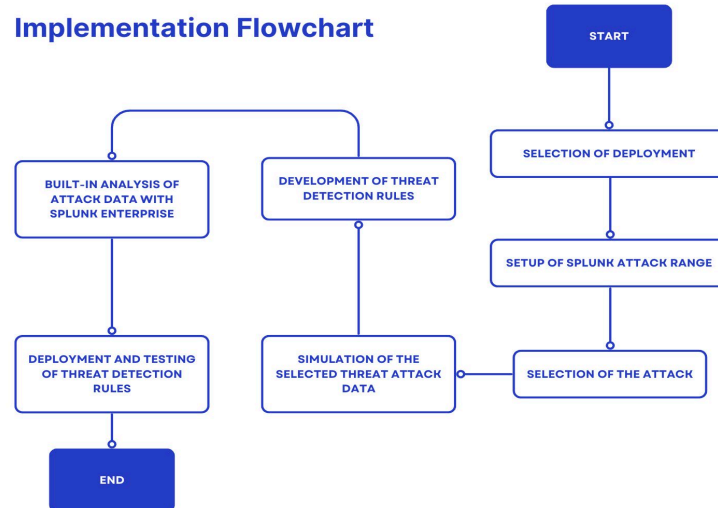
In this section, the Splunk attack range's command and its actions feature is briefed. Splunk Attack range supports various command actions which help in the control of the simulation environment. The below table provide a detail information on the command and its usage.

Command Action	Usage
python attack_range.py configure	To configure the attack simulation environment.
python attack_range.py build	To build the attack simulation environment.
python attack_range.py show	Show the details of the created simulation environment.
python attack_range.py destroy	To destroy the created simulation environment.
python attack_range.py stop	To stop the running simulation environment.
python attack_range.py resume	To start the running simulation environment.
python attack_range.py simulate	To simulate attack in the simulation environment.
python attack_range.py dump	To dump the data from the simulation environment.
python attack_range.py replay	To replay dump into the simulation environment.

7 Implementation

This section provides a comprehensive report on the implementation phase of setting up the Splunk Attack Range tool to develop optimal threat detection rule for organizations, Covering each step in detail, ensuring that security professionals can effectively configure and utilize the tool to

enhance their threat detection capabilities. Organization can leverage the full potential of Splunk Attack Range to identify and mitigate security threats, using the insights aligned with the MITRE ATT&CK framework. This approach ensures that detection rules are based on industry-standard tactics and techniques, leading to more accurate and effective threat detection.



7.1 Selection of Deployment

As Splunk attack range tool offers both local and cloud deployment options for setting up the simulation environment for threat detection rules. After careful consideration and analysis of all the deployment options, Amazon Web Services (AWS) was chosen for this research. AWS Platform provides more control over the environment and is more cost-effective and resource-efficient compared to local deployment setups with VirtualBox and Vagrant. Additionally, since many organizations already use the Amazon cloud platform, it was selected as the best suitable deployment environment option for this research.

7.2 Splunk Attack Range Environment Setup

With Amazon Web Services (AWS) chosen as the deployment platform, the setup of the Splunk Attack Range environment proceeds. An EC2 instance with the t2.micro instance type is launched in the AWS console, serving as the control panel for the entire attack simulation environment. After initializing the instance, Docker is installed. Once Docker is installed on the EC2 instance, the Splunk Attack Range Docker image is pulled from Docker Hub. The Splunk Attack Range Docker image is utilized in the research to streamline the process of installing dependencies necessary for the Splunk Attack Range script and configuration files. This approach ensures a smooth setup of the simulation environment, minimizing errors and issues.

Configuring with AWS

To set up the Splunk Attack Range simulation environment, an AWS connection is established using an Access ID and secret key. However, following best practices and recommendations, it's advisable not to use the Access ID and secret key of an AWS root user account. Instead, a new

IAM role should be created specifically for the research purposes. This approach enhances security by limiting permissions and following the principle of least privilege, ensuring that the critical credentials of the root user remain uncompromised while providing necessary access for the simulation environment setup.

The next step is to configure the attack range environment. The Splunk attack range configuration is specified in the `attack_range.yml` file. When we run `python attack_range configure`, an interactive prompt appears in the terminal, allowing us to choose the cloud provider, where AWS will be selected. We are then prompted to decide whether to use prebuilt Packer images for the simulation environment setup; in this research, we will use these prebuilt images. During the configuration, an SSH key will be created, which will be used to connect to all instances created by the attack range build automation.

Figure 1.5 – attack_range.yml configuration setup

The next phase is to build the attack simulation environment using the python `attack_range` build command. Based on the configuration specified in the `attack_range.yml` file, the servers with the specified configurations will be launched on the configured AWS platform. This automation

process, which utilizes Terraform and Ansible, takes several minutes to complete. During the build automation, a new VPC will be created, the specified servers will be set up, and elastic IPs will be created and associated with the instances. The Splunk attack range also provides a Guacamole server, which will be used to connect to the instances in the simulation environment.

```
Apply complete! Resources: 16 added, 0 changed, 0 destroyed.
2024-08-05 15:21:03,674 - INFO - attack_range - attack_range has been built using terraform successfully
2024-08-05 15:21:03,674 - INFO - attack_range - [action] > show

Status Virtual Machines

Name                Status    IP Address    Instance ID
-----
ar-win-root-68570-ar-0    running  52.4.217.125  i-0dceedf357e9b788a
ar-linux-root-68570-ar-0  running  44.215.95.32  i-01f9429f93df352e1
ar-splunk-root-68570-ar   running  52.71.170.186 i-0cfbab996db9feb69

Access Windows via:
RDP > rdp://52.4.217.125:3389
      username: Administrator
      password: LpVHvd15f0ZQ3QYKAI0

Access Linux via:
SSH > ssh -i/attack_range/root-68570.key ubuntu@44.215.95.32
      username: ubuntu
      password: LpVHvd15f0ZQ3QYKAI0

Access Guacamole via:
Web > http://52.71.170.186:8080/guacamole
      username: Admin
      password: LpVHvd15f0ZQ3QYKAI0

Access Splunk via:
Web > http://52.71.170.186:8000
SSH > ssh -i/attack_range/root-68570.key ubuntu@52.71.170.186
      username: admin
      password: LpVHvd15f0ZQ3QYKAI0
```

Figure 1.6 – Once the automation is completed, information about the created simulation environment is displayed.

7.3 Attack Simulation – OS Credential Dumping

OS Credential Dumping is a technique attackers use to steal credential data from a system, including usernames, passwords, tokens, and other credential values. Credentials can be dumped using various methods, such as keyloggers, sniffing, and tools like Mimikatz, GetPassword_x64 and Axiom that can extract sensitive credential data. Once attackers obtain these credentials, they can use them for lateral movement to carry out further attacks within a system or network. Detecting the credential dumping is crucial to maintain the security posture of the network.

The OS Credential Dumping attack falls under the credential access tactic and includes eight sub-techniques according to the MITRE ATT&CK framework. The table below provides details on the sub-techniques of the OS Credential Dumping attack.

Technique ID	Name
T1003.001	LSASS Memory
T1003.002	Security Account Manager
T1003.003	NTDS

T1003.004	LSA Secrets
T1003.005	Cached Domain Credentials
T1003.006	DCSync
T1003.007	Proc FileSystem
T1003.008	/etc/passwd and /etc/shadow

The Local Security Authority Subsystem Service (LSASS) process memory is a prime target for attackers aiming to capture sensitive credential data. Detecting and preventing LSASS memory dumps is essential, as gaining access to this data can lead to system compromise. A technique involving a quiet process exit is used to generate a memory dump of lsass.exe through Windows Error Reporting. As a result, the OS Credential Dumping – LSASS Memory attack was selected for the simulation on the Windows machine 'ar-win-root-68570-ar-0' utilizing the Atomic Red Team simulation engine.

The following Splunk Attack Range simulate command action is used to simulate the attack on the windows machine in the attack simulation environment.

`'python.py attack_range.py simulate -e ART -te T1003.001 -t ar-win-root-68570-ar-0'`

```

" + ... ($exePath = resolve-path \"$env:ProgramFiles\dotnet\shared\Microsoft.N ...",
" + CategoryInfo          : ObjectNotFound: (C:\Program File...oft.NETCore.App:String) [Resolve-Path], ItemNotFoundE ",
" + Exception             : xception",
" + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.ResolvePathCommand",
" ",
"The expression after '&' in a pipeline element produced an object that was not valid. It must result in a command ",
"name, a script block, or a CommandInfo object.",
"At line:2 char:3",
"+ & \"$exePath\" -u -f $env:Temp\dotnet-lsass.dmp (Get-Process lsass).id}",
" + ",
" + CategoryInfo          : InvalidOperation: (:String) [], RuntimeException",
" + FullyQualifiedErrorId : BadExpression",
"Exit code: 0",
"Done executing test: T1003.001-11 Dump LSASS with createdump.exe from .Net v5",
"Executing test: T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs",
"Exit code: 0",
"Done executing test: T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs",
"Executing test: T1003.001-13 Dump LSASS.exe using lolbin rdrleakdiag.exe",
"Directory: C:\Users\ADMINI-1\AppData\Local\Temp",
"Mode                LastWriteTime         Length Name",
"-----",
"d-----          7/23/2024   6:56 PM                t1003.001-13-rdrleakdiag",
"C:\Windows\System32\rdrleakdiag.exe /p 596 /o C:\Users\ADMINI-1\AppData\Local\Temp\t1003.001-13-rdrleakdiag /fullmemdump /wait 1",
"Minidump file, minidump_596.dmp can be found inside C:\Users\ADMINI-1\AppData\Local\Temp\t1003.001-13-rdrleakdiag directory.",
"Exit code: 0",
"Done executing test: T1003.001-13 Dump LSASS.exe using lolbin rdrleakdiag.exe",
"Executing test: T1003.001-14 Dump LSASS.exe Memory through Silent Process Exit",
"This version of C:\AtomicRedTeam\ExternalPayloads\nanodump.x64.exe is not compatible with the version of Windows you're running. Check your compu",
"ter's system information and then contact the software publisher.",
"Exit code: 1",
"Done executing test: T1003.001-14 Dump LSASS.exe Memory through Silent Process Exit"
]
}

TASK [atomic_red_team : Cleanup after execution] *****
changed: [100.27.123.96]

PLAY RECAP *****
100.27.123.96      : ok=8    changed=3    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
(attack-range-py3.10) root@1fbd25d2952f:/attack_range#

```

Figure 1.7 – OS Credential Dumping: LSASS Memory T1003.001 attack simulated

The Windows machine log is sent by the universal forwarder and indexed into the Splunk Enterprise server. The logs from the Windows machine are stored in the 'win' index, while the attack data logs are stored in the 'attack' index within the Splunk Enterprise server.

7.5 Attack data Built-in analysis with Splunk Enterprise

In the attack simulation environment, the Splunk Enterprise server comes with various pre-installed apps, including Splunk Security Essentials, Splunk Security Content Update, Splunk Attack Range, and Splunk Machine Learning Toolkit, among others. These applications are essential for analyzing simulated attack data effectively. Logs from the Windows machine are sent by the universal forwarder and indexed on the Splunk Enterprise server. The general logs are stored in the 'win' index, while logs related to attack data are placed in the 'attack' index.

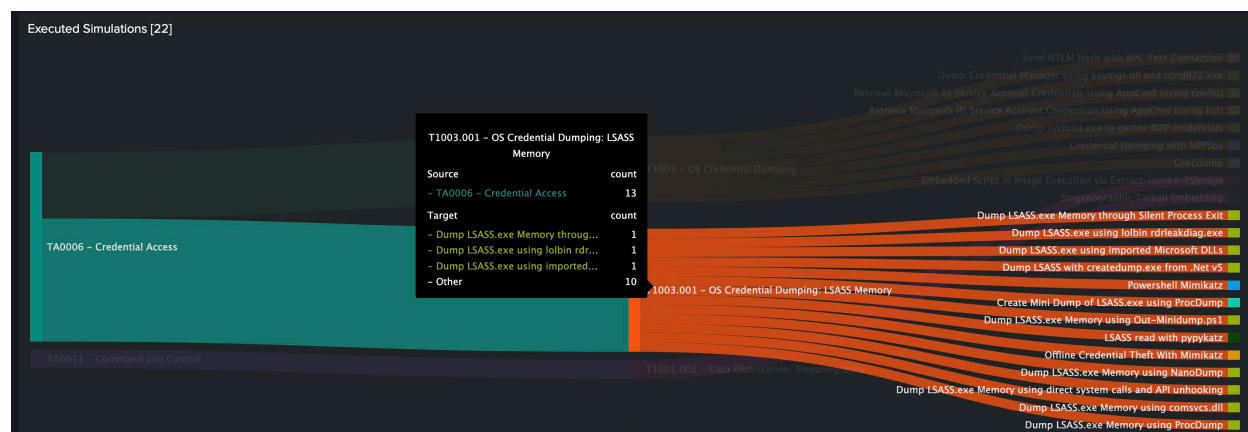


Figure 1.8 – Executed Simulation panel from attack range Splunk app

The Splunk Attack Range app features a dashboard that displays previously run tests and relevant statistics. It also provides possible analytic stories and detections that can be used to identify executed tests. This app currently supports only Atomic Red Team tests, offering specific insights for analyzing attack simulations. The Splunk Security Essentials app offers valuable insights into various types of attacks and plays a critical role in developing effective threat detection rules for an organization. It helps users understand common attack techniques and patterns, providing a comprehensive overview of potential security threats.

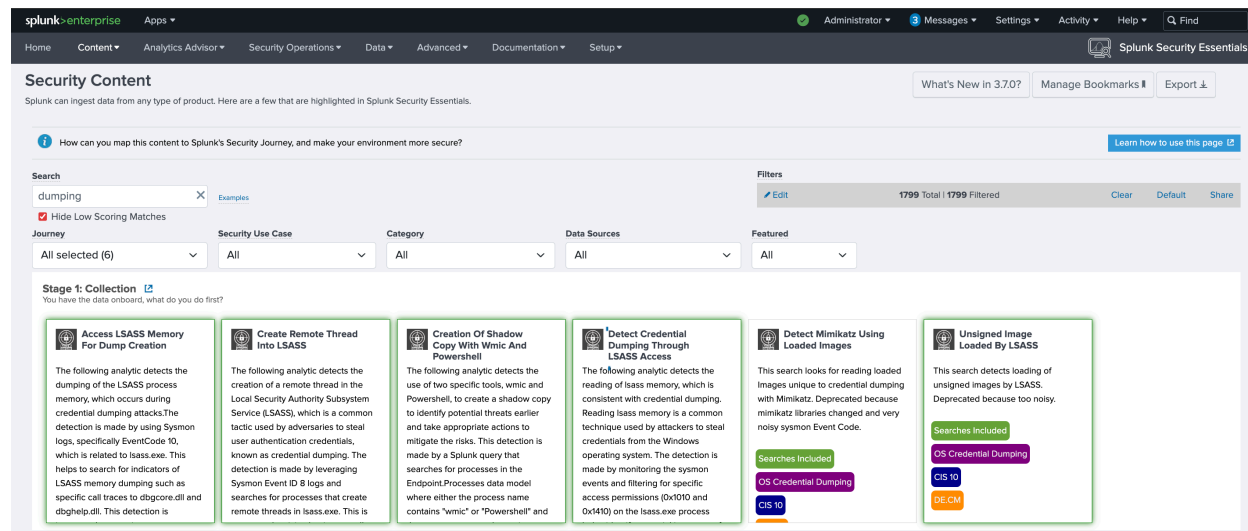
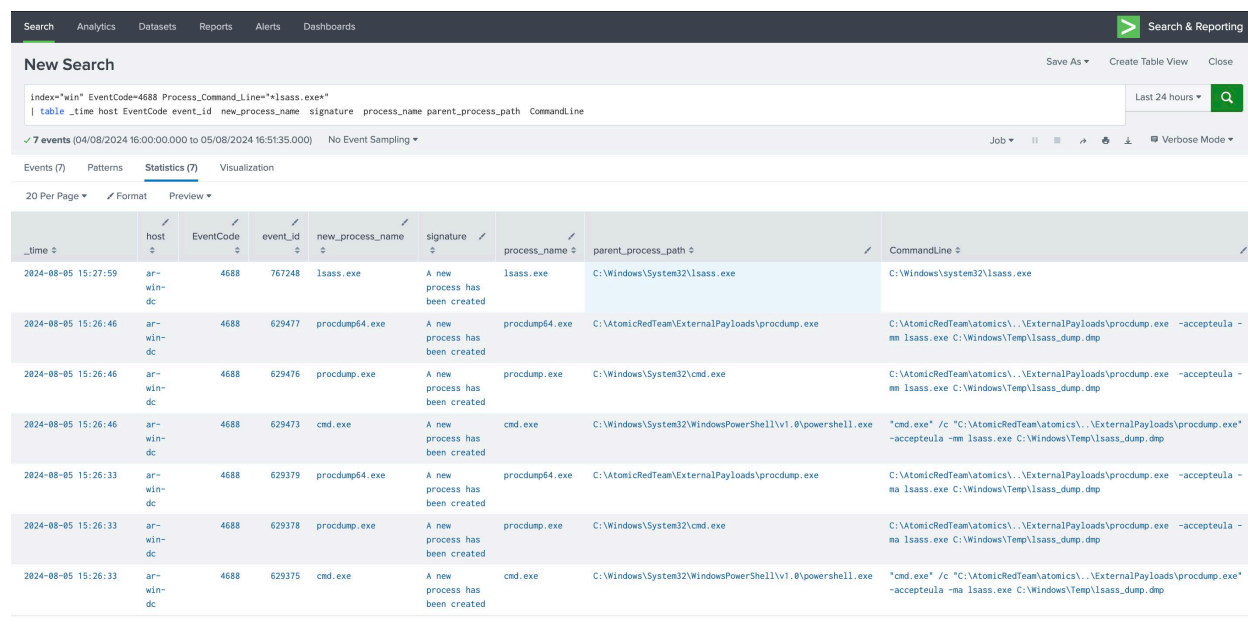


Figure 1.9 – Splunk Security Essentials App

7.6 Threat detection rule development Phase

During the development phase of the threat detection rule, Windows events are thoroughly analyzed. To identify credential dumping involving LSASS, the process associated with LSASS is matched with Windows event code '4688'. As the Windows event code correspond to various processes and activities on a Windows Machine making them valuable information for identifying potential threats within a network, creating a Splunk search query based on these event codes can create an effective threat detection rule to help prevent malicious activity on Windows machines. Therefore, the events with the windows event code '4688' and command line where lsass.exe used used to run are filtered out with an efficient Splunk search query and the following fields are tabled using the Splunk table command- `_time`, `host`, `EventCode`, `event_id`, `new_process_name`, `signature`, `process_name`, `parent_process_path` and `CommandLine`. The below is the Splunk SPL search query developed to capture the event related to the lsass credentials dumping:

```
index="win" EventCode=4688 Process_Command_Line="*lsass.exe*" | table _time host EventCode event_id new_process_name signature process_name parent_process_path CommandLine
```



The screenshot shows the Splunk Search interface. The search bar contains the query: `index="win" EventCode=4688 Process_Command_Line="*lsass.exe*" | table _time host EventCode event_id new_process_name signature process_name parent_process_path CommandLine`. The results table displays 7 events. Each row includes columns for `_time`, `host`, `EventCode`, `event_id`, `new_process_name`, `signature`, `process_name`, `parent_process_path`, and `CommandLine`.

_time	host	EventCode	event_id	new_process_name	signature	process_name	parent_process_path	CommandLine
2024-08-05 15:27:59	ar-win-dc	4688	767248	lsass.exe	A new process has been created	lsass.exe	C:\Windows\System32\lsass.exe	C:\Windows\system32\lsass.exe
2024-08-05 15:26:46	ar-win-dc	4688	629477	procdump64.exe	A new process has been created	procdump64.exe	C:\AtomicRedTeam\ExternalPayloads\procdump.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -accepteula -mm lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:46	ar-win-dc	4688	629476	procdump.exe	A new process has been created	procdump.exe	C:\Windows\System32\cmd.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -accepteula -mm lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:46	ar-win-dc	4688	629473	cmd.exe	A new process has been created	cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"cmd.exe" /c "C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe" -accepteula -mm lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:33	ar-win-dc	4688	629379	procdump64.exe	A new process has been created	procdump64.exe	C:\AtomicRedTeam\ExternalPayloads\procdump.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:33	ar-win-dc	4688	629378	procdump.exe	A new process has been created	procdump.exe	C:\Windows\System32\cmd.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:33	ar-win-dc	4688	629375	cmd.exe	A new process has been created	cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"cmd.exe" /c "C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe" -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp

Figure 1.10 – Splunk SPL query to detect minidump of Lsass Memory OS credential Dumping

The above SPL (Search Processing Language) query is straightforward yet highly effective for detecting malicious activity related to OS credential dumping from the LSASS memory on a Windows machine. Despite its simplicity, the query is designed to efficiently identify signs of unauthorized credential extraction attempts by searching through relevant logs and data. This ensures that any suspicious activity involving LSASS memory is promptly captured and addressed, enhancing the overall security monitoring of the system.

The Splunk search query has been configured and saved as an alert within Splunk Enterprise. It is scheduled to run every 15 minutes using a Cron job expression, with the search time range set to the last 15 minutes. This setup enhances the efficiency of the threat detection rule by enabling near-real-time monitoring of potential malicious activities. The alert is designed to trigger whenever the search query identifies one or more events, with a notification of high severity sent to the Splunk Enterprise server whenever the alert is triggered.

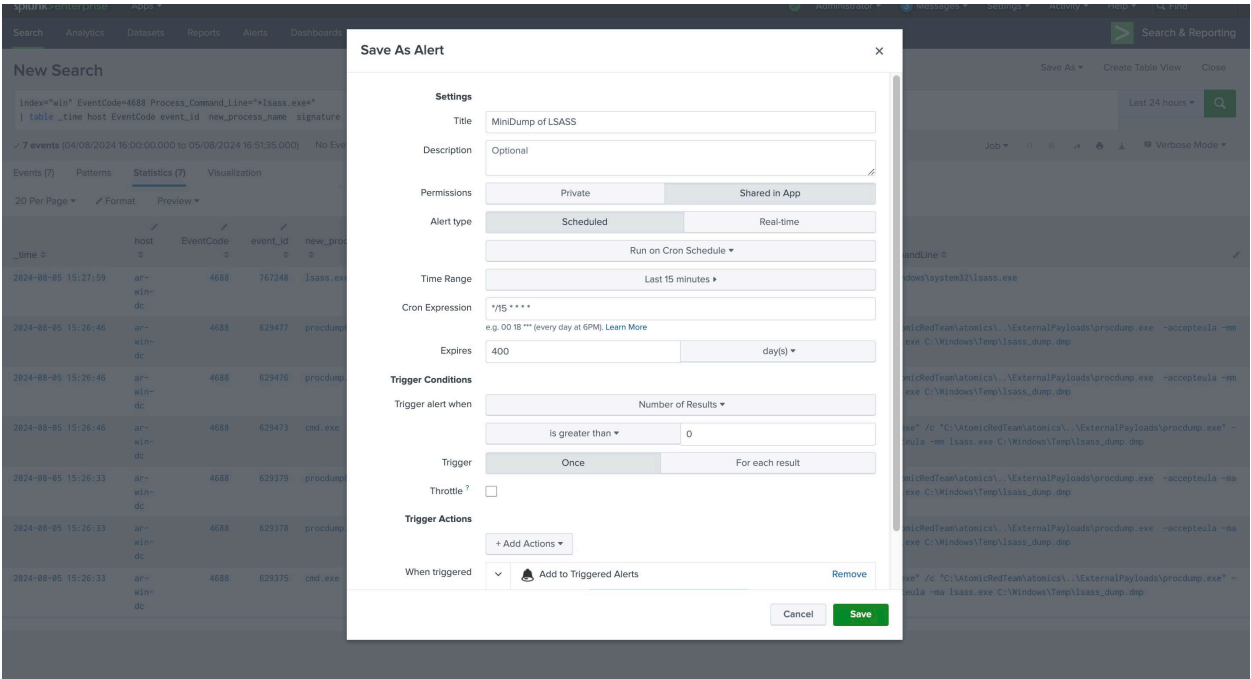


Figure 1.11 – Deployment of Minidump of LSAAS threat detection rule

8 Evaluation

This evaluation section examines how effectively the "MiniDump of LSAAS" threat detection rule operates within the deployed Splunk Enterprise server environment. To thoroughly assess the rule's performance, we simulated the attack technique T1003.001, which pertains to credential dumping, on a Windows instance. This simulation was conducted in the same controlled attack simulation environment specifically set up using Splunk's attack range automation tools. By replicating this attack technique, we aim to determine the rule's accuracy and efficiency in identifying and responding to this threat within the Splunk monitoring framework.

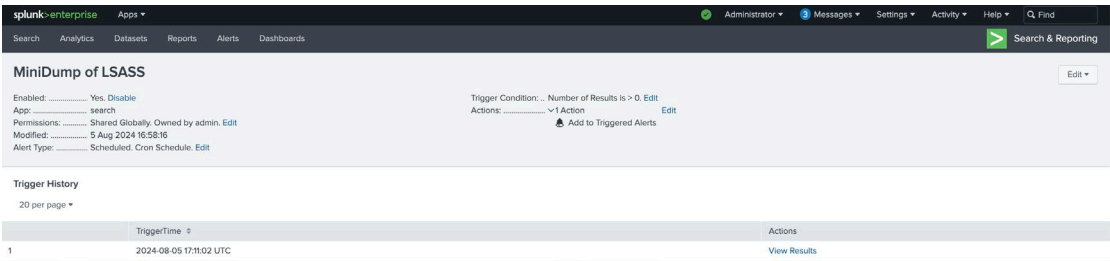


Figure 1.12 – Minidump of LSAAS: threat detection rule triggered.

After validating the effectiveness of the developed "Minidump of LSAAS" threat detection rule, the alert is ready for deployment in the organization's production environment. There are two options for transferring the detection rule from the simulation environment to production. Either the SPL (Search Processing Language) query of the developed Splunk threat detection rule can be directly copied, or the entire saved search configuration can be exported from the simulation environment and imported into the production environment. This ensures a seamless transition and integration of the threat detection capabilities into the organization's operational monitoring framework.

9 Future Work

The primary objectives of the research on the exploration of Splunk Attack Range tool features for developing threat detection have been successfully achieved. Through this research, the features of the Splunk Attack Range tool have been analysed and detailed in the research paper. This paper clearly explains the deployment options for Splunk Attack Range, the available attack simulation engines, the attack range configuration file, and how Terraform and Ansible contribute to the automated setup of the environment used to create and perform attack simulations.

The research successfully implemented the setup of the attack simulation environment using the Splunk Attack Range tool within the designated research timeframe. For the simulation, the OS credential dumping attack (T1003.001) was selected and executed using the Atomic Red Team attack simulation engine. Leveraging the Splunk Attack Range tool and the built-in analysis Splunk app, the development of the desired threat detection rule based on the simulated attack data was achieved. The research also validated the developed threat detection rule for the OS Credential Dump – LSAAS Memory attack technique by re-simulating the attack on a Windows machine, successfully verifying that the threat detection rule was triggered.

However, despite exploring the extensive features of the Splunk Attack Range tool in this research paper, only one attack technique was performed, and its corresponding threat detection rule was developed. The simulation focused exclusively on a Windows server, although the Splunk Attack Range tool also supports attack simulations on Linux instances.

Additionally, the Splunk Attack Range tool offers SOAR (Security Orchestration, Automation, and Response) implementation features within the attack simulation environment, enabling the development, testing, and optimization of Splunk SOAR playbooks. Due to prioritization based on deadlines, the implementation of Splunk SOAR was not included in the research setup, which focused solely on developing an efficient threat detection alert using the Splunk Enterprise SIEM tool.

This research paper on the exploration of Splunk Attack Range features and the development of threat detection rules will be highly beneficial for organizations aiming to fortify an efficient defense mechanism within their networks.

10 Conclusion

Establishing an efficient threat defense mechanism for an organization is an important fact to maintain its security posture. This research successfully explored the features of the Splunk Attack Range tool for developing threat detection rules. The insights gained from this research will be valuable for organizations aiming to enhance their IT security defences. By providing a comprehensive understanding of how to utilize the Splunk Attack Range tool for creating tailored threat detection rules, this research contributes to more effective and efficient protection against malicious threats. The methodologies and findings presented here can serve as a foundation for future work, including expanding simulations to other environments and incorporating automated response strategies using Splunk SOAR playbooks.

Reference

1. Korving, F., & Vaarandi, R. (2023). DACA: Automated Attack Scenarios and Dataset Generation. *Proceedings of the . . . International Conference on Information Warfare and Security*/the *Proceedings of the . . . International Conference on Information Warfare and Security*, 18(1), 550–559. <https://doi.org/10.34190/iccws.18.1.962>
2. Korving, F. (2022) DACA: Automated attack scenarios and dataset generation, Master thesis, Tallinn University of Technology, Department of Software Science.
3. Mustafa, H.M. *et al.* (2023) 'CPGrid-OT: Cyber-Power Data Generation Using Real-Time Reconfigurable Testbed for Resiliency,' *IEEE* [Preprint]. <https://doi.org/10.1109/mscpes58582.2023.10123420>.
4. Ananthapadmanabhan, A. and Achuthan, K. (2022) 'Threat Modeling and Threat Intelligence System for Cloud using Splunk,' *IEEE* [Preprint]. <https://doi.org/10.1109/isdfs55398.2022.9800787>.
5. Selvaganesh, M. *et al.* (2022) 'Efficient Brute-force handling methodology using Indexed-Cluster Architecture of Splunk,' *2022 International Conference on Electronics and Renewable Systems (ICEARS)* [Preprint]. <https://doi.org/10.1109/icears53579.2022.9752323>.
6. Su, T. *et al.* (2016) 'Attack detection of distributed denial of service based on Splunk,' *IEEE* [Preprint]. <https://doi.org/10.1109/icamse.2016.7840355>.
7. *A log aggregation design criteria for robust SIEM (Security Information and Event Management) in enhancing threat detection.* (2023, December 2). IEEE Conference Publication | IEEE Xplore. <https://ieeexplore.ieee.org/abstract/document/10468438>
8. *Attack Range AWS — Attack Range 3.0.0 documentation.* (n.d.). https://attack-range.readthedocs.io/en/latest/Attack_Range_AWS.html

9. C, B. (2023, April 18). Threat Hunting Series 1 — OS Credential Dumping - Balasubramanya C - Medium. *Medium*. <https://medium.com/@balasubramanya.c/threat-hunting-series-1-os-credential-dumping-6cc9559ecd13>
10. *Detecting Cyber Attacks through Measurements: Learnings from a Cyber Range*. (2022, September 1). IEEE Journals & Magazine | IEEE Xplore. <https://ieeexplore.ieee.org/abstract/document/9847127>
11. Kruck, G. P. (n.d.). *Combating Non-Compliance: Leveraging Breach & Attack Simulation Techniques to Continuously Validate Information Assurance Controls* - ProQuest. <https://www.proquest.com/openview/d78c3af49dbb84f51b9a635d2f529f99/1?pq-origsite=gscholar&cbl=18750&diss=y>
12. *Log Analysis for network Anomalies Detection in Splunk* - WebThesis. (n.d.). <https://webthesis.biblio.polito.it/30825/>
13. *MITRE Tactics Inference from Splunk Queries*. (2023, October 26). IEEE Conference Publication | IEEE Xplore. <https://ieeexplore.ieee.org/abstract/document/10398612>
14. Mvelazc. (n.d.). *GitHub - mvelazc0/PurpleSharp: PurpleSharp is a C# adversary simulation tool that executes adversary techniques with the purpose of generating attack telemetry in monitored Windows environments*. GitHub. <https://github.com/mvelazc0/PurpleSharp>
15. *OS credential Dumping: LSASS Memory, Sub-Technique T1003.001 - Enterprise* | MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/techniques/T1003/001/>
16. *OS Credential Dumping, Technique T1003 - Enterprise* | MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/techniques/T1003/>
17. Redcanaryco. (n.d.). *GitHub - redcanaryco/atomic-red-team: Small and highly portable detection tests based on MITRE's ATT&CK*. GitHub. <https://github.com/redcanaryco/atomic-red-team>
18. Splunk. (n.d.). *GitHub - splunk/attack_range: A tool that allows you to create vulnerable instrumented local or cloud environments to simulate attacks against and collect the data into Splunk*. GitHub. https://github.com/splunk/attack_range