

Marquette University

e-Publications@Marquette

Master's Theses (2009 -)

Dissertations, Theses, and Professional
Projects

Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab

Kunal Singh
Marquette University

Follow this and additional works at: https://epublications.marquette.edu/theses_open



Part of the [Computer Sciences Commons](#)

Recommended Citation

Singh, Kunal, "Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab" (2020). *Master's Theses (2009 -)*. 602.

https://epublications.marquette.edu/theses_open/602

APPLICATION OF
SIEM/UEBA/SOAR/SOC (Cyber SUSS)
CONCEPTS TO THE
MSCS 6560 COMPUTER LAB

by
Kunal Singh

A Thesis submitted to the Faculty of the Graduate School,
Marquette University,
in Partial Fulfillment of the Requirements for
the Degree of Master of Computing

Milwaukee, Wisconsin

August 2020

ABSTRACT

APPLICATION OF
SIEM/UEBA/SOAR/SOC (Cyber SUSS)
CONCEPTS ON
MSCS 6560 COMPUTER LAB

Kunal Singh

Marquette University, 2020

Increased Cyber-attacks on the IT infrastructure is a grave concern for organizations. Cyber defense and cyber threat remediation have become topmost priority of organizations. This thesis explains the core concepts of SIEM, UEBA, SOAR and SOC (SUSS) and explains the details of an experimental solution to which was applied MSCS 6560 lab computers for real time cyber threat detection and remediations. To test and validate SUSS concepts, these technologies were successfully applied to a small lab environment in the MSCS infrastructure for the graduate class on the Principle of Service Management and System Administration. Lab machines in this class were used by students in a progression of assignments to implement a common web service, WordPress, and other services. We hope this study would encourage use of commercial tools like Splunk on university lab computers for improving its cyber defense posture.

ACKNOWLEDGMENTS

I would like to thank my wife, my son, my manager, and my director for supporting all through my master's degree program. I would like to extend my sincere appreciation to my advisor Dr. Thomas Kaczmarek for his unwavering guidance and mentorship. I would also like to thank the Graduate School and all the Marquette University administration.

CONTENTS

ACKNOWLEDGMENTS.....	i
LIST OF FIGURES	iv
ACRONYMS AND ABBREVIATIONS	vi
PROBLEM STATEMENT	1
Background	1
Study Environment	7
BACKGROUND/PRIOR WORK.....	9
SOC (Security Operation Center)	9
SIEM (System Information and Event Management)	9
UEBA (User and Entity behavior analytics)	12
SOAR (Security Orchestration, Automated and Response)	15
HYPOTHESIS	19
Splunk Enterprise for SIEM:	19
Splunk Machine Learning for UEBA:	20
Splunk Phantom for SOAR:	20
EXPERIMENT	23
LAB Environment	23
Prior Work to Establish Splunk Enterprise Services.	25
Lab Assignments	30
Splunk Machine learning Implementation.....	38
ML model creation by SPL ML toolkit.	38
Setup Splunk Phantom App on Splunk Enterprise	44
Establish connection with Splunk Phantom server	46
Publish SPL ML model	48
Forward SPL ML events to Splunk Phantom	50
Splunk Phantom SOAR Setup	55
Splunk Phantom Install	55
Splunk SOAR playbook	56
Handling New Event via Splunk Phantom UI	59
RESULTS.....	62

CONCLUSION	67
FUTURE WORK	69
Bibliography	71

LIST OF FIGURES

FIGURE 1. NIDS/NIPS IN THE IT INFRASTRUCTURE.....	4
FIGURE 2. HIDS/HIPS IN THE IT INFRASTRUCTURE	5
FIGURE 3. SOC ARCHITECTURE.....	11
FIGURE 4. LAB ARCHITECTURE	25
FIGURE 5. AUDITD LOG STATUS	31
FIGURE 6. AUDITD LOGS SAMPLE.....	33
FIGURE 7. SPLUNK TABLE DISPLAY	34
FIGURE 8. UPDATED SPLUNK TABLE.....	36
FIGURE 9. SPL SNIPPET	38
FIGURE 10. SPLUNK ML LEARNING TOOL KIT	39
FIGURE 11. SPLUNK ML OPTIONS.....	39
FIGURE 12. CREATE A ML EXPERIMENT.....	39
FIGURE 13. CATEGORICAL PREDICTION.....	40
FIGURE 14. MACHINE LEARNING RESULTS.....	41
FIGURE 15. SPL ML SEARCH.....	41
FIGURE 16. SPL ML SEARCH FOR ANOMALIES.....	42
FIGURE 17. SPLUNK ML EXPERIMENT PAGE.....	42
FIGURE 18. MANAGING SPLUNK ML MODELS	43
FIGURE 19. SETTING A TRAINING SCHEDULE FOR THE ML MODEL.....	43
FIGURE 20. ADDING PHANTOM APPLICATION	45
FIGURE 21. SELECTING THE PHANTOM ADD-ON	45
FIGURE 22. AFTER ADDING THE APPLICATION	46
FIGURE 23. CREATING A CONNECTION TO THE PHANTOM SERVER	46
FIGURE 24. TESTING CONNECTIVITY WITH PHANTOM	48
FIGURE 25. STATUS AFTER CONFIGURATION	48

FIGURE 26. PUBLISHING THE MODEL	49
FIGURE 27. DISPLAYING MODELS	49
FIGURE 28. GRANTING READ PERMISSION	50
FIGURE 29. SAVE SEARCH AS REPORT	51
FIGURE 30. FORWARDING THE EVENT TO PHANTOM	51
FIGURE 31. NAME THE EVENT	52
FIGURE 32. COMMON EVENT FORMAT MAPPING	53
FIGURE 33. ALERT PREVIEW	54
FIGURE 34. PHANTOM DASHBOARD	56
FIGURE 35. CREATING PLAYBOOKS	56
FIGURE 36. DISPLAYING PLAYBOOKS	57
FIGURE 37. ADDING TASKS TO THE PLAYBOOK.....	57
FIGURE 38. EMAIL ALERTS.....	57
FIGURE 39. SAVING THE PLAYBOOK.....	58
FIGURE 40. PYTHON GENERATED FOR THE PLAYBOOK.....	59
FIGURE 41. ANALYST ALERT DASHBOARD.....	59
FIGURE 42. EVENT ID CHECKING	60
FIGURE 43. RUN THE PLAYBOOK	60
FIGURE 44. EMAIL ALERT.....	61
FIGURE 45. SPLUNK ENTERPRISE ALERT	63
FIGURE 46. FAILED ATTEMPTS DISPLAY	64
FIGURE 47. SPL LOGIN RESULTS	64
FIGURE 48. SPLUNK ML RESULTS	65
FIGURE 49. SPLUNK PHANTOM PLAYBOOK.....	66

ACRONYMS AND ABBREVIATIONS

SEM	Security Event Management
SIM	Security Information Management
LEM	Log Management
SIEM	Security Information and Event Management
UEBA	User and Entity Behavior Analytics
SOAR	Security Orchestration Automation and Response
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
SPL	Splunk Processing Language.
CEF	Common Event Processing
VPE	Visual Playbook Editor
ML	Machine Learning

PROBLEM STATEMENT

Background

Cybersecurity breaches have caused serious consequences to organizations, such as revenue loss, damage to reputation, and theft of proprietary data and customer information. Defending and monitoring enterprise IT infrastructure from cyber threats has become a priority for every organization today. Companies continue to invest billions of dollars in setting up security tools to improve their cyber defense posture, but nothing seems to be working against the growing cyber security threats [1]. To better understand current cyber security challenges, we need to understand the historical cyber paradigm and solutions built around it.

Historically, cyber-attacks began with malicious software such as worms, trojans, and viruses. These types of attacks were detected and neutralized using Antivirus Software (McAfee, Symantec, TrendMicro etc.) [2].

While Antivirus software was protecting host machines, the network connecting those hosts was protected by “Firewalls”. A ‘Firewall’ monitors the incoming and outgoing traffic from a host to allow traffic to trusted networks and deny traffic to untrusted external networks [3].

Antivirus software and firewalls were only effective on detecting external attacks because of their allow/deny network traffic rules and malicious software

signature-based detection. Signature based intrusion detection could only detect known patterns of threat and it was not effective in detecting unknown threat patterns [2].

To cope up with the increasing number of threats, administrators for conventional security tools had to keep updating their network rules and signature databases with the latest threat intelligence. The increasing size of the signature database created two problems:

1. Growing size of the signature databases degraded the performance of the signature-based threat engine [2]. The performance of the anti-virus software is roughly linear with respect to the number of signatures being investigated ($O(N)$).
2. Attackers made their code more sophisticated to hide malicious code within, this led to dramatic increase in the numbers of false alerts [4].

Based on an understanding that if an attack were intended to exfiltrate data, network monitoring could be the focus for defensive actions, organizations increased their reliance on firewalls and the development of network intrusion detection and prevention. This gave birth to SIM and SEM tools. SEM (Security Event Management) tools were designed to provide real time threat monitoring, correlation of security events, to generate alerts in case of threat events, and to provide a complete security posture via a security-console view [5]. SIM (Security Information management) tools collected and stored log data for forensic analysis after a security breach [6]. Later, these two types of systems were merged, and Security Information and Event Management (SIEM) solutions were created. SIEM solutions were designed to reduce false positives while detecting potential threats, their rule-based co-relation engines were able to focus on IDS

(Intrusion detection system) and IPS (Intrusion prevention system) events which were in violation of an organization's policy [4].

Vendors created security tools such as NIDS, NIPS, HIDS, and HIPS that focused on either the host or the network in the infrastructure. NIDS and HIDS are two types of Intrusion Detection Systems (IDSs) and NIPS and HIPS are two types of Intrusion Prevention Systems (IPSs).

- **Network Intrusion Detection Systems (NIDS):** NIDS works as a gate keeper; it searches the inbound traffic for any potential threat and issues potential threat alerts to administrators who are expected to respond. An IDS compares the inbound traffic against a database of known attack signatures; when a known event is detected an alert is generated detailing the incident [5]. IDSs evaluate the traffic but can't stop the traffic from entering the network.
- **Network Intrusion Prevention Systems (NIPS):** NIPS works as a security guard. It scans the inbound traffic and stops the suspected malicious traffic from getting into the network. The IPS compares the inbound traffic against database of known attack signatures; when a known event is detected then the IPS rejects that traffic [5]. IPS evaluates traffic at a deeper level than most firewalls before it allows the traffic through a port.

As shown in figure 1, NIDS/NIPS are installed at the network layer for packet inspection for cyber threat detection or prevention.

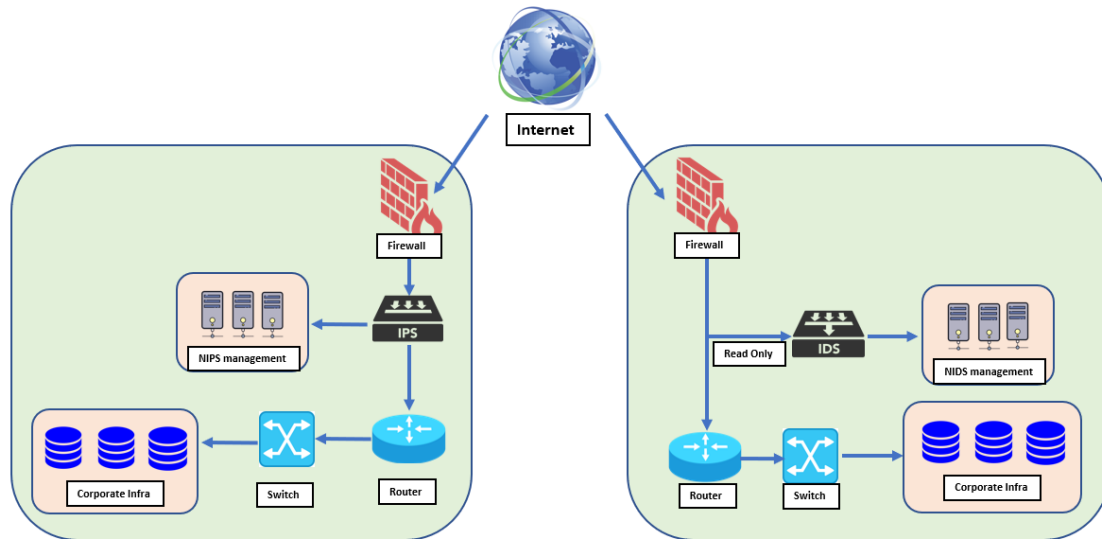


Figure 1. NIDS/NIPS in the IT Infrastructure

- **Host Intrusion Detection Systems (HIDS):** HIDS are applications such as firewalls, antivirus software and spyware-detection programs that are installed on individual systems [7]. Typically, HIDS monitors activities on the client computer and in some cases will monitor incoming network traffic. Similar to NIDS, HIDS also generates alerts but do not deploy preventive actions.
- **Host Intrusion Protection Systems (HIPS):** Like HIDS, HIPS is also installed on individual systems. Apart from identifying cyber threats, it also deploys measure to remediate the threat. Like, if a program oversteps its permissions, is blocked from carrying out unapproved actions [8].

As shown in figure 2, HIDS/HIPS are installed on the end point machine for Cyber threat detection and prevention.

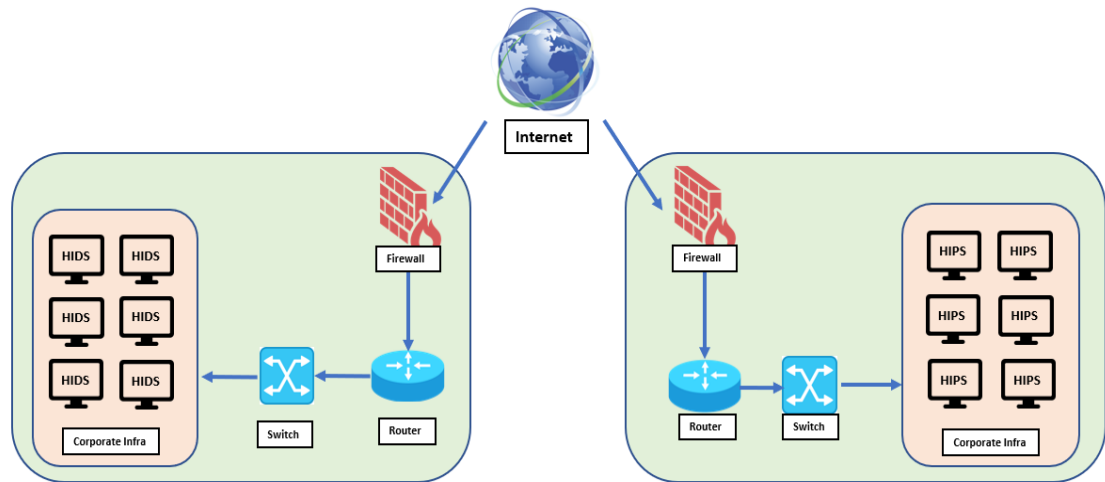


Figure 2. HIDS/HIPS in the IT Infrastructure

Apart from security threats of exfiltration, organizations must also stay compliant with regulatory requirements, which directed organizations to collect, analyze, report and archive logs that monitor access to protected data in the IT infrastructure [4]. To stay complaint organizations invested in log management (LEM) products which had capabilities to handle large volume of data and the ability to scale up with the organization's growth. Organizations that were already spending millions of dollars on SIEM tools, IDS (Intrusion detection systems), IPS (Intrusion prevention systems) and LEM tools added additional expense to keep them compliant with regulatory requirements.

Over time, organizations realized that Security Event Management (SEM) tools and Log Event Management tools (LEM) could work hand in hand to provide better threat intelligence and can be more cost effective. This led to the rise of the SIEM based solution [4]. SIEM systems performed correlation analysis on logs and issued real-time alerts for suspicious activities. Improved rule-based co-relation engines helped cut down

the false positives and focused only on a subset of more sophisticated events to identify critical threats [4]. A good co-relation-based solution was able to provide better threat intelligence, but constant updates to correlation engines was challenging; This required manual intervention to deal with the growth and upgrades of organization's IT infrastructure [4].

Many organizations created a process to deal with the volumes of data and alerts coming from SIEM tools. A SOC (Security Operation Center) team of security analysts was created to monitor and respond to cyber threats based on the alerts issued by SIEM systems. SOC teams in many organizations have security analyst working 24/7 monitoring and responding to cyber threats/attacks [9]. SOC teams are responsible for constantly updating the correlation engine to account for their experiences [9]. Overtime, following the lead of Homeland Security, organizations combined the SOC team and SOC process with other forms of business and cybersecurity knowledge in fusion centers [10].

While organizations were constantly adjusting their SIEM correlation engine to the changing IT infrastructure and new cyber threats, they faced with two other grave challenges.

1. The increased sophistication & frequency of cyber-attacks.
2. Need for a prompt response to an active cyber-attack or a breach.

Modern cyber threats/attacks are much more sophisticated and more frequent; too sophisticated and frequent for a human being to keep up with. Today, organizations are working on convergence of different cybersecurity tool stacks that

include concepts from SEM, LEM, SIEM, UBEA and SOAR solutions to proactively predict a cyber-attack/threat and deploy preventive measures to protect organization assets. We have investigated and pursued application of UBEA and SOAR. This thesis document is the study of SUSS which combines the use of SIEM, UEBA, and SOAR in a SOC.

Study Environment

The lab for the class on The Principles of Service Management and System Administration contains virtual servers that are assigned to students. Like all servers they are targets and they are vulnerable to external and internal cyber threats. While these servers should not host any sensitive data, an attacker seizing control can leverage the infrastructure to attack other internal/external network infrastructure. Since these servers are used by students to learn, among other things, elements of cyber defense, security is initially relaxed and then increased over the course of the semester through instruction and exercises. As a result, they are more susceptible to cyber-attacks than production servers.

The lab infrastructure for the class does not support university research; the use of the infrastructure is based on a set of assigned exercises which are performed by students over the semester. Thus, these servers have a time-dependent and varying usage pattern driven by coursework resulting in an expected pattern of usage and user behavior over the course of the semester. Based on this information, the experiments reported here utilize Machine learning capabilities to learn user behavior and system usage by monitoring

server logs (UEBA). In this context an alert is issued when an anomaly in usage behavior is detected. This alert would then be sent to a system for automated response (SOAR).

In this thesis, we investigate and experiment how organizations are able to solve the challenges of this lab environment using a current set of commercially available tools. We will be leveraging our department lab infrastructure for this investigation and experiment. Our proposed solution suggests applying Cyber-SUSS (a combination of a SOC, UEBA, SIEM and SOAR) concepts to the lab infrastructure to have the ability to automatically detect and respond to cyber threats.

Applying Cyber-SUSS concepts on lab infrastructure would be more challenging than applying the same on any organization's infrastructure because unlike organization's infrastructure, lab infrastructure does not have the same degree of variations in activity patterns. While assignments guide the use of the infrastructure more variation is expected as students learn to solve lab assignments. This means that machine learning algorithms had to be adaptive to compensate for the abnormal behavior on the lab computers that occurs while students are learning. We have chosen and utilize common enterprise tools (available from Splunk) to build a solution by applying Cyber-SUSS concepts.

BACKGROUND/PRIOR WORK

Organizations are investing in solutions which can provide automated threat intelligence and threat response to the evolving cyber threat landscape [1]. The increased number of automated and sophisticated cyber-attacks has led to centralized and optimized Security Operation Centers. Typically, an organization would deploy a bunch of security tools to monitor and alert on different functions of the business. In larger and more mature organizations, the business infrastructures is typically supported by a centralized IT infrastructure operations team; in this context the SOC (Security Operation Center) is responsible for the cybersecurity of the infrastructure [11].

SOC (Security Operation Center)

A SOC team is an organization responsible for responding to an imminent cyber threat. Typically, a SOC team works 24/7/365, monitoring the organizations infrastructure through the examination of machine logs [12]. These logs are captured from various security devices, services and sensors, including perimeter defense systems (network firewalls and intrusion prevention systems), host sensors (Intrusion detection systems and Antivirus systems), applications (Web application firewalls and authentication systems), and network sensors by a SIEM system [13].

SIEM (System Information and Event Management)

The latest SIEM systems have the capabilities to parse, normalize and integrate logs from multiple sources/endpoints. These systems can ingest logs from different

vendor's devices in the organization and normalize them into a common format. The normalized logs data is typically stored for historical and forensic analysis purpose for up to three to six months [13].

This normalized data is then used to derive rules for a rule-based engine using correlation analysis, behavioral analytics, anomaly analytics and external threat intelligence linking techniques.

Every rule used in the rule-based engine is designed to detect and alert any malicious behavior in the environment. Recently in UEBA systems, rules can be created by Artificial intelligence (AI) to augment rules created by Human intelligence (HI). AI (Artificial intelligence) creates rules by applying machine learning algorithms to the normalized log data to determine possible cyber threats. To complement the AI, a SOC analyst (Human intelligence) develops various use-cases based on their experience and knowledge of the services and business use of the infrastructure. These use-cases are built by correlation of indicators from different log datasets. Any predefined (Human Intelligence) or AI (Artificial intelligence) defined rules will generate a threat alert in the SIEM system. In many organizations a SOC Tier-1 analyst will then review these alerts and determine if an alert is substantive (a true positive) or not (a false positive) [14]. If the alert seems to be suspicious then it gets escalated to SOC Tier-2 analyst for further analysis [14]. The tier-2 analyst then determines the cause of the issue and if a successful attack is identified then the analyst creates a case for the Tier-3 engineer to perform forensics on the incident to determine the impact of the attack and take remediation

action. If an alert is a false positive, then it gets assigned to a security engineering team to refine rules [14].

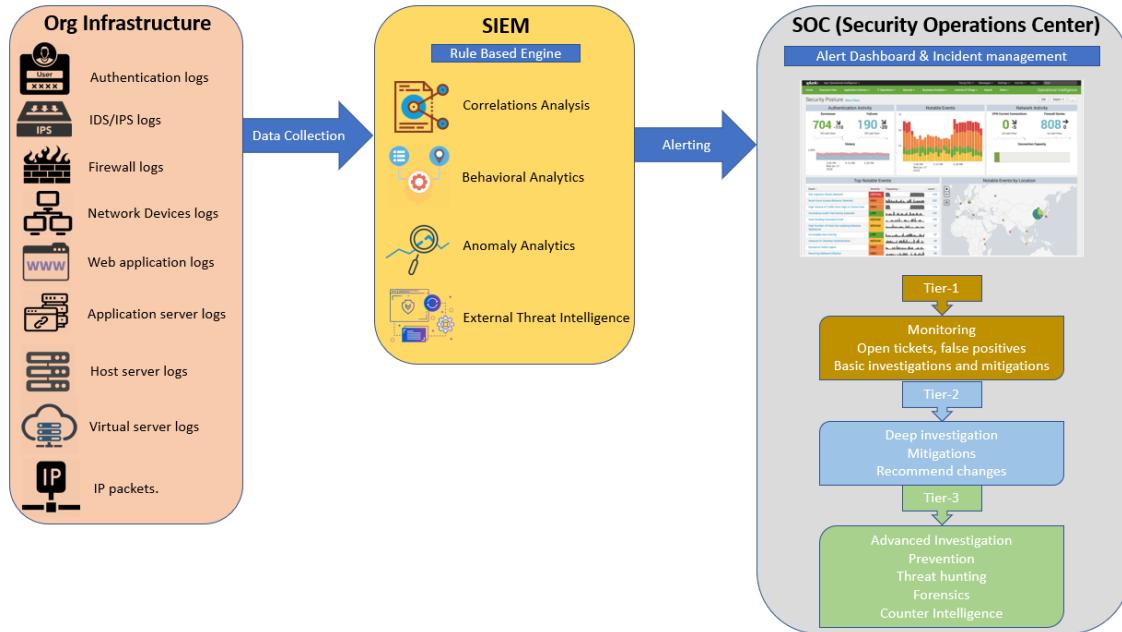


Figure 3. SOC Architecture

A SIEM system usually creates many alerts and SOC analysts can only focus on the high priority alerts due to the sheer high volume of alerts. This may cause the analyst to miss high potential threats as they were tagged as medium/low priority by the rule-based correlation engine. Organizations have solved this problem by assigning a threat score to each of the alerts based on historical event information. A machine learning algorithm can perform statistical analysis on similar kinds of historical data and provides a score to the alert. So, instead of reviewing only high alerts, SOC analyst were able to review the alerts based on risk scores generated by machine learning algorithms. This greatly improved the efficiency of SOC team members [9]. Though, machine learning algorithms eased the burden on SOC team member, it did not eliminate the need for real

time corrective actions in cases of a breach. Because of the delays in the processing, the time to identify a breach and to deploy corrective action may take months.

Organizations are looking to build the next-generation SOC's on a single suite of technology which should be able to integrate with all other vendor products [13]. The security suite should have strong analytics capabilities that can give meaningful insight on a potential cyber threat. The suite of tools should be able to utilize advanced machine learning techniques and provide automation and orchestration technology [13]. The next-generation SOC's should leverage SIEM, UBEA and SOAR concepts for monitoring, detecting and proactively deploying preventive measures in case of an imminent cyber-attack. There are vendors (for example, AT&T and Splunk) in the market who are offering a unified solution in a single security suite, but each solution will have its pros and cons.

UEBA (User and Entity behavior analytics)

Gone are the days when organizations were only worried about spam emails, trojan viruses or phishing attacks from external actors. Organizations now must deal with existing and new sophisticated cyber-threats like ransomware attacks and Advanced Persistent Threats (APT). These security threats do not always come from outside the organization; there have been threats from internal actors which cause huge financial and reputation losses to an organization. Internal threat can be malicious or accidental. To complicate the situation even more, what appears as an internal threat may be the result of account takeover.

Traditionally deployed security investigation and event management (SIEM) based solutions are no longer effective in combating emerging threats. Due to increase in the complexity and frequency of sophisticated cyber-attacks, there was a need for a machine learning based solution that can detect unknown threats and suspicious behavior across users, endpoint devices and applications. This dire need for intelligent cyber defense solutions gave birth to User and Entity behavior analytics (UEBA) solutions, which complemented current SIEM solutions.

User and Entity Behavior Analytics (UEBA) is an enhancement to current security solutions that uses innovative data analytics technology, such as machine learning and deep learning, to discover abnormal and unusual behavior by users, machines and other entities in the organization's network [15]. UEBA is known by other names, like User Behavior Analytics (UBA) and Security User Behavior Analytics (SUBA) but all of them seem to serve the same purpose of analyzing user behavior via user behavior analytics.

While the SIEM enables organizations to effectively handle some security events, a UEBA solution helped dig deeper by augmenting SOC team capabilities and making the team more efficient. UEBA can detect cyber security threats that traditional SIEM tools might not be able to see, because they do not match with the predefined correlation rules or attack patterns. It can create baselines of activities across users, endpoint devices and applications and then generate risk scores based on threat events, user and entity context, and user analytics to alert security analysts of unusual activity. UBA is neither an

alternate to SIEM, nor it is a substitute; it is applied on top of the SIEM solutions to enhance capabilities of cyber threat detection using user behavior analytics [16].

UEBA Solution has three main components called the 3 pillars of UEBA [15].

Data Source: UEBA intelligence is heavily dependent on the organizational log data which gets fed into it. It is very important that UEBA has access to all the logs from users, endpoint devices and applications across organizations. Either UEBA can be implemented on existing SIEM application which collects all the logs data across organization's assets or UEBA can be fetch the data from a Log Management tool for its user behavior analytics [15].

Use cases: UEBA solutions provide information on the behavior of users, machines and applications and other entities within the organization through independent use cases. UBEA performs monitoring, detection and alerting of anomalies for multiple use cases like employee monitoring, trusted hosts monitoring, fraud, etc. Examples of use cases are: Malicious Insider, Compromised User, known threats, and IOT device behavior [15].

Analytics: UBEA has advanced analytics abilities that employs several modern technologies that can help identify abnormal behavior by capturing patterns of normal.

- **Supervised machine learning** – In Supervised learning the UEBA system analyzes the log data and understands known expected behavior and known unexpected behavior. It continues to learn and analyze new behavior patterns and determine if they conform to the expected behavior set.

- **Unsupervised learning** – In Unsupervised learning, the UEBA system learns expected behavior and it will be able to detect and alert unexpected behavior, but it will not be able to determine if the unexpected behavior is acceptable or not. A SOC analyst must perform analysis on the alert and determine if it is acceptable or not.
- **Deep learning** – In Deep learning, the UEBA system is trained on security alerts data sets and their triage result; this enables UEBA system to performs self-identification of features and it can predict/triage results for the new set of security alerts.

SOAR (Security Orchestration, Automated and Response)

Security Orchestration, Automated and Response (SOAR) is a process of automatically detecting, preventing, and recovering from cyber-attacks without human interference using information technology, automation algorithms, and artificial intelligence [17]. A security orchestration process enables people, practices, and technologies to work together to improve an organization's security posture. Security orchestration and automation response is intended to build a technical and socio-technical solution which can integrate various vendor's security tools in a unified system to support security staff in building a next generation SOC.

An organization's cybersecurity solutions would create thousands of alerts and these alerts are monitored and actioned by SOC analysts. Typically, SOC analysts follow a manual or semi-automated processes and practices for actioning alerts. For example, after getting an alert from Intrusion detection system (IDS) for suspicious behavior, a

security analyst would login to endpoint defense system to collect more information [17]. Security analyst traverses through network logs and validates whether the potential threat is real or not. Once the threat is confirmed, a level-2 security analyst would log an incident and isolate or block the incoming/outgoing traffic from the affected network and update the existing rule-based threat intelligence engine with the latest threat information. This manual and semi-automated process is time consuming and by the time remediation action is taken by the security analyst the damage may already be done.

A security orchestration solution can address these concerns of manual threat analysis and delays in responses to security incidents. Security orchestration solutions can automatically identify suspicious behavior in an environment and proactively deploy preventive measure in case of a cyber-attack. A Gartner's report predicts that by 2019 30% of the big, medium and small organizations will deploy security automation and orchestration solutions that can bundle different security solutions and human intelligence together for the automation of security services within an organization [17]. Security orchestration platforms integrate security tools to accelerate security incident response by automating the manual activities. Orchestrating and automating the activities of multivendor security solutions is a challenging task and requires comprehensive view of the orchestration platform. Current SOAR solutions have proprietary ways of generating different formats of alerts; they do not have capabilities that support different quality attributes such as flexibility, interoperability, scalability, modifiability, accuracy, and extensibility [17]. Given the increasing demand for security orchestration, a significant amount of research is needed to help understand the challenges in security orchestration, existing solutions, and practices to address the challenges.

Organizations are increasingly adopting security orchestration and automation response platforms that are proactive, autonomous, and collaborative solutions to enable security staff to perform their responsibilities effectively and efficiently .

MITRE ATT&CK

MITRE ATT&CK is a framework developed by the non-profit organization, Mitre. It was developed to organize and classify cyber threats and their adversarial behaviors. ATT&CK stands for “Adversarial Tactics, Techniques, and Common Knowledge”. Basically, ATT&CK collects and organizes the various tactics, techniques, and procedure (TTPs) used by the cyber criminals [18].

ATT&CK aims to break down and classify historical attacks in a consistent and structured manner, the framework documents the actions taken by cyber criminals during the cyber-attack; it contains elements like, a characterization of how did cyber criminals got in, how did the attacker move inside the network, how did the attacker access sensitive data, and how did attacker exfiltrate the data out of enterprise network [19].

By bringing all the historical attacks (TTPs) under a single platform, ATT&CK has created a cybersecurity knowledgebase which enables cybersecurity teams to better classify attacks and assess an organization's risk. Organizations can perform compare with specific TTP adversaries to gauge their cyber defense posture.

There are several ways an organization can use MITRE ATT&CK. The primary use cases are as follows.

- Adversary Emulation – ATT&CK can be used to create adversary emulation scenarios to test and verify defenses against common adversary techniques.
- Red Teaming – ATT&CK can be used to create red team plans and organize operations to avoid certain defensive measures that may be in place within a network.
- Behavioral Analytics Development – ATT&CK can be used to construct and test behavioral analytics to detect adversarial behavior within an environment.
- Defensive Gap Assessment – ATT&CK can be used as a common behavior-focused adversary model to assess tools, monitoring, and mitigations of existing defenses within an organization's enterprise.
- SOC Maturity Assessment – ATT&CK can be used as one measurement to determine how effective a SOC is at detecting, analyzing, and responding to intrusions.
- Cyber Threat Intelligence Enrichment – ATT&CK is useful for understanding and documenting adversary group profiles from a behavioral perspective that is agnostic of the tools the group may use [20].

In future work, we are looking to expand our work to perform Adversary Emulation and Behavioral Analytics Development for our computer lab environment.

HYPOTHESIS

Cyber SUSS consists of 3 technologies (SIEM, SOAR, and UEBA) used in a security operations environment (SOC). The hypothesis we are testing is whether we can use a collection of functionalities found in Splunk products to implement a Cyber SUSS to monitor and protect a laboratory used in a class to teach the Principles of Service Management and System Administration. We base the work on an existing lab environment with SIEM tools and extend it to include UEBA and SOAR capabilities.

The computer lab designed for the Principles of Service Management and System Administration has proven to be vulnerable to frequent cyber-attacks. To implement Cyber SUSS for this environment SIEM, UBEA and SOAR concepts are applied the environment and tested using one of the MITRE ATT&CK advisory use cases.

We chose to use Splunk for SIEM, UBEA and SOAR implementation in our lab of virtual machines. Splunk can ingest data from diverse sources. Also, Splunk has capabilities such as Splunk Enterprise Security and a UEBA add-in for User Behavior analytics. Splunk's machine learning toolkit provides flexibility to build custom machine learning models on the data. Finally, Splunk Phantom provides the platform to setup SOAR capabilities.

Splunk Enterprise for SIEM:

A Splunk enterprise server is setup to receive logs from computer lab infrastructure such as virtual servers, various security devices and sensors, including perimeter defense systems (network firewalls and intrusion prevention systems), host

sensors (IDSs and AVSs), applications (Web application firewalls and authentication systems), and network sensors. This data can be normalized and parsed by Splunk. Once the data is available in Splunk, we can use SPL (the Splunk Processing language) to pre-process our data for data Machine Learning implementation.

Splunk Machine Learning for UEBA:

We can leverage Splunk's machine learning toolkit to implement machine learnings algorithms for each of our use case scenarios. We can also use Splunk's UBEA for User behavior analytics. Alternatively, a set of co-relation rules can be built based on human expertise and intelligence. These correlation rules can generate alerts similar to those of machine learning algorithm alerts. Once the analytics starts generating alerts on suspicious behavior, we can match them with the manual correlation rules to confirm that machine learning algorithms are working as expected.

Splunk Phantom for SOAR:

We can leverage Splunk Phantom to implement SOAR capabilities. Splunk Phantom can be leveraged to create playbooks, collaborate, response and manage security threats across IT infrastructure.

VPE – Visual Playbook Editor: Splunk Phantom playbooks can reduce the workload on Security team by automating the manual tasks via defined playbooks. Analysts and studies can easily create Splunk Phantom playbooks in VPE with drag-and-drop ease. VPE generates supporting Python code to define the analysis and response. Users can easily get started with playbooks creation with VPE and later switch to a

Python playbook editor for debugging and fine tuning. The VPE allows users to create playbooks using function blocks and connectors; these blocks and connectors describe the order of operations that are to be taken in response to a threat. While creating a playbook function block, VPE presents all possible function block types to define a security action to execute, filter data, make a decision using encoded logic, prompt a user for input or confirmation, or call another playbook [21].

Phantom Investigations: Security Analyst can collaborate and review the action taken on the threat events. Phantom investigation screen acts as hub for security analyst for collaboration, case review, event review and real-time decision on the ingested data analytics [21].

Splunk Phantom Mission Guidance: Phantom mission guidance is an intelligent guidance assistance. It uses a form of Artificial intelligence, known as reinforcement learning. It provides real time suggestion/guidance steps to investigate, contain, eradicate and recover from security incidents. This is very useful for the new security analyst. They can validate the steps taken and compare them with the steps taken by an experienced security analyst. Mission Guidance guides human analyst through the actions and playbooks needed to effectively handle an event [22].

Activity Feed: The Activity Feed in Splunk Phantom is similar to activity streams on social media. Activity Feed displays all current and historical actions performed by Security Analysts including the playbook activities. The activity feed also provides team collaboration capabilities that are integrated in line with automation details and other data, forming a record of all relevant event information. This allows security teams to

quickly see the success, ongoing execution, and results of all automation operations for the historical and ongoing security events [23].

Case Management: Case management is very important tools for SOC's. This is how a security event is logged and tracked through phases of the security remediation cycle. Splunk Phantom has an integrated case management system. This allows security team to easily create a case from a confirmed threat event. A SOC team's Standard Operating Procedures (SOPs) can easily be mapped to case management tasks. Splunk Phantom integrated case management has complete access to the Phantom automation Engine. This allow security teams to launch actions and playbooks as part of case tasks [21].

Workbook: Splunk Phantom workbooks enables security teams to codify the SOPs into reusable templates. Phantom workbooks support custom and industry standard workbooks, such as the NIST-800-61 template for incident response. With Phantom workbook a security team can divide tasks into phases (e.g. detection, analysis, containment, eradication, and recovery) and assign tasks to security analysts. Security analyst can also embed the automation actions and playbooks directly into the workbook templates [21].

MITRE ATT&CK – Use Cases

We can model our use cases on the TTPs listed under ATT&CK framework and test adversary emulation.

EXPERIMENT

To confirm the hypothesis, an experiment was conducted. The experiment was conducted in a lab environment that extends the environment previously used for the class, Principles of Service Management and System Administration. Successful demonstration of the full set of Cyber SUSS capabilities in that environment are judged as successful execution of the experiment and validation of our hypothesis.

LAB Environment

Marquette University has many computing labs. The environment of each lab has similar base software and operating system configurations, but often unique softwares are installed in support of research or student learning. Lab builds to support undergraduate courses have a consistent environment; many workstations have a locked-down common build. The software lab environment for our experiment with the Principles of Service Management and System Administration consists of the following:

- VMWare on a shared server,
- Two servers supporting Splunk.
 - One of these is shared and supports Splunk Enterprise and
 - The other is dedicated to Splunk Phantom.

As we are going to perform this experiment on MSCS 6560 (Principle of Service Management and System Administration) class lab, the high-level architecture of the MSCS 6560 lab is explained in conjunction with Splunk Enterprise and Splunk Phantom.

VMWare

Our VMWare lab environment consists of a collection of Linux (UBUNTU) VMs which are assigned to students who are responsible for the UBUNTU build and all other software installation. These virtual servers are used by students for their assignments and projects. Students are tasked with multiple assignments that are described below. The allocation of the virtual machines is administrated and managed by the instructor for the class.

Virtual Machines

Through the course of a school term, students are instructed to collect and forward system logs to Splunk Enterprise using Splunk's Universal Forwarder as they perform each assignment on the lab servers.

Splunk Enterprise Server

The lab has a Splunk Enterprise Server which collects the logs coming from the Splunk Universal Forwarder that is installed on the virtual machines. Splunk admin access is granted to the instructor and to students acting as security analysts.

Splunk Phantom Server

The final major element of the environment is the dedicated server hosting Splunk Phantom. This element is an addition to the environment that is a major focus of the current work reported in this Thesis. Splunk Phantom server will receive potential cyber

attached alerts from Splunk Enterprise server and deploy preventive measure as defined in the playbooks.

The lab architecture is depicted in Figure 4.

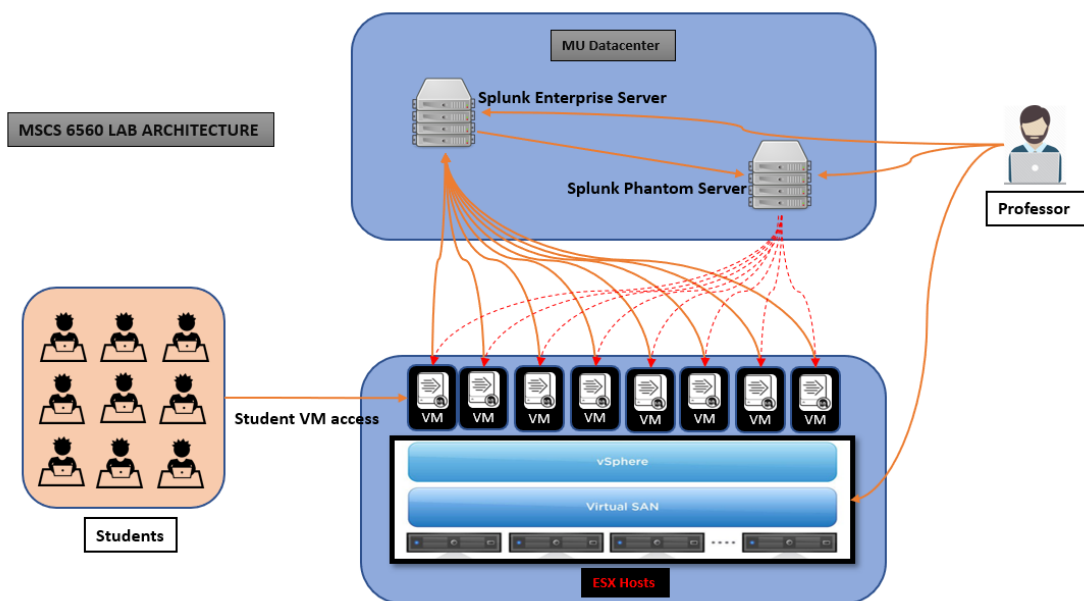


Figure 4. Lab Architecture

Prior Work to Establish Splunk Enterprise Services.

For purposes of being able to replicate this experiment and support the operation of the Cyber-SUSS, we document the detailed installation instructions below:

Splunk Enterprise install via TAR file on UBUNTU

1. Verify system requirements
2. Download the tar file from Splunk website

https://www.splunk.com/en_us/download/splunk-enterprise.html (or use CLI

downloadable WGET)[26]. You would have to create an account with Splunk in order to download the tar file.

3. Copy on tar file to target server.

4. Expand the tar file into an appropriate directory using the tar command:

```
tar -xvzf splunk_package_name.tgz
```

5. The default installation directory is splunk in the current working directory. To install into /opt/splunk, use the following command:

```
tar -xvzf splunk_package_name.tgz -C /opt
```

Splunk Enterprise install via DEB package on Ubuntu

1. Verify system requirements

You can install the Splunk Enterprise Debian package only into the default location, /opt/splunk.

This location must be a regular directory and cannot be a symbolic link.

You must have access to the root user or have sudo permissions to install the package.

The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for /opt/splunk, then use a tar file to install the software.

2. Download the DEB file via CLI downloadable WGET [26]. You would have to create an account with Splunk in order to download the deb file.

```
wget -O splunk_package_name.deb
```

3.Installation procedure

Run the dpkg installer with the Splunk Enterprise Debian package name as an argument.

```
dpkg -i splunk_package_name.deb
```

4. Debian commands for showing installation status

Splunk package status:

```
dpkg --status splunk
```

5. List all packages:

```
dpkg -list
```

Next, we installed Splunk universal forwarder in MSCS 6560 Lab virtual machine VM0. mscsnet.edu.

Splunk Universal Forwarder Install via TAR file on UBUNTU

1. Verify system requirements

2. Download the tar file from Splunk website

https://www.splunk.com/en_us/download/universal-forwarder.html (or use CLI

downloadable WGET)[26]. You would have to create an account with Splunk in order to download the tar file.

3. Copy on tar file to the server on a temp location.

4. To install the forwarder into the folder /opt/splunkforwarder, run:

```
tar xvzf splunkforwarder-<...>-Linux-x86_64.tgz -C /opt
```

5. To install the forwarder into the current working directory under the splunkforwarder folder, run:

```
tar xvzf splunkforwarder-<...>-Linux-x86_64.tgz
```

Splunk Universal Forwarder Install via DEB package on UBUNTU Linux

1. Verify system requirements

You can install the Splunk Enterprise Debian package only into the default location, /opt/splunk.

This location must be a regular directory and cannot be a symbolic link.

You must have access to the root user or have sudo permissions to install the package.

The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for /opt/splunk, then use a tar file to install the software.

2. Download the DEB file via CLI downloadable WGET [26]. You would have to create an account with Splunk in order to download the deb file.

```
wget -O splunk_package_name.deb
```

3.Installation procedure

Run the dpkg installer with the Splunk Enterprise Debian package name as an argument.

```
dpkg -i splunk_package_name.deb
```

4. Debian commands for showing installation status

Splunk package status:

```
dpkg --status splunk
```

Once the Splunk enterprise and Splunk universal forwarder was installed, it was time to start harvesting logs from the target server which were our MSCS 6560 lab computers.

The same process can be applied to any server in Marquette University.

Log forwarding from Splunk Universal forwarder to Splunk Enterprise.

Step1: Identify the log file name and location.

Step2: Use below syntax to setup log forwarding.

```
sudo /opt/splunkforwarder/bin/splunk add monitor  
log_path/file -index index_name -  
sourcetype Source_type_name.
```

Escape :

```
sudo /opt/splunkforwarder/bin/splunk add monitor  
/opt/tomcat7/logs -index main -sourcetype Tomcat7
```

Verify configuration by opening file at the following:

```
sudo su  
vi opt/splunkforwarder/etc/apps/search/local/inputs.conf
```

As part of the MSCS 6560 class students go through weekly assignments. Our plan is to harvest logs from servers after completion of each week, when students completes their weekly assignment.

The following sections trace the sequence of assignments for students in the Principles of Service Management and System Administration

Lab Assignments

Assignment 1:

VMs are assigned to the students for performing lab assignments. During the assignment students' setup their accounts and update the VMs with required updates. During this process we harvest syslog, authlog and dpkglog.

- syslog: these logs are used to obtain general information about the system.
- auth.log: these logs are used specifically for authentications and logging into the system.

- dpkg.log: these logs are concerned with packages installed into the system.

While reviewing the first day logs, students discover something suspicious; it turns out that our lab VMs were attacked by malicious actors. They were trying to gain access to our server via brute force attacks. Students learn the ubiquitous nature of surveillance and attack by adversaries.

Below is the screenshot of the Failed login attempts during 1st week of log collection.

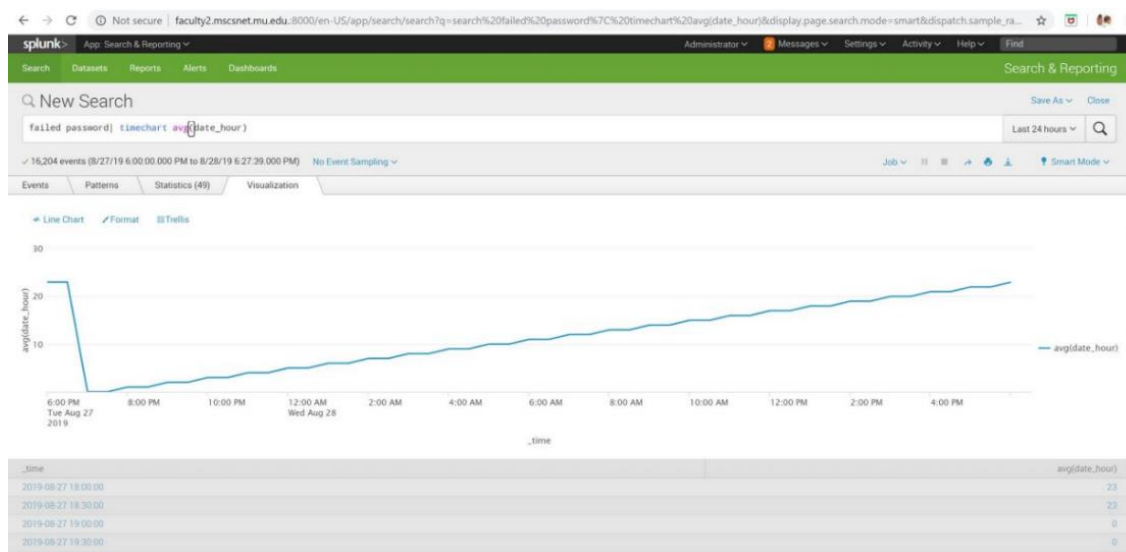


Figure 5. Auditd Log Status

To counter this, we installed “Fail2ban” package on the server. This was then added to student’s initial assignment to install “Fail2ban” during their first week assignment.

Assignment 2:

During Assignment 2 students are required to create necessary accounts on the server for future assignments. These accounts will be used for activities such as installing LAMP (Suite of Softwares). To monitor login attempts made by the new accounts, students are instructed to install auditd [28]. Auditd can track many event types:

- Audit file access and modification
- See who changed a particular file
- Detect unauthorized changes
- Monitoring of system calls and functions
- Detect anomalies like crashing processes
- Set tripwires for intrusion detection purposes
- Record commands used by individual users

Our focus was limited to monitoring of the successful and unsuccessful login attempts made on to the server.

Students enable auditlog forwarding to Splunk enterprise by running the following command on the server.

```
sudo /opt/splunkforwarder/bin/splunk add monitor  
/var/log/audit/audit.log -index main -sourcetype auditlog
```

Below is the screenshot of the audit log stats which was being monitored.

Events										
Patterns		Statistics (2,390,926)		Visualization						
20 Per Page		Format		Preview						
				< Prev 1 19 20 21 22 23 24 25 26 ... Next >						
.time	acct	date_hour	date_mday	date_minute	date_month	date_second	date_wday	date_year	result	
2019-11-10 02:36:52.911	28696E76616C6964207573657229	8	10	36	november	52	sunday	2019	res=failed	
2019-11-10 02:36:52.911	root	8	10	36	november	52	sunday	2019	res=failed	
2020-01-06 06:25:05.206	root	12	6	25	january	5	monday	2020	res=failed	
2020-01-06 06:25:05.206	root	12	6	25	january	5	monday	2020	res=failed	
2020-01-06 06:25:03.458	root	12	6	25	january	3	monday	2020	res=success	
2020-01-06 06:25:03.454	root	12	6	25	january	3	monday	2020	res=success	
2020-01-06 06:25:01.958	root	12	6	25	january	1	monday	2020	res=failed	
2020-01-06 06:25:01.958	root	12	6	25	january	1	monday	2020	res=failed	
2020-01-06 06:25:01.042	root	12	6	25	january	1	monday	2020	res=success	

Figure 6. Auditd Logs Sample

Assignment 3:

In this assignment students add LAMP (Suite of Software) into the system.

LAMP is a software bundle that stands for Linux, Apache, MySQL and PHP/Perl/Python; these software packages are essential for forming a web service solution stack. With the LAMP (Suite of software) being installed to the system, it broadens the threat landscape as more services running on the system. It becomes imperative to have a monitoring setup for the installed applications.

Since it is essential to closely monitor those services, Apache's logs must be monitored and forwarded using Splunk Forwarder. The two main logs that will be monitored in this environment are "access.log" and "error.log"; which are located at the Apache2 folder under the log folder directory.

As more services are running within the system, the more discoverable that system becomes. Discoverability can be associated with the increased number of events as shown in Snapshot 3. However, not all of these events and attacks pose threats to systems if those systems are well maintained and secure. The total amount of events recorded by Splunk in this stage between 10/01/2019 and 10/31/2019 was around

3,062,802 events and the following Snapshot gives a brief summary of the events collected.

source

×

13 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%	
/var/log/auth.log	2,115,577	69.071%	<div></div>
/var/log/audit/audit.log	907,015	29.613%	<div></div>
/var/log/mysql/error.log	20,485	0.669%	<div></div>
/var/log/syslog	14,670	0.479%	
/var/log/dpkg.log	2,722	0.089%	
/var/log/apache2/access.log	1,266	0.041%	
/var/log/apache2/error.log	730	0.024%	
/var/log/unattended-upgrades/unattended-upgrades-dpkg.log	134	0.004%	
/var/log/apt/term.log	125	0.004%	
/var/log/apt/history.log	78	0.002%	

Figure 7. Splunk Table Display

The table indicates that there was a vast increase of events recorded from the Authlog files because of the added services that were running in the system. It is also important to mention that the “fail2ban” package installed in the system has helped reduce the number of these attacks. If the “fail2ban” package was not installed and configured, then the entries of Authlog file would have increased vastly.

Assignment 4:

This stage is devoted to the WordPress installation, the student's first externally focused service. It is important to note that while trying to install WordPress in the latest Ubuntu version using the documents provided, the installation failed many times and snapshots were used to go to the previous stage and redo the installation process until WordPress was installed properly. The instructions that were followed to install WordPress were taken from an online-article titled "How to Install WordPress with LAMP Stack on Ubuntu 18.04" that provided an easier approach to install WordPress (How to Install WordPress with LAMP Stack on Ubuntu 18.04: RoseHosting).

While log files were monitored for a short period of time in this stage; about 2 days, it clearly showed that attacks are rising against the system. This is due to running more services in the system that advertise their existence to external entities; hence, the increase of discovery of the system by others and the rise of the attacks in this stage. The following snapshot breaks-down the file collected at this stage:

source ×

18 Values, 100% of events Selected Yes No

Reports

[Top values](#)
[Top values by time](#)
[Rare values](#)

Events with this field

Top 10 Values	Count	%	
/var/log/auth.log	4,386,286	80.863%	<div></div>
/var/log/audit/audit.log	907,015	16.721%	<div></div>
/var/log/mysql/error.log	42,336	0.78%	<div></div>
/var/log/dpkg.log	41,622	0.767%	<div></div>
egsyslog.csv	20,803	0.384%	
/var/log/syslog	19,663	0.362%	
/var/log/cloud-init.log	2,043	0.038%	
/var/log/kern.log	1,371	0.025%	
/var/log/apache2/access.log	1,266	0.023%	
/var/log/apache2/error.log	730	0.013%	

Figure 8. Updated Splunk Table

Assignment 5:

While this stage is dedicated to a lab that requires students to learn about hardening the security of their systems by reading few articles, there are no mandatory requirements for changes to be made into the systems. However, it is useful to consider monitoring some of the logs such as `dpkg.log` files to detect any new packages in this stage. Another logs that is useful in this stage is to look into the file that lists the current users of the system, which was created in the second assignment to determine whether the users were removed from the system or not.

Due to the nature of this stage and how it might differ from one virtual machine to another based on the students' choices of maintaining the environment and hardening the system's security, there are no other recommendations of monitoring the systems other than the ones suggested in the previous section.

Assignment 6:

In this stage, Nagios software will be installed in the system by the students to provide them with hand-on experience of one of the well-known monitoring tools used for Linux systems. Nagios logs will be forwarded to Splunk enterprise for UBEA. However, this stage was not covered in our Cyber-SUSS experiment.

Final Assignment:

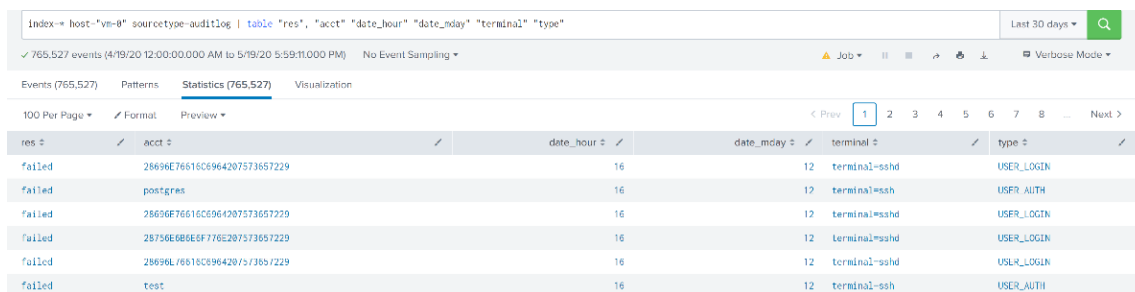
The activity of this stage is to monitor the virtual machines after students are done adding and using services. In this stage, all unused packages should be uninstalled, all user ids for other students should be removed and all unused services must be turned-off or paused. During this stage, a vulnerability scanning tool is used to provide reports that students review.

Splunk Machine learning Implementation

The following sections document the measures performed for the experiment.

ML model creation by SPL ML toolkit.

We collected about a month's worth of data into Splunk Enterprise from the student VM machines and developed a simple use case of "Suspicious logins" on the server. We used SPL (Splunk Processing Language) to select and format specific machine's login data as shown below.



The screenshot shows a Splunk search interface with the following SPL query: `Index=* host="vm-0" sourcetype=auditlog | table "res", "acct" "date_hour" "date_mday" "terminal" "type"`. The results table displays failed login attempts with columns for result status, account ID, date hour, date mday, terminal type, and event type.

res	acct	date_hour	date_mday	terminal	type
failed	28696E76616C6964207573657229	16	12	terminal-sshd	USER_LOGIN
failed	postgres	16	12	terminal-ssh	USER_AUTH
failed	28696E76616C6964207573657229	16	12	terminal-sshd	USER_LOGIN
failed	28756E08060F776E207573657229	16	12	terminal-sshd	USER_LOGIN
failed	28696E76616C6964207573657229	16	12	terminal-sshd	USER_LOGIN
failed	test	16	12	terminal-ssh	USER_AUTH

Figure 9. SPL Snippet

Splunk has a variety of functionalities that can be used for various purposes. We downloaded the "Splunk Machine Learning Toolkit" and "Phantom Add on" on the Splunk Enterprise server, as shown in the screenshot below.

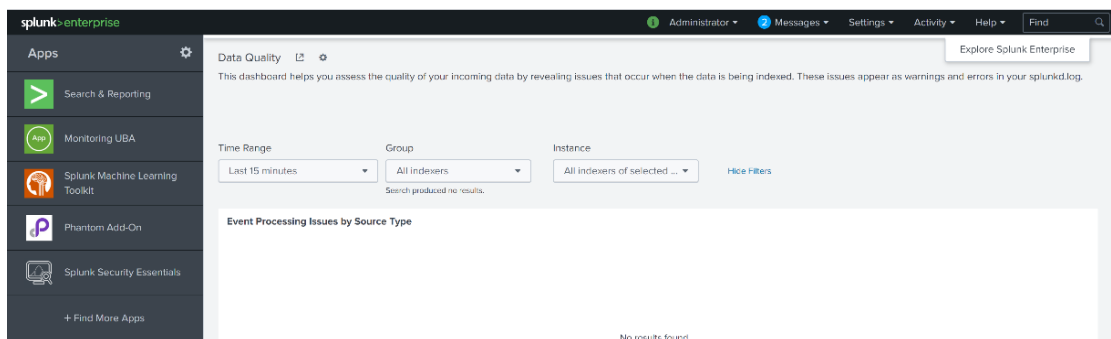


Figure 10. Splunk ML Learning Tool Kit

After loading the tool, “Splunk Machine learning” was used to build a regression model.

We needed the “Phantom Add-On” App to connect to the Phantom server and send alerts to it. The Phantom server required installation on a separate server.

To initiate communication and send data, inside the “Splunk Machine Learning” App click on “Experiments” tab to create a New Experiment.

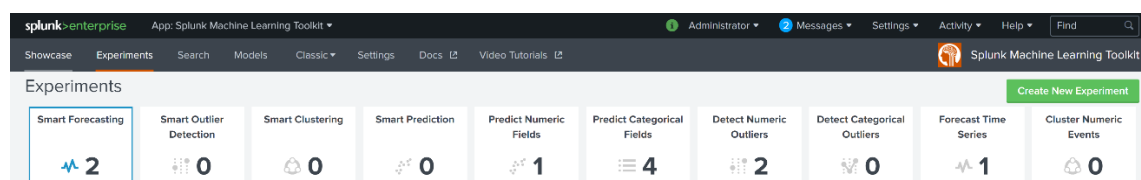


Figure 11. Splunk ML Options

For our use-case we selected “Predict Categorical fields” and clicked on “Create new Experiment”

 The screenshot shows a 'Create New Experiment' dialog box. It has a title bar with a close button (X). Inside, there are three input fields: 'Experiment Type' with a dropdown menu showing 'Predict Categorical Fields', 'Experiment Title' with the text 'Suspected Login Model Experiment', and 'Description' with the text 'Experiment on Login data from server VM-0'. At the bottom right, there are two buttons: 'Cancel' and 'Create'.

Figure 12. Create a ML Experiment

Under Experiment search bar, use an SPL command to fetch the data and according to requirements, choose last data for our regression modelling.

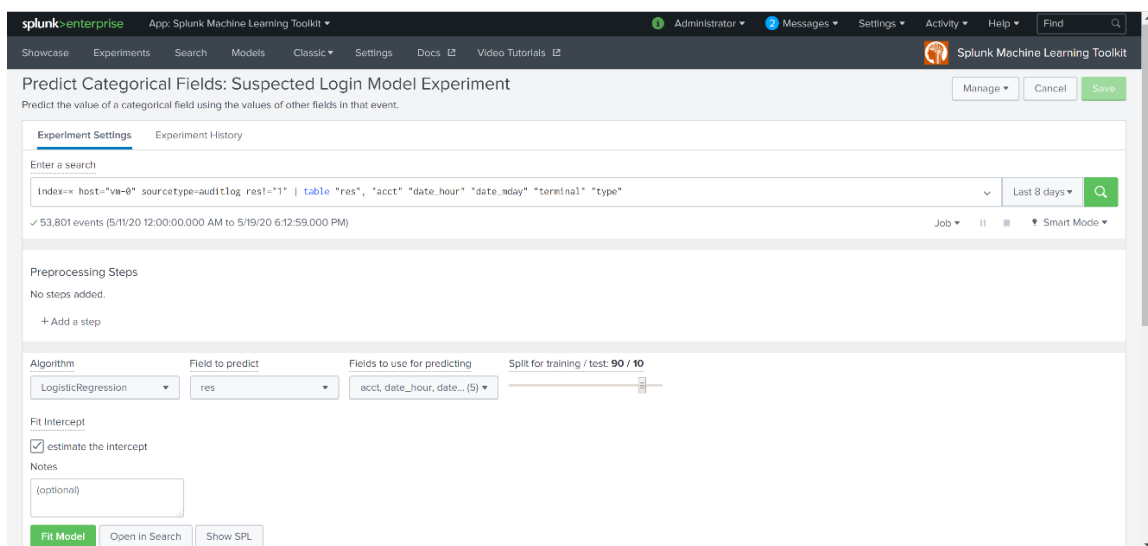


Figure 13. Categorical Prediction

Use the drop-down list to select the desired algorithm (Logistic Regression was chosen in this experiment) for modelling. “res” is our resultant field which is to be predicted. We have selected features for modelling under tab “field to use for predicting”. Lastly, use the slide bar to select the training and test partition. Once all fields are completed, we select “Fit Model” and we will have our predictions.

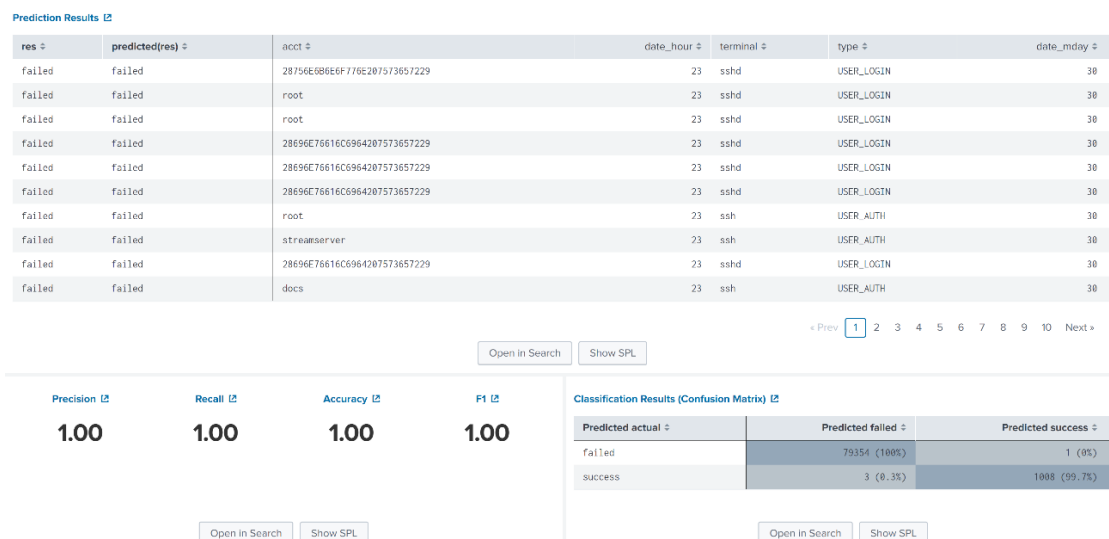


Figure 14. Machine Learning Results

You can view the SPL running behind the scene by right clicking on the Blue highlighted hyperlinks. Please see the below screenshot.

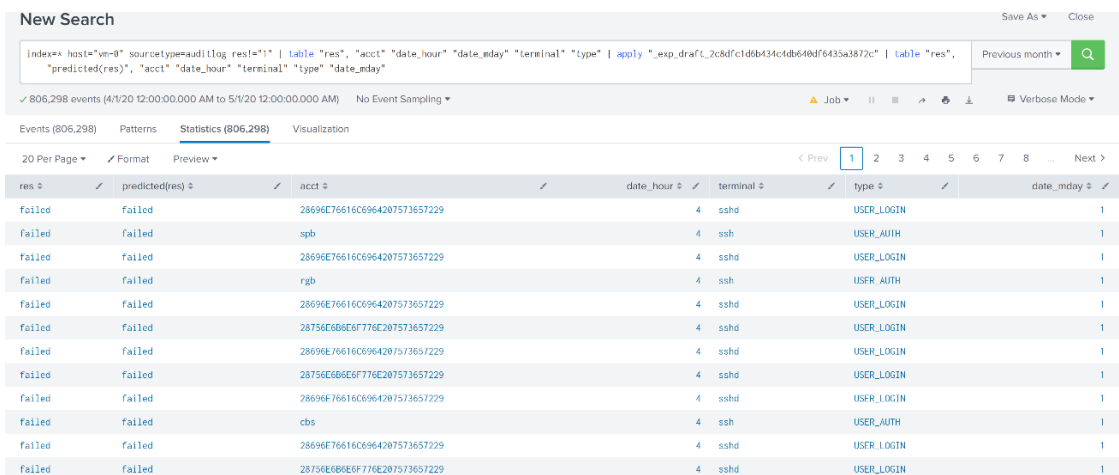


Figure 15. SPL ML Search

A small tweak to the SPL will give us the suspected login result.

New Search Save As Close

Index= host="vm-6" sourcetype=auditlog res="1" | apply "exp_draft_2c8dfc1d8b434c4db648cf6435a3872c" | table "res", "predicted(res)", "acct" "date_hour" "date_mday" "terminal" "type"

search "predicted(res)"="failed" | search res=success

✓ 47 events (4/1/20 12:00:00.000 AM to 5/1/20 12:00:00.000 AM) No Event Sampling

Events (47) Patterns **Statistics (47)** Visualization

20 Per Page Format Preview Prev 1 2 3 Next

res	predicted(res)	acct	date_hour	date_mday	terminal	type
success	failed	tom	1	1	ssh	USER_AUTH
success	failed	tom	15	38	ssh	USER_AUTH
success	failed	kunal	5	38	ssh	USER_AUTH
success	failed	tom	14	29	ssh	USER_AUTH
success	failed	tom	11	28	ssh	USER_AUTH
success	failed	tom	2	27	ssh	USER_AUTH
success	failed	kunal	1	27	ssh	USER_AUTH
success	failed	tom	23	26	ssh	USER_AUTH
success	failed	tom	23	26	ssh	USER_AUTH
success	failed	tom	22	26	ssh	USER_AUTH
success	failed	tom	22	26	ssh	USER_AUTH
success	failed	tom	22	26	ssh	USER_AUTH
success	failed	tom	21	26	ssh	USER_AUTH
success	failed	tom	21	26	ssh	USER_AUTH

Figure 16. SPL ML Search for anomalies

To apply the model to incoming rows, we save the model by selecting the “Save” button on the top right corner. Once the model is saved it appears in the list of saved experiments as shown in this Figure.

splunk enterprise App: Splunk Machine Learning Toolkit Administrator Messages Settings Activity Help Find

Showcase **Experiments** Search Models Classic Settings Docs Video Tutorials

Experiments Create New Experiment

Smart Forecasting 2	Smart Outlier Detection 0	Smart Clustering 0	Smart Prediction 0	Predict Numeric Fields 1	Predict Categorical Fields 4	Detect Numeric Outliers 2	Detect Categorical Outliers 0	Forecast Time Series 1	Cluster Numeric Events 0
----------------------------	----------------------------------	---------------------------	---------------------------	---------------------------------	-------------------------------------	----------------------------------	--------------------------------------	-------------------------------	---------------------------------

4 Experiments Filter by experiment name

Experiment Name	Algorithm	Actions
> 24 hour suspected login	LogisticRegression	Manage Publish
> Login Experiment - Test2	LogisticRegression	Manage Publish
> Login_Experiment_04_26	LogisticRegression	Manage Publish
> Suspected Login Model Experiment	LogisticRegression	Manage Publish

Figure 17. Splunk ML Experiment page

We use this saved experiment model to issue alerts on the incoming data. By clicking on the manage button and selecting the option of “create alert” we enable us sending an alert in case of any suspicious logins on the server. However, in this experiment to demonstrate the use of Phantom as a SOAR system, we wanted an

automated action to be taken. We have the option of setting/editing the option of training schedule by clicking “Edit Training Schedule”

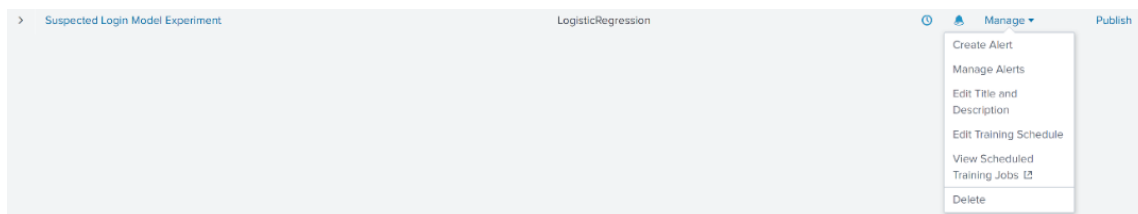


Figure 18. Managing Splunk ML models

This option allows us to periodically train our models based on the last captured data.

 A screenshot of the 'Edit Training Schedule' dialog box. It has a title bar with 'Edit Training Schedule' and a close button. The main content area includes:

- 'Enable Scheduled Training' with a checked checkbox.
- 'Schedule' dropdown set to 'Run every day'.
- 'At' dropdown set to '0:00'.
- 'Time Range' dropdown set to 'Last 7 days'.
- 'Schedule Priority' dropdown set to 'Default'.
- 'Schedule Window' dropdown set to 'No window'.
- 'Trigger Actions' section with a '+ Add Actions' button.
- 'When triggered' section with a dropdown showing 'Send email' (with an envelope icon) and a 'Remove' button.
- 'To' field containing 'kunal.singh@marquette.edu'.
- Text below the field: 'Comma separated list of email addresses. Show CC and BCC'.

 At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 19. Setting a Training Schedule for the ML model

We were able to create the model and validate that the predictions are working as expected; we were also able to create alerts and train the model based on a schedule.

Setup Splunk Phantom App on Splunk Enterprise

In our experiment we used the SIEM via Splunk and performed UEBA via a Splunk Machine Algorithm model on the incoming data. We would send the suspected alerts to Splunk Phantom to implement SOAR capabilities.

To setup SOAR capabilities we would need to send the suspicious alert to the Splunk Phantom Server.

Splunk Phantom needs to be configured to talk to the Splunk Enterprise to allow Splunk Machine Learning to send alerts to Phantom for further investigation and preventive measures.

After Splunk Phantom app is installed, we navigate to Phantom Add On app

We login to Splunk UI and click on button called “+Find more Apps” as shown in below Figure.

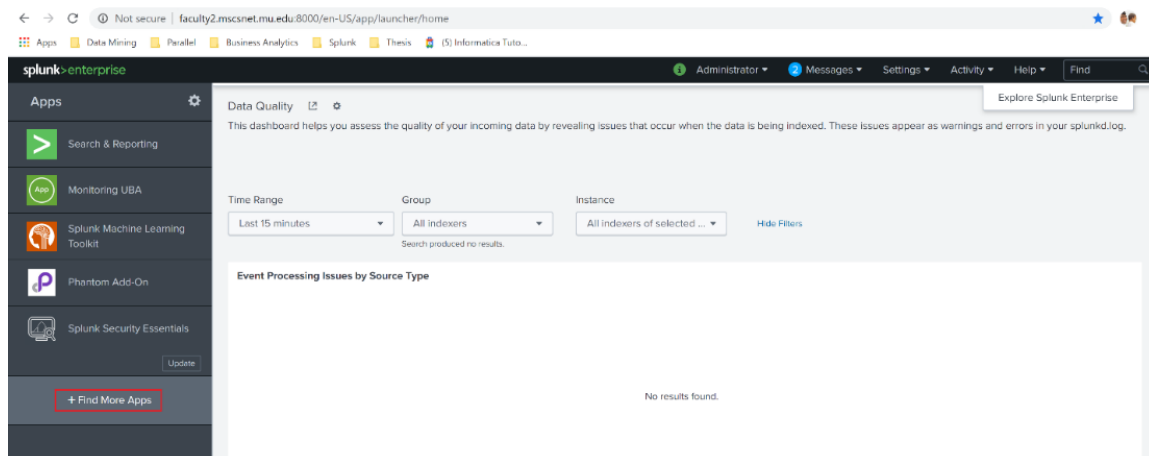


Figure 20. Adding Phantom Application

Type “Phantom” in the search box and Hit Enter to receive search results.

Click on the install button to install Phantom App on Splunk Enterprise.

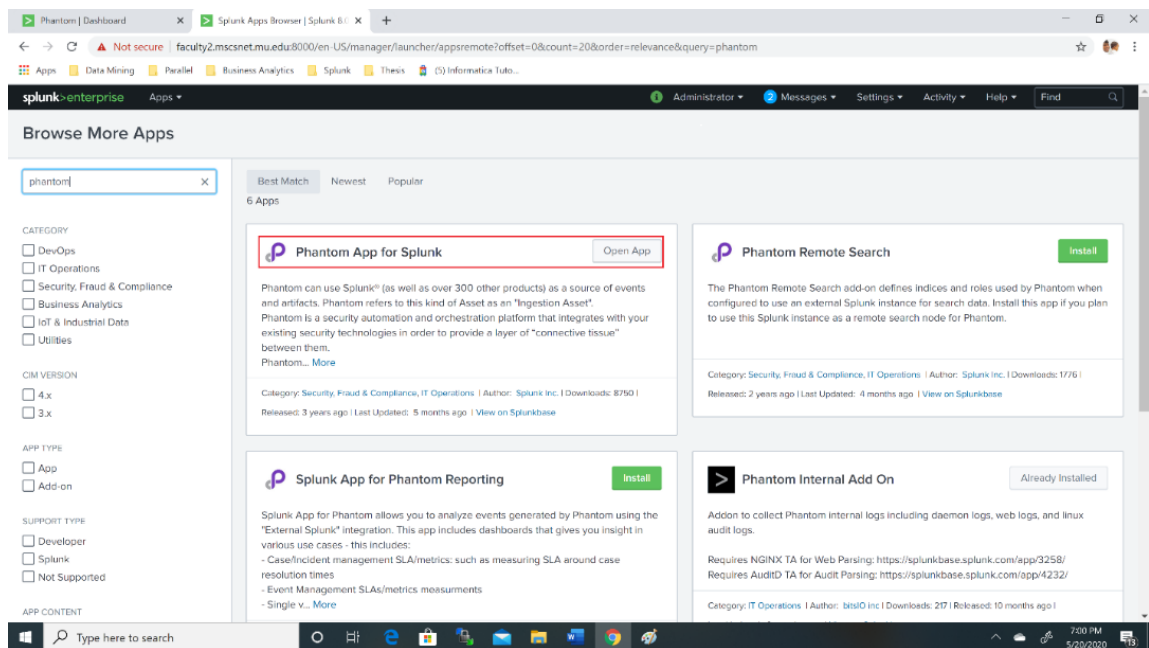


Figure 21. Selecting the Phantom Add-on

Once the app is installed, it will appear on the left-hand panel of the Splunk Enterprise main page.

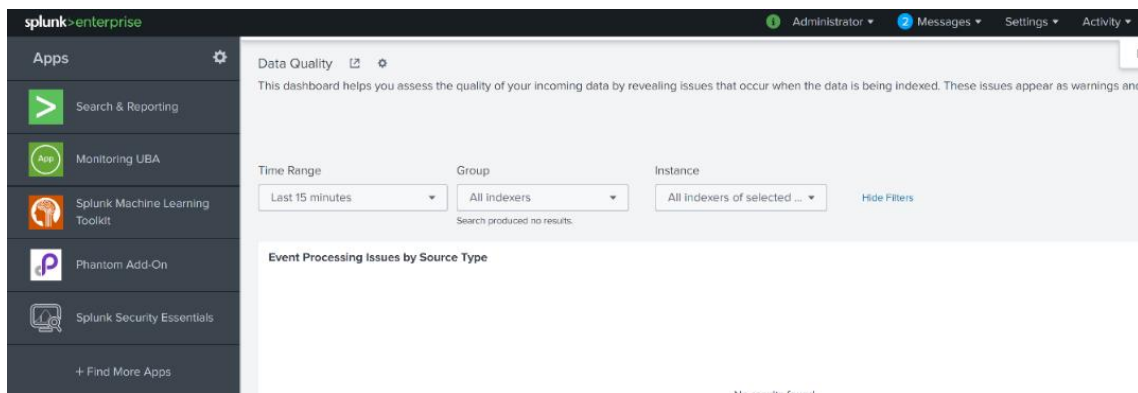


Figure 22. After adding the Application

Next step would be to setup Splunk Phantom Add-On to talk to Splunk Phantom server on its dedicated server by clicking on create server button.

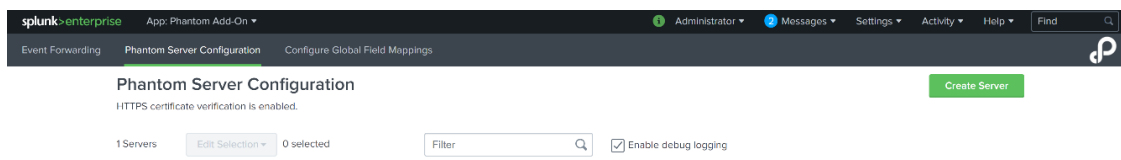


Figure 23. Creating a Connection to the Phantom Server

Establish connection with Splunk Phantom server

To configure the Splunk Phantom server, follow these steps: [24]

1. Navigate to the Phantom Add-On for Splunk installed on your Splunk platform instance.
2. Click the Phantom Server Configuration tab.
3. Click Create Server.

To add a new server, use an authorization token from Splunk Phantom. To get an authorization token, follow these steps:

1. Navigate to your Splunk Phantom instance.
2. From the main menu, select Administration.
3. Select User Management > Users.
4. Click on the ... icon in the card for any Automation user and select Edit.
5. Change the Allowed IPs field to reflect the IP address or IP range for the Splunk platform instance.
6. Copy the text in the Authorization Configuration for REST API box.
7. Click Save.
8. Navigate back to the Phantom Add-On for Splunk on your Splunk platform instance and paste the authorization token in the Authorization Configuration box.
9. Enter an optional name for the server. This will show up later in Splunk Phantom as your container name, so pick a name you can easily identify.
10. (Optional) Configure a Proxy server.
11. Click Save. A page shows your new server. If you have multiple servers, they are listed on this page.
12. To test your server, click Manage > Test Connectivity. A success message appears if the server is working correctly.

The screenshot below shows confirmation of the connectivity test with the Splunk Phantom server.

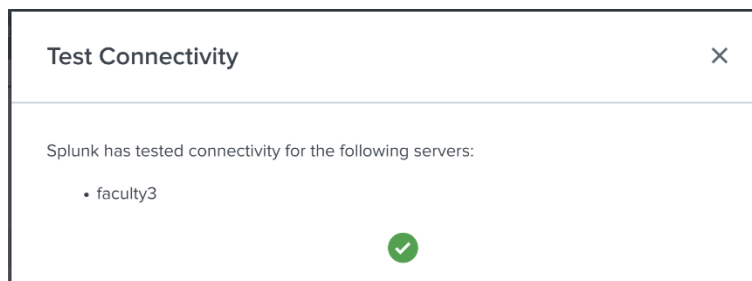


Figure 24. Testing Connectivity with Phantom

After connectivity test, Phantom Server Configuration tab should look like this

Figure 25.

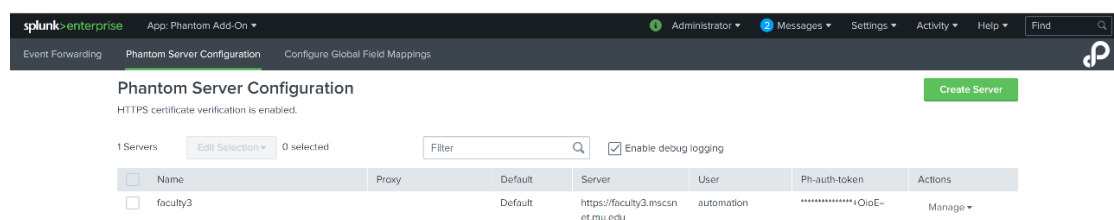


Figure 25. Status after Configuration

Publish SPL ML model

To send suspicious login event alerts to Splunk Phantom server, we need to publish the model on the Splunk Add-On app. Below are the steps to publish a model to the Splunk Add-On app.

Click on the publish button to publish the model, provide a name to the model as shown in the figure below. Please make sure to select Destination App as “Phantom Add-On”.

Publish the Models

Publishing an Experiment model means the main model with any associated preprocessing models will be copied as lookup files in the user's namespace within the selected destination app.

New Main Model Title:

Model names must start with a letter or underscore and contain only letters, numbers, and underscores

Destination App:

- Monitoring UBA
- ✓ Phantom Add-On
- Search & Reporting
- Splunk Machine Learning Toolkit
- Splunk Security Essentials

Figure 26. Publishing the Model

Once the model is published, it will appear under the “Models” section of the “Splunk Machine Learning” App.

Model Name	Algorithm	Actions	Owner	App	Sharing
Suspected_Login_Model	LogisticRegression	Delete	admin	phantom	Global

Figure 27. Displaying Models

Please make sure you open the permission for the model to have to access to other Apps as well. Otherwise you will not be able to use this model in any other Splunk apps.

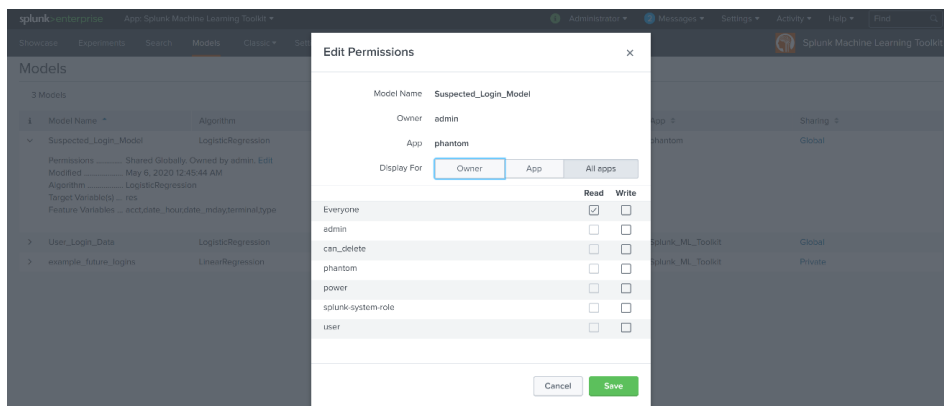


Figure 28. Granting Read permission

Forward SPL ML events to Splunk Phantom

To forward events to Splunk Phantom via Phantom Add on app, we must have our search saved as “Report”.

Follow below steps to save search as “Report”

Click on “Search and Reporting” Tab on the left panel and use below SPL to run the search.

```
"index=* host="vm-0" sourcetype=auditlog res!="1" |
apply "Suspected_Login_Model " | table "res", "predicted(res)",
"acct" "date_hour" "date_mday" "terminal" "type" | search
"predicted(res)="failed" | search res=success"
```

We have updated the apply part of the search from

```
"_exp_draft_2c8dfc1d6b434c4db640df6435a3872c" to
```

“Suspected_Login_Model” because we have published our model and it can be used against the incoming data.

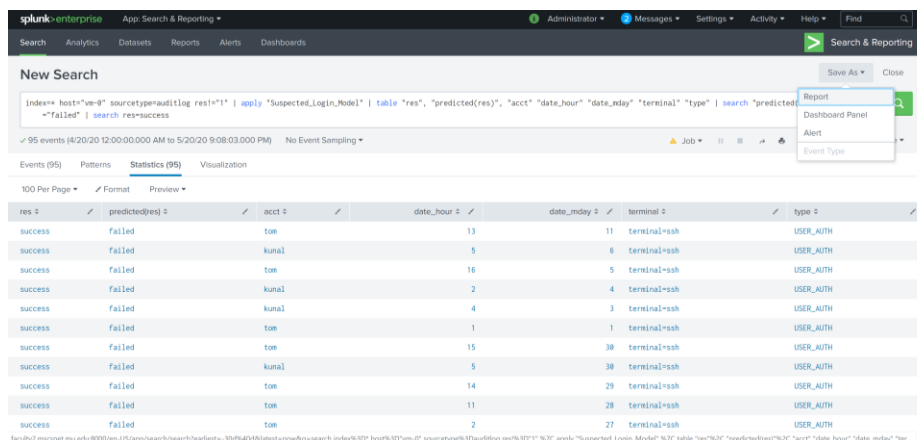


Figure 29. Save Search as report

Save this search as report and open read permission. We saved this as “Suspicious Login Report”. Now, this report is going to be visible under Phantom App event forwarding.

To setup event forwarding to Splunk Phantom, go back to Splunk Phantom App by clicking on “Splunk Phantom App” on the left panel icon.

Click on the “Add New” button to setup event forwarding from Splunk Enterprise to Splunk Phantom.



Figure 30. Forwarding the Event to Phantom

Click on the option “Saved Search Export”

Provide a desired name for the Saved Event forwarding. We named it as “Suspicious Logins”. Also, choose the desired “Saved Report” from the drop-down list. Your Saved search will not appear in this drop down if you have not saved one and opened the read permission. You can leave the “Container Label” blank.

Click on Next

The screenshot shows the 'Add New' dialog in the Splunk Phantom interface, specifically for the 'Saved Search Export' configuration. The dialog is titled 'Step 1 of 2'. It contains the following fields and options:

- Name:** A text input field containing 'Suspected Logins'.
- Saved Search:** A dropdown menu showing 'Suspicious Login Report'.
- Artifact Label - Optional:** A text input field containing 'Default Artifact Label'.
- Select Destination:** A dropdown menu showing 'faculty3'.
- Container Name - Optional:** A dropdown menu showing 'Auto-generate'.
- Container Label - Optional:** A text input field containing 'Default Container Label'.
- Schedule:** Radio buttons for 'Real Time' and 'Every'. The 'Every' option is selected, with a value of '5' in a spinner box and 'Minutes' as the unit.

At the bottom right of the dialog are 'Cancel' and 'Next' buttons. The background shows the 'Event Forwarding' section of the Splunk Phantom dashboard with a table listing existing configurations.

Figure 31. Name the Event

Choose the “Severity” and “Sensitivity” of the alert which you would like to see on the Splunk phantom dashboard.

Map the required fields with CEF (Common Event Format) fields to setup alert forwarding to Splunk Phantom.

Add New
Step 2 of 2

Configuring [Suspicious Login Report](#) on **faculty3**

Severity and Sensitivity Fields

Severity ? High

Sensitivity ? TLP: Red

Unmapped Fields (7)

Group ?	Search Fields	CEF Fields	Contains	
<input checked="" type="checkbox"/>	acct	Choose the CEF field n...	Select contains	-
<input checked="" type="checkbox"/>	date_hour	Choose the CEF field n...	Select contains	-
<input checked="" type="checkbox"/>	date_mday	Choose the CEF field n...	Select contains	-
<input checked="" type="checkbox"/>	predicted(res)	Choose the CEF field n...	Select contains	-

Cancel
Previous
Save and Preview
Save and Close

Figure 32. Common Event Format mapping

Click on Save and preview to verify the events which will be forwarded to Splunk phantom. You could also modify the preview window time to “All Time” to validate event creation.

Click on the green button called “Send to Phantom” to send a test alert to the Splunk Phantom.

Preview for Suspected Logins1

Preview window

All time

✓ All time

Last 5 minutes

Last hour

Last day

data

Suspected Logins1

red

Severity high

Send to Phantom

Your search matched the following data

Successfully parsed CEF fields

Container Name	Suspected Logins1
Sensitivity	red
Severity	high

Send to Phantom

Your search matched the following data

Done

Figure 33. Alert Preview

Open the Splunk Phantom UI and check for the event alert on the main page. If you see the alert, then your event forwarding setup is complete. Congratulations!!

Splunk Phantom SOAR Setup

Splunk Phantom enables SOAR capabilities. It hosts playbooks for the automation, and they are executed as per designed directions. Splunk phantom playbooks could be used by a SOC analyst to further investigate a suspicious activity and initiate preventive action as defined in the playbook. These playbooks can be setup to execute automatically or they can seek approval before execution. Splunk Phantom also enables us to directly execute playbooks for any set of event/events.

Splunk Phantom Install

Splunk phantom was installed on server “faculty3.mscsnet.edu”. Detailed documentation for Splunk phantom install can be found here <https://docs.splunk.com/Documentation/Phantom/4.8/Install/InstallRPM>.

Once Splunk installation is completed, we were able to access “Splunk Phantom” UI as shown in below Figure.

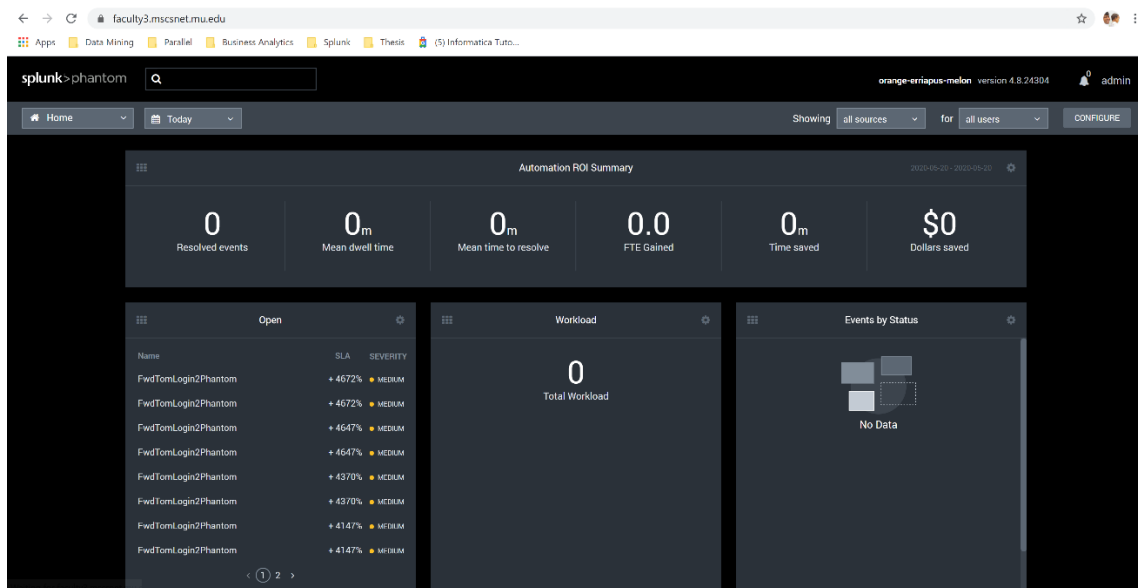


Figure 34. Phantom Dashboard

Splunk SOAR playbook

To create a new playbook, click on drop down on the left-hand panel. Select option “Playbooks”

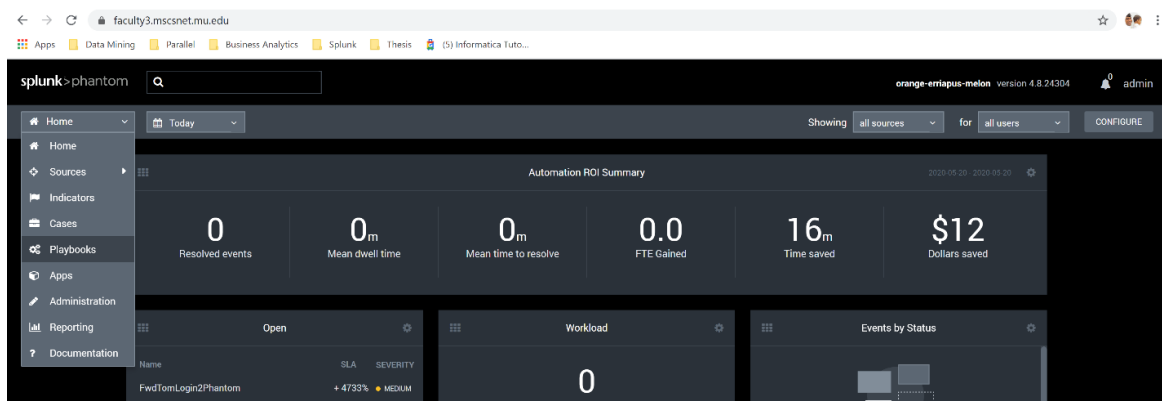


Figure 35. Creating Playbooks

You will see list of pre-defined playbook, you can either use them or create your own by clicking “+ Playbook” button.

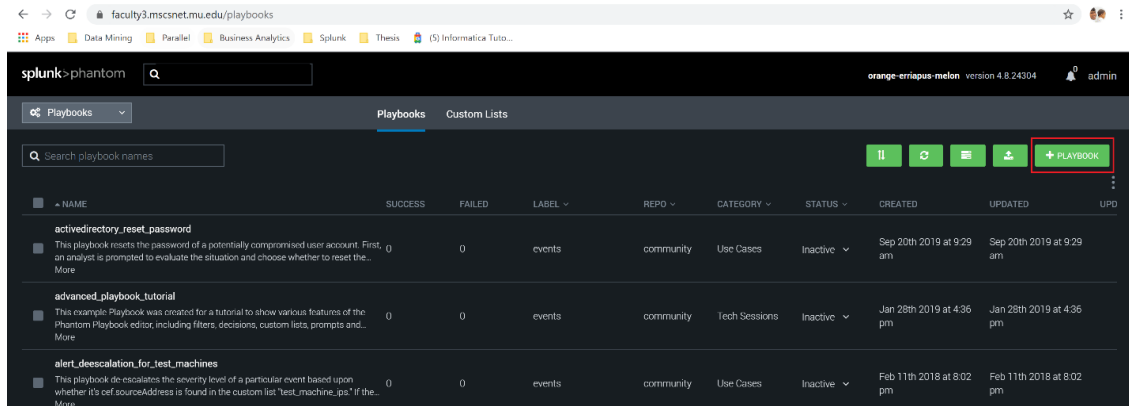


Figure 36. Displaying Playbooks

New window will open with Start and End task already in place. We can add desired tasks as per our requirement.

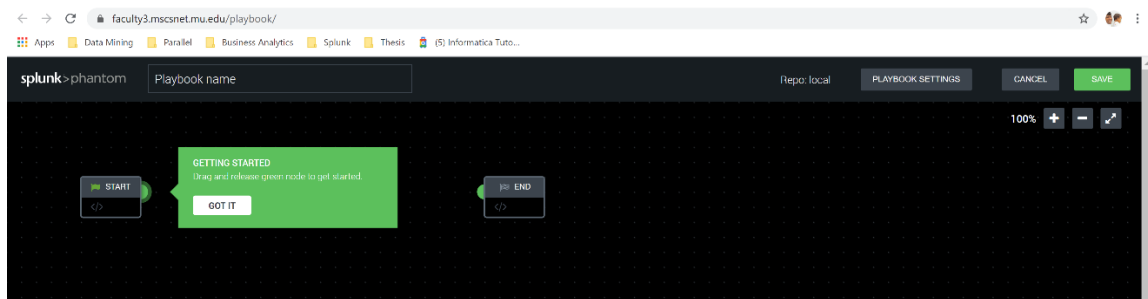


Figure 37. Adding tasks to the Playbook

At this time, we have added an approver task and an email task to the playbook. This will send us an email alert as and when an event is forwarded to Splunk Phantom.

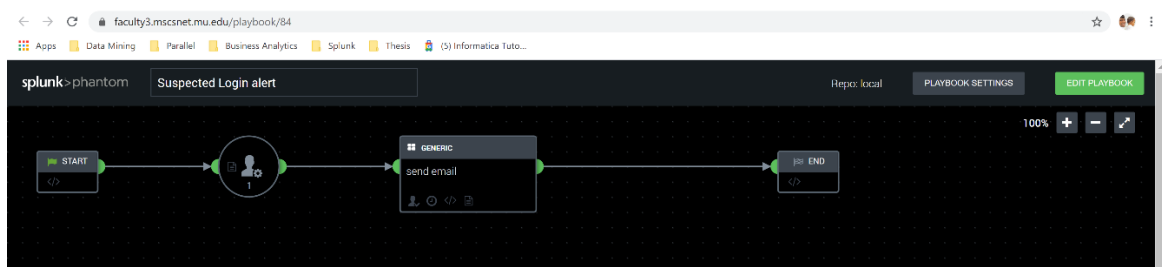


Figure 38. Email Alerts

Provide the “From” and “To” email address in the configuration screen and you are good to go. Click on the save button to save the playbook.

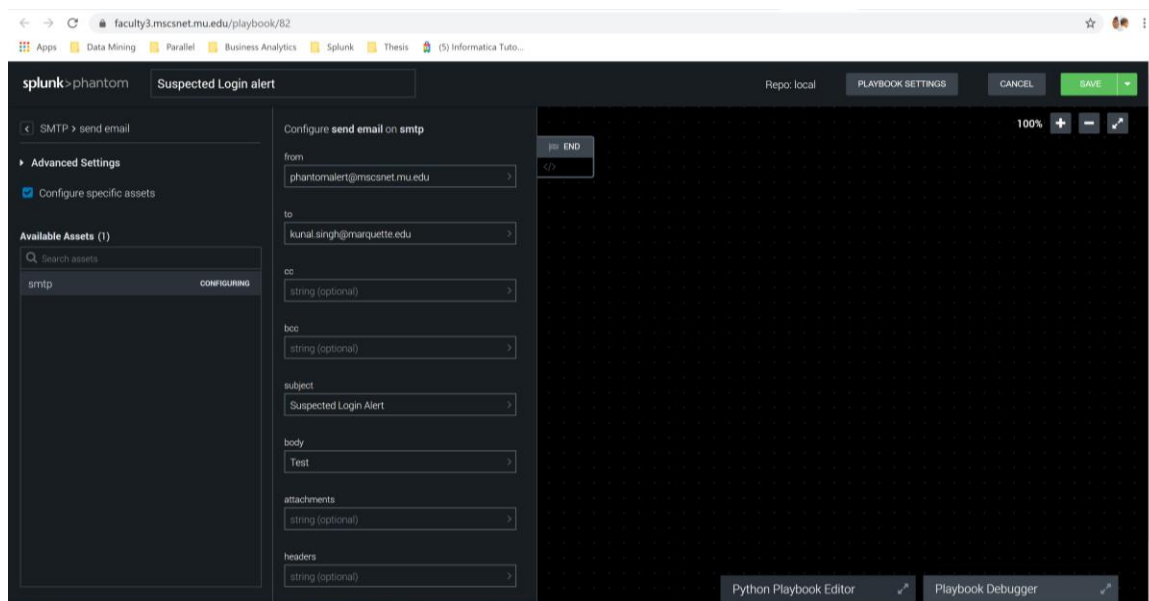


Figure 39. Saving the Playbook

You could also view the python code by clicking “Python Playbook Editor” which gets executed in the background while playbook execution.

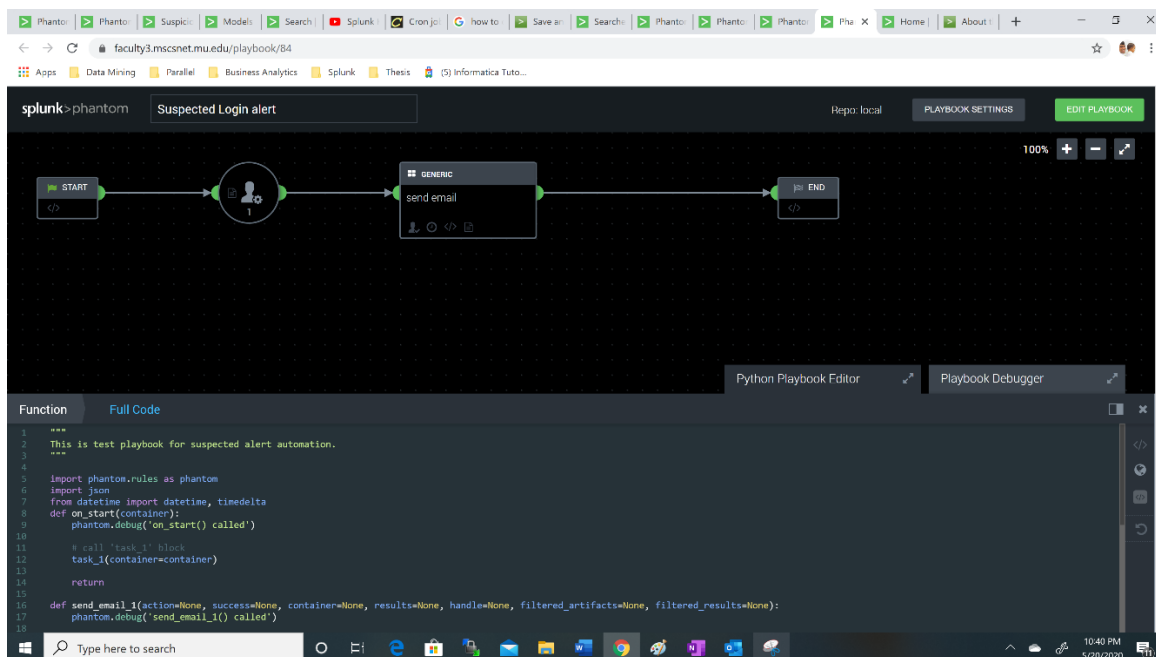


Figure 40. Python Generated for the Playbook

Handling New Event via Splunk Phantom UI

A SOC analyst can look at the new events by going to Source --> New Events.

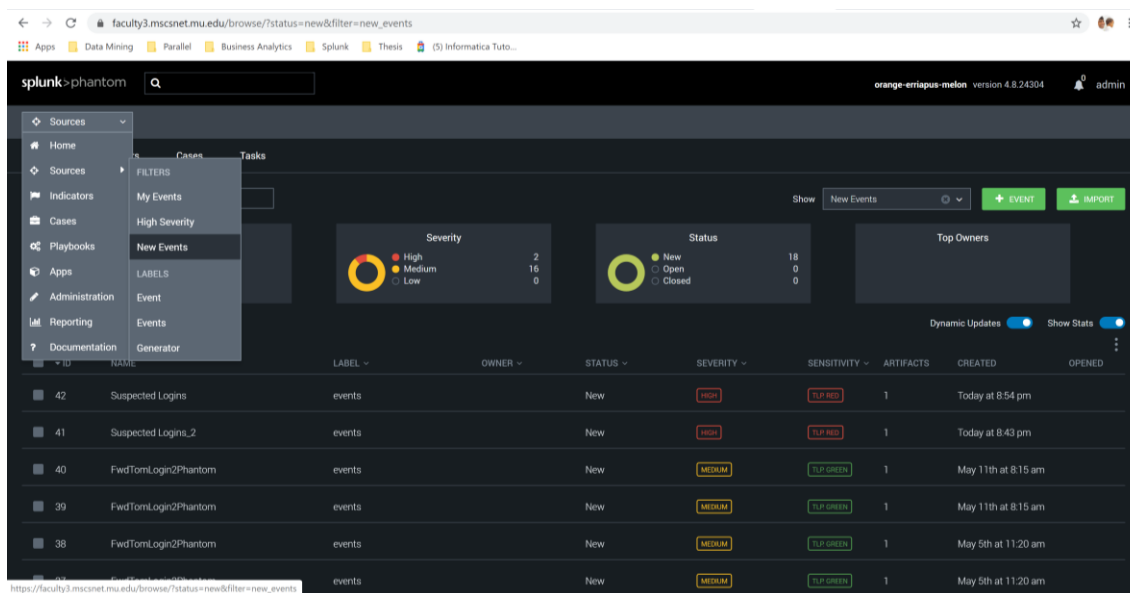


Figure 41. Analyst Alert Dashboard

The SOC analyst will then check the Event ID being worked on and then click the play book button.

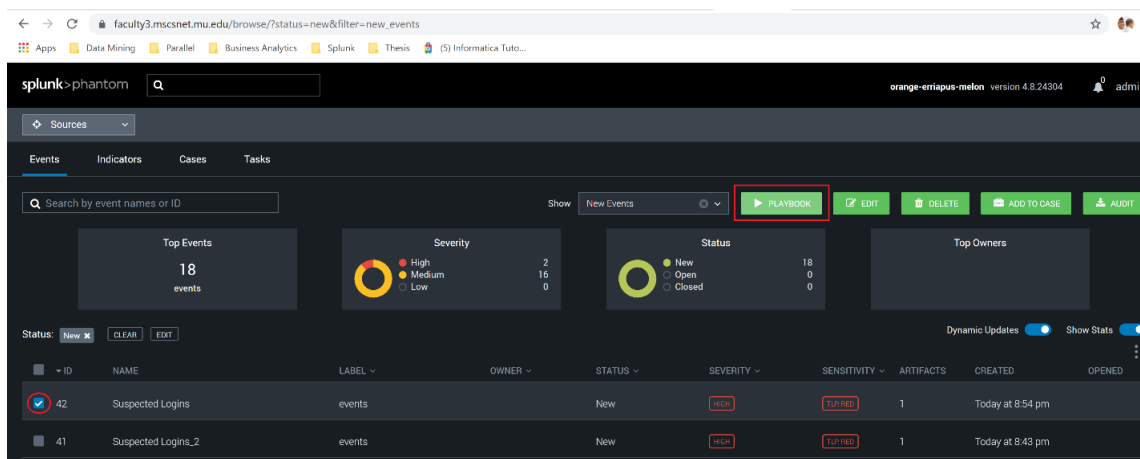


Figure 42. Event ID Checking

Next, Splunk Phantom will display the list of playbooks available for the execution. A quick search will narrow down the search to desired playbook.

The SOC analyst can then select on the desired playbook to be executed and click on “Run Playbook” button.

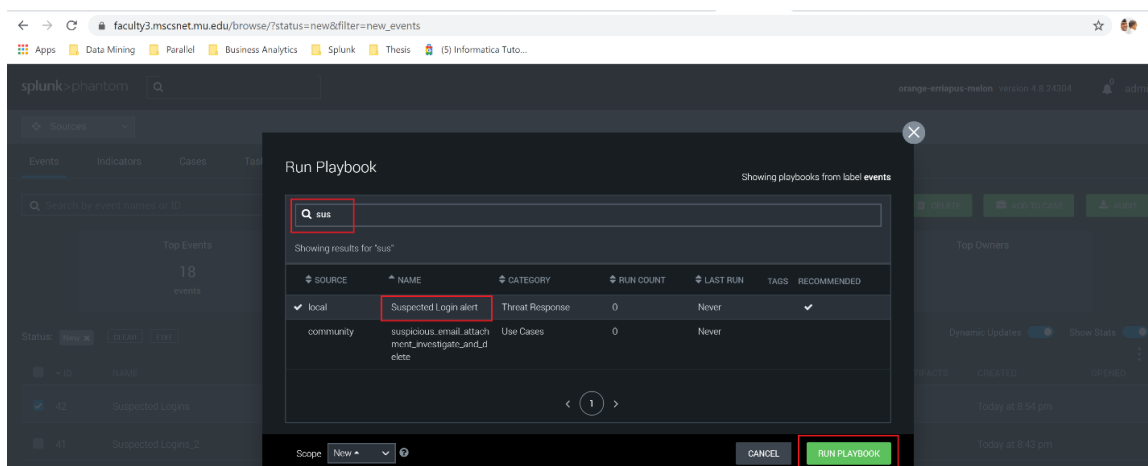


Figure 43. Run the Playbook

The below shown Figure 44 shows the screen shot from alert which was sent to mailbox.

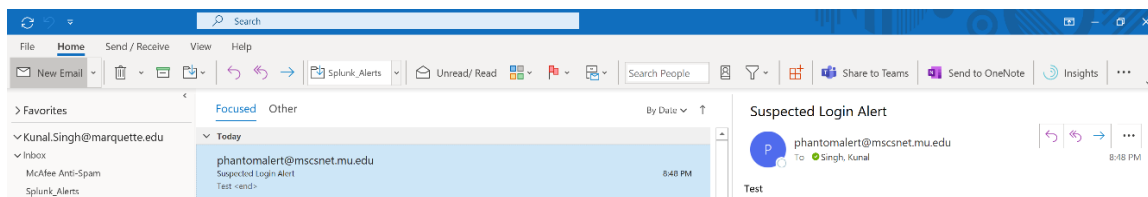


Figure 44. Email Alert

RESULTS

The Lab servers are not protected by enterprise firewalls and at the time of this experiment we did not have access to firewall or network logs. We conducted our experiment with system logs from the virtual machine. We installed Splunk forwarder on each of the student machines to collect the auth log, system log etc.

We applied these SUSS concepts to lab where students are tasked to perform a set of assignments and while students perform the assignments, server will be monitored for any abnormal activity on the servers via SIEM and UBEA. As students will progress through the semester and they would work through their assignments the corresponding logs will be captured into Splunk enterprise via Splunk forwarder. Each assignment would change the way the server is being used and based on these captured log historical data our machine learning would learn and generate alerts in case of abnormal behavior. Issued alerts will be analyzed manually first and if they happen to be real threats, the remediation/proactive action plan would be established. Once we have an established and approved plan in place then it can be automated via Splunk Phantom (SOAR).

As part of our semester long experiment we had installed Splunk forwarder on several virtual machines and log forwarding as setup via Splunk Universal Forwarder. MSCS 6560 class students were tasked to work on set of assignments during lab sessions. While, students performed assignments during semester long project, their machines forwarded logs to Splunk Enterprise. Splunk ML created suspicious login alerts based on the collected logs.

In our experiment, we narrowed down to work on ‘T113-External Remote Services’ TTPs [15] from MITTRE ATTACK framework. To detect any incoming attacks via an external remote service, we forwarded login audit logs from the virtual machines to Splunk enterprise. While analyzing audit logs via SPL (Splunk processing language) we discovered that a brute force attack was being attempted on our servers. We leveraged Splunk to send alerts of every unsuccessful login was attempted on our servers. We created a scheduled report for every 24hours for the failed logins and sent it to our email addresses. Figure 45 and Figure 46 are the screenshots from the emails we received via automated alerts.

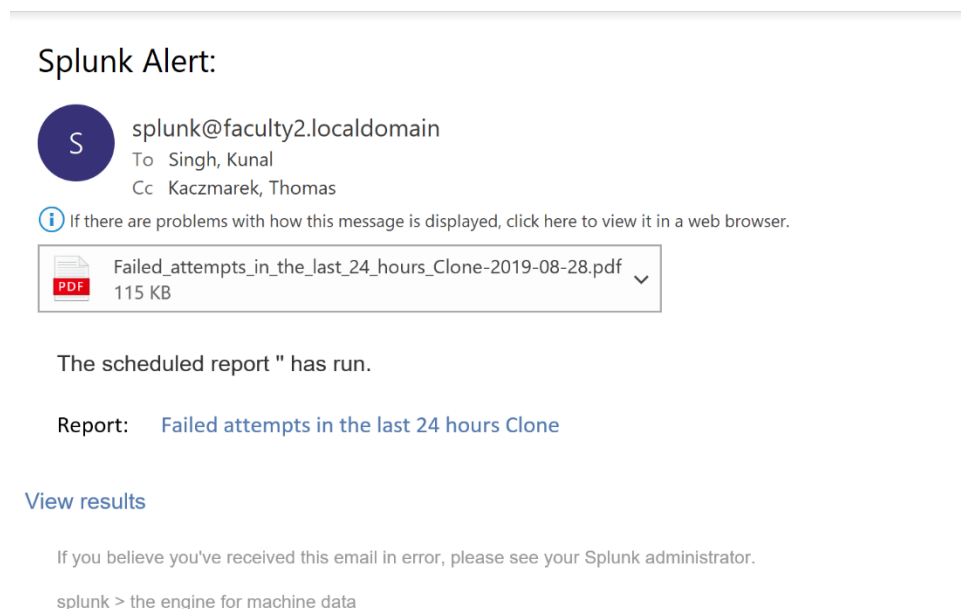


Figure 45. Splunk Enterprise Alert

Failed attempts in the last 24 hours Clone

Failed login attempts in last 24 hours

Time	Event
2019-08-28T19:44:56-0500	Aug 29 00:44:56 vm-0 sshd[15809]: Failed password for root from 218.92.0.168 port 61052 ssh2
2019-08-28T19:44:51-0500	Aug 29 00:44:51 vm-0 sshd[15807]: message repeated 5 times: [Failed password for root from 218.92.0.168 port 38001 ssh2]
2019-08-28T19:44:38-0500	Aug 29 00:44:38 vm-0 sshd[15807]: Failed password for root from 218.92.0.168 port 38001 ssh2
2019-08-28T19:44:32-0500	Aug 29 00:44:32 vm-0 sshd[15797]: Failed password for root from 218.92.0.168 port 15013 ssh2
2019-08-28T19:44:32-0500	Aug 29 00:44:32 vm-0 sshd[15805]: Failed password for invalid user ami from 103.249.100.12 port 34818 ssh2
2019-08-28T19:44:30-0500	Aug 29 00:44:30 vm-0 sshd[15797]: Failed password for root from 218.92.0.168 port 15013 ssh2
2019-08-28T19:44:29-0500	Aug 29 00:44:29 vm-0 sshd[15803]: Failed password for invalid user sales from 128.199.196.155 port 59370 ssh2
2019-08-28T19:44:27-0500	Aug 29 00:44:27 vm-0 sshd[15797]: Failed password for root from 218.92.0.168 port 15013 ssh2
2019-08-28T19:44:27-0500	Aug 29 00:44:27 vm-0 sshd[15800]: Failed password for invalid user tester from 125.130.142.12 port 60394 ssh2
2019-08-28T19:44:25-0500	Aug 29 00:44:25 vm-0 sshd[15797]: message repeated 2 times: [Failed password for root from 218.92.0.168 port 15013 ssh2]
2019-08-28T19:44:19-0500	Aug 29 00:44:19 vm-0 sshd[15797]: Failed password for root from 218.92.0.168 port 15013 ssh2
2019-08-28T19:44:15-0500	Aug 29 00:44:15 vm-0 sshd[15795]: Failed password for invalid user nginx from 106.13.142.247 port 58960 ssh2
2019-08-28T19:44:14-0500	Aug 29 00:44:14 vm-0 sshd[15793]: Failed password for root from 218.92.0.168 port 56278 ssh2
2019-08-28T19:44:11-0500	Aug 29 00:44:11 vm-0 sshd[15793]: message repeated 4 times: [Failed password for root from 218.92.0.168 port 56278 ssh2]
2019-08-28T19:44:01-0500	Aug 29 00:44:01 vm-0 sshd[15793]: Failed password for root from 218.92.0.168 port 56278 ssh2
2019-08-28T19:43:56-0500	Aug 29 00:43:56 vm-0 sshd[15791]: Failed password for invalid user emilia from 171.244.0.81 port 51195 ssh2
2019-08-28T19:43:56-0500	Aug 29 00:43:56 vm-0 sshd[15786]: Failed password for root from 218.92.0.168 port 31810 ssh2
2019-08-28T19:43:53-0500	Aug 29 00:43:53 vm-0 sshd[15786]: message repeated 2 times: [Failed password for root from 218.92.0.168 port 31810 ssh2]
2019-08-28T19:43:47-0500	Aug 29 00:43:47 vm-0 sshd[15786]: Failed password for root from 218.92.0.168 port 31810 ssh2
2019-08-28T19:43:47-0500	Aug 29 00:43:47 vm-0 sshd[15789]: Failed password for invalid user admin from 165.227.49.242 port 59216 ssh2
2019-08-28T19:43:45-0500	Aug 29 00:43:45 vm-0 sshd[15785]: Failed password for root from 112.85.42.188 port 30459 ssh2
2019-08-28T19:43:44-0500	Aug 29 00:43:44 vm-0 sshd[15786]: Failed password for root from 218.92.0.168 port 31810 ssh2

Figure 46. Failed Attempts Display

Next, we built a Machine learning model (UEBA) to automatically detect unusual behavior on the servers. Splunk has variety of apps which can provide UEBA capabilities, but we worked with “Splunk machine learning toolkit” to perform our experiment. We used SPL to preprocess the logs data. Figure 47 shows the SPL used for preprocessing of the data. By using the SPL table command, we could select the required columns for our regression experiment.

res	acct	date_hour	date_mday	terminal	type
failed	28696f76615c964207573657229	16	12	terminal-sshd	USER_LOGIN
failed	postgres	16	12	terminal-sshd	USER_AUTH
failed	28696f76615c964207573657229	16	12	terminal-sshd	USER_LOGIN
failed	28750e686e5f776e207573657229	16	12	terminal-sshd	USER_LOGIN
failed	28696f76615c964207573657229	16	12	terminal-sshd	USER_LOGIN
failed	test	16	12	terminal-sshd	USER_AUTH

Figure 47. SPL Login results

Logistic regression was run using Splunk machine learning toolkit on the pre-processed data to predict the next login possibility on the servers. Below shown Figure 6 shows the results from Logistic regression.

Our Logistic regression model was able to predict 100% TP (true positive or Sensitivity or Recall) unsuccessful login and 99.7 % of TN (true negative or specificity) successful logins. Precision is, what proportion success prediction were correct. In our case, it looked like the model was able to predict 99.7% correct.

Figure 6: Logistic regression results

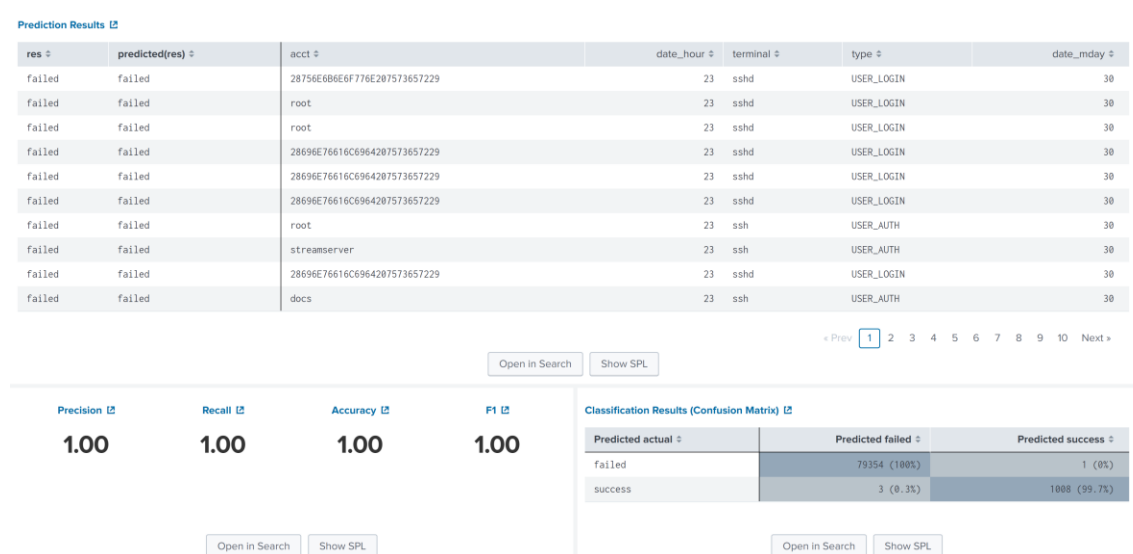


Figure 48. Splunk ML Results

We applied this regression model to our incoming rows and any possible mismatch in prediction with actual result was sent to Splunk phantom for further investigation. We were interested in the false negative because we wanted to investigate

the logins which were predicted failed but logged in successfully into the server. The set of suspected alerts were then sent to Splunk Phantom for further investigation and remediation. Within Splunk phantom we created a custom playbook which would send email to desired mailing list to alert them. Below figure shows the sample playbook creation.

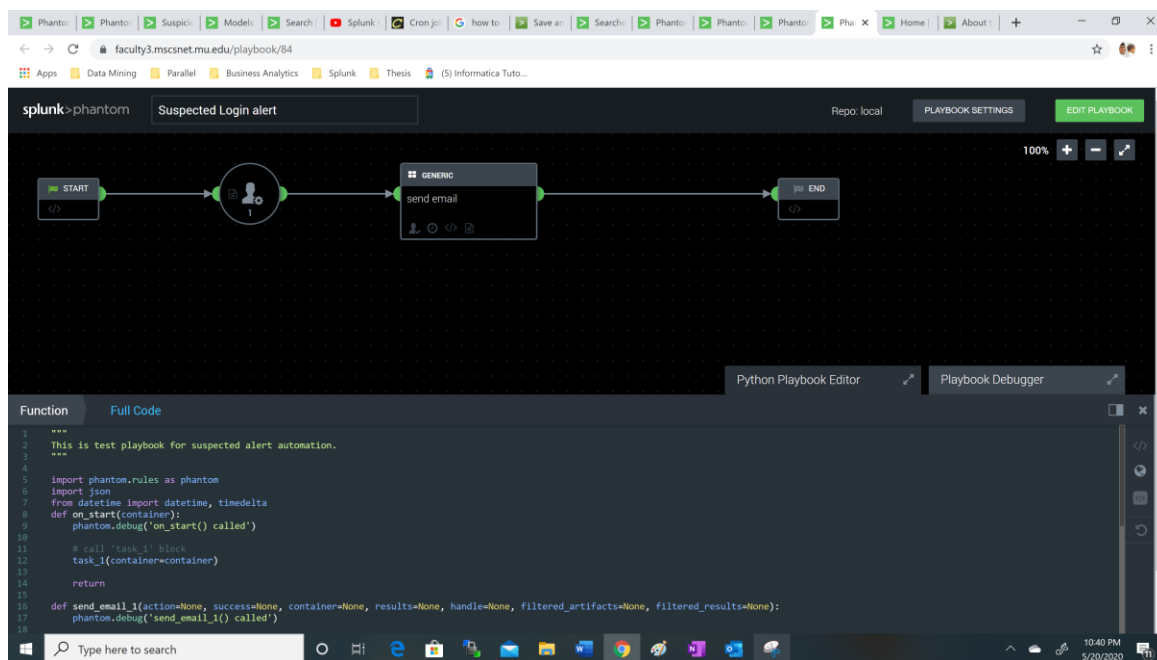


Figure 49. Splunk Phantom Playbook

Below is the email which was received from Splunk phantom in case of an abnormal behavior.

CONCLUSION

The intent of this thesis was to prove the feasibility of Cyber-SUSS implementation on lab computers using commercial tools. Our appreciation for Cyber-SUSS implementation was not realized until we discovered the ongoing brute force attack on MSCS 650 lab computers. Using Splunk SIEM we were able to setup alerting and reporting of the cyber-attacks.

Our countless hours of work were able to demonstrate that Machine Learning Algorithms can detect anomalies for lab environment servers. We were impressed with the Splunk machine learning Logistic regression algorithm's accurate predictions. Splunk processing language was made easy to create an alert report of the abnormal logins on the servers which was forwarded to Splunk Phantom for investigation and remediation. Suspected login alerts were processed by Splunk phantom where an investigation/remediation playbook was executed. Splunk phantom playbooks were simple to create, thanks to the simple and intuitive graphical workflow created.

Our first Auditd log experiment with Splunk machine learning model corresponds to MITRE ATT&CK's 'T113-External Remote Services' [22] advisories. We used this as our first use case for our experiment and we successfully generated automated alerts for the unsuccessful attempts on the server. We were successfully able to send alerts of any abnormal behavior based on machine learning algorithm analysis and launched an automated remediation plan.

Based on our work, we can confirm that Cyber-SUSS solution is ready and can be expanded to other MU IT infrastructure to improve Cyber defense capabilities.

FUTURE WORK

This thesis was focused on proving the feasibility that Cyber-SUSS can be implemented on lab computers. In this process, we were successfully able to setup a SIEM for the lab computers and created Splunk Machine learning models with auditd log data. We also completed the Splunk phantom setup and demonstrated that we can send an automated response with the Splunk Phantom. Here are few recommendations for the future work.

- Splunk Phantom to be configured to grant elevated access to the servers so that it can deploy preventive measures like shutting down the server or isolating the sever from the network.
- Ingest log data from other university devices like routers, firewall, VM ware logs, application logs etc. and continue to build UBEA and SOAR capabilities.
- Collect network and firewall logs which could give insight to the communication being sent and received to the lab computers.
- As we add each type to log, we must consider building use case for each type and complete the cycle of UEBA and SOAR implementation as well. Each use cases could be derived from the MITTRE ATT&CK guidelines.
- Our next used cases could be ‘T1078-Valid Accounts’ [23], where we can check for valid accounts which are being attempted to exploit. So, we could relate MITTRE ATT&CK TTP advisories matrix with our assignment logs and build a threat response playbook accordingly.

- Splunk Enterprise UEBA can be used to design our machine learning model for each of the collected logs. Detected anomalies from Splunk machine learning will then be sent to Splunk phantom for mitigation alerts which will can be automated via Splunk phantom playbooks.
- Complete the cycle of Cyber SUSS implantation by creating SIEM (logs collection), UEBA (Machine learning), SOAR (automated response) for each of the use cases.
- Considering collecting logs /var/log/dmesg to monitor and remediate any usb connected devices.

Bibliography

- [1] "Cybercrime Magazine," 16 May 2019. [Online]. Available: <https://cybersecurityventures.com/cybersecurity-market-report/>.
- [2] "Ebrary," [Online]. Available: https://ebrary.net/26722/computer_science/detection_work.
- [3] "Firewall (computing)," 08 May 2020. [Online]. Available: [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing)).
- [4] "Whitepaper: Compare AlienVault USM with the Traditional SIEM," 2018. [Online]. Available: <https://learn.alienvault.com/c/usm-vs-siem-alien-va?x=M6R9kL>.
- [5] T. Lewis, "IDS and IPS 101: How Each System Works and Why You Need Them," 3 Aug 2019. [Online]. Available: <https://www.lbmc.com/blog/ids-vs-ips/>.
- [6] J. Stoltzfus, "What's the difference between SEM, SIM and SIEM?," [Online]. Available: <https://www.techopedia.com/7/31201/security/whats-the-difference-between-sem-sim-and-siem>.
- [7] "techtarget," techtarget, [Online]. Available: <https://searchsecurity.techtarget.com/definition/HIDS-NIDS>.
- [8] "comparitech," comparitech, 25 April 2020. [Online]. Available: <https://www.comparitech.com/net-admin/network-intrusion-detection-tools/>.
- [9] "What Is a Security Operations Center (SOC)?: Security," 2019. [Online]. Available: https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html.
- [10] C. Zimmerman, "pr-13-1028-mitre-10-strategies-cyber-ops-center," 2014. [Online]. Available: <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>.
- [11] "SOC," 07 Oct 2017. [Online]. Available: <https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html>.
- [12] "What Is a SOC?: Security," 2019. [Online]. Available: https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html.

- [13] S. Bhatt, P. K. Manadhata and L. Zomlot, "The Operational Role of Security Information and Event Management Systems - IEEE Journals & Magazine," 15 Oct 2014. [Online]. Available: <https://ieeexplore.ieee.org/document/6924640>.
- [14] "Building A SOC with Splunk," 2019. [Online]. Available: https://www.splunk.com/en_us/cyber-security/security-operations-automation/building-a-soc-with-splunk.html.
- [15] "User and Entity Behavior Analytics (UEBA)," 2020. [Online]. Available: <https://www.exabeam.com/siem-guide/ueba/>.
- [16] "4 reasons to add user behavior analytics to your SIEM," 21 Mar 2019. [Online]. Available: https://media.bitpipe.com/io_14x/io_146636/item_1892951/4-reasons-to-add-uba-to-your-siem.pdf.
- [17] M. A. B. S. N. CHADNI ISLAM, "A Multi-Vocal Review of Security Orchestration," Apr 2019. [Online]. Available: <https://dl.acm.org/doi/pdf/10.1145/3305268>.
- [18] L. Lubeck, "What is MITRE ATT&CK and how is it useful?," 03 Sep 2019. [Online]. Available: <https://www.welivesecurity.com/2019/09/03/what-is-mitre-attck-useful/>.
- [19] C. BROOK, "What is the MITRE ATT&CK Framework?," 23 Apr 2020. [Online]. Available: <https://digitalguardian.com/blog/what-mitre-attck-framework>.
- [20] T. MATTHEWS, "What is MITRE ATT&CK: An Explainer," 30 July 2019. [Online]. Available: <https://www.exabeam.com/information-security/what-is-mitre-attck-an-explainer/>.
- [21] "splunk.com," Splunk, 2020. [Online]. Available: https://www.splunk.com/en_us/software/splunk-security-orchestration-and-automation/features.html.
- [22] "businesswire.com," businesswire, 05 Sep 2017. [Online]. Available: <https://www.businesswire.com/news/home/20170905005121/en/Phantom-Security-Automation-Orchestration-Platform-Reduces-MTTR>.
- [23] "Splunk.com," 24 Jan 2020. [Online]. Available: <https://docs.splunk.com/Documentation/Phantom/4.8/User/MC>.

- [24] "Splunk," 2020. [Online]. Available:
<https://docs.splunk.com/Documentation/PhantomApp/latest/Install/ConfigurePhantomServer>.
- [25] "LogRhythm_sSecurity," 07 Feb 2018. [Online]. Available:
https://media.bitpipe.com/io_14x/io_141436/item_1668091/LogRhythm_sSecurity_IO%23141436_Eguide_021518_LI%231668091.pdf.
- [26] T. B. G. S. Kelly Kavanagh, "Magic Quadrant for Security Information and Event Management," 18 Feb 2020. [Online]. Available:
<https://www.gartner.com/doc/reprints?id=1-1YE69EYM&ct=200218&st=sb>.
- [27] Splunk, "Splunk," Splunk, 2020. [Online]. Available:
<https://docs.splunk.com/Documentation/PhantomApp/latest/Install/ConfigurePhantomServer>.