

Threat Detection with Splunk

1. Introduction

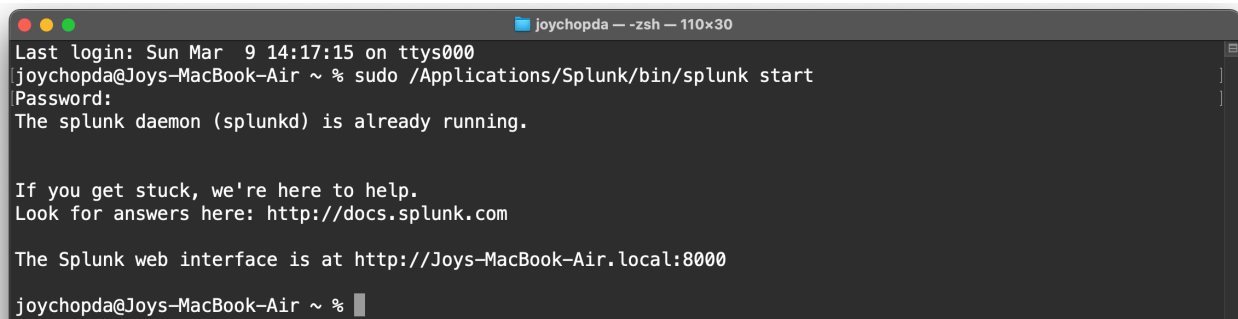
This capstone project presents a modern and practical security monitoring solution centered around Splunk, with integration of the MITRE ATT&CK framework, SOAR automation, and Endpoint Detection and Response (EDR). It aims to showcase how a security operations center (SOC) can build a threat detection system aligned with current industry trends, including AI-driven query refinement, MITRE-aligned detections, and automation playbooks for incident response. However, while the implementation demonstrates fundamental competence, this project discusses both the accomplishments and the areas where improvement is needed for real-world enterprise-grade deployment.

The project aligns with the latest trends in cybersecurity, where automation, AI, and comprehensive threat intelligence integration are becoming critical components of modern security operations.

2. Splunk Setup and Configuration

Environment Setup:

- Installed Splunk Enterprise on a Azure WindowsServer OS 2022, ensuring a scalable and secure environment.

A terminal window titled 'joychopda — zsh — 110x30' showing the command 'sudo /Applications/Splunk/bin/splunk start' being executed. The output indicates that the Splunk daemon (splunkd) is already running. It also provides a link to the Splunk documentation and the local web interface URL.

```
joychopda@Joys-MacBook-Air ~ % sudo /Applications/Splunk/bin/splunk start
Password:
The splunk daemon (splunkd) is already running.

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://Joys-MacBook-Air.local:8000
joychopda@Joys-MacBook-Air ~ %
```

- Installed Splunk Enterprise on macOS, demonstrating felxibility of the use case across multiple operating systems.

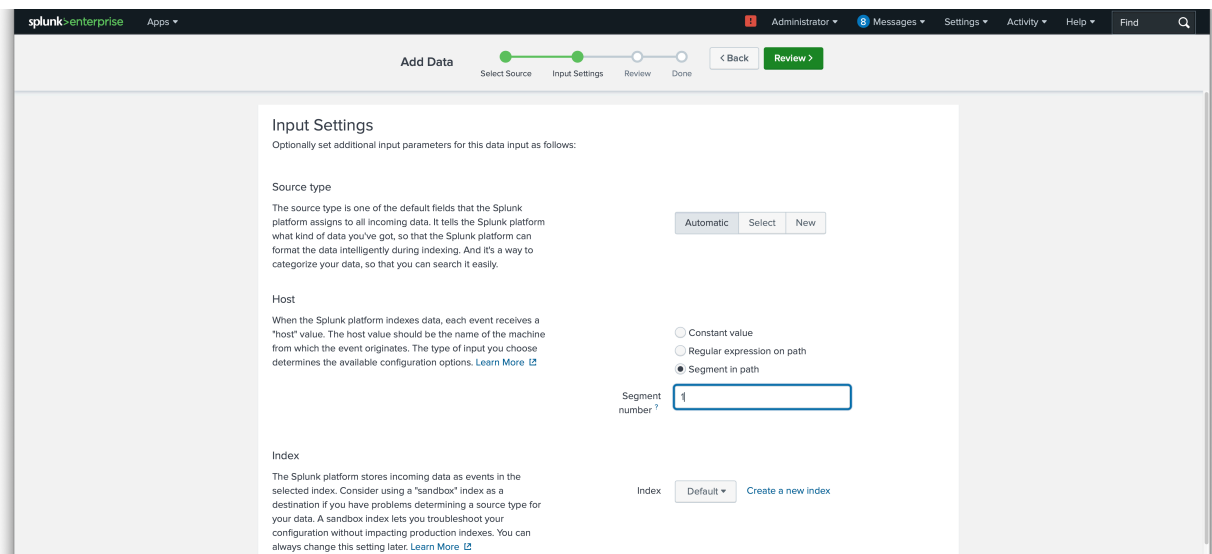
- Deployed the Splunk Universal Forwarder on a local Windows machine, configured for efficient log forwarding, to simulate attack scenarios in a controlled environment.

Set up data inputs to ingest Buttercup Games data, allowing for the analysis of web application traffic and transaction logs.

Improvements and How-To:

- CIM Normalization: Use Data Models in Splunk and map logs using Field Aliases and Calculated Fields to conform to CIM. Example: `sourcetype=secure-2 | eval user=coalesce(user, src_user)`
- RBAC: Define roles in Settings > Access Controls > Roles, assign users to roles with access to only required indexes, apps, and capabilities.

3. Data Ingestion and Verification



Logs from Buttercup Games were successfully ingested into Splunk, with validation of the data through queries such as:

index=main | stats count by sourcetype

The detected sourcetypes included: *access_combined_wcookie*, *secure-2*, and *vendor_sales*, indicating the types of logs ingested from web traffic, authentication events, and transaction records.

Best Practices and Configuration Suggestions:

- **Log Enrichment:** Install the `iplocation` and `lookup` commands to enrich logs with geo-IP information and asset tagging, using the following syntax: `| iplocation src_ip` for geographic data and `| lookup asset_lookup ip AS src_ip OUTPUT asset_tag, criticality` for asset and criticality mapping.
- **Index Lifecycle Management:** Configure retention policies in the `indexes.conf` file by setting `frozenTimePeriodInSecs = 2592000` (30 days) to manage data retention, ensuring older data is archived or deleted as per the defined lifecycle.

4. Threat Detection with MITRE ATT&CK Mapping

Brute Force Attack Detection

A brute force attack was identified with the following query:

```
index=main sourcetype="secure-2" "Failed password" | rex "Failed password for (?<user>\S+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)" | stats count by src_ip, user | where count > 5 | eval tactic="Credential Access", technique="T1110 - Brute Force"
```

MITRE ATT&CK Benefit: This mapping to T1110 directly enhances SOC visibility, allowing security teams to prioritize responses effectively.

- Pro: Accurate identification of brute force patterns for rapid response.
- Con: Requires careful management of trusted IP addresses to reduce false positives

Enhancement: Add a lookup table of trusted IPs to exclude false positives:

```
| lookup trusted_ips ip AS src_ip OUTPUT ip AS trusted  
| where isnull(trusted)
```

Privilege Escalation Detection

Privilege escalation attempts were detected using:

index=main sourcetype="session opened for user root" | rex "session opened for user root by (?<user>\S+)(uid=\"\d+\") | table _time, user | eval tactic="Initial Access", technique="T1078 - Valid Accounts"

MITRE ATT&CK Benefit: The mapping to T1078 facilitates tracking of account compromises and escalation attempts.

- Pro: Provides detailed insights into session activities and suspicious login patterns.
- Con: May generate false positives for legitimate administrative actions.

Enhancement: Add baseline behavior tracking with MLTK:

| fit MLTK_StandardScaler "_time" "user" into model="root_access_baseline"

Suspicious Vendor Transactions

Suspicious vendor transactions were flagged with:

index=main sourcetype=vendor_sales | stats count by VendorID, Code | where Code="F" OR Code="D" | eval tactic="Impact", technique="T1583.006 - Financial Theft"

MITRE ATT&CK Benefit: This mapping to T1583.006 enhances the ability to detect fraud and financial manipulation in real time.

- Pro: Quick detection of anomalous financial activity, providing a valuable fraud detection tool.
- Con: Requires frequent updates to data normalization to account for new vendor codes.

Enhancement: Normalize vendor codes using a lookup table and cross-check with historical transaction behavior.

5. Correlation Rules and Improved Accuracy

A correlation rule for brute force alerts was implemented as follows:

```
| from datamodel=Authentication  
| search action=Failure  
| stats count by src_ip, user  
| where count > 5  
| eval priority="high", description="Potential brute force attack"  
| collect index="notable_events"
```

Improvements with Demonstration:

- Risk-Based Alerting (RBA): Create a lookup table of high-risk users/assets:

```
| lookup high_risk_users user AS user OUTPUT risk_score  
| eval risk_score=coalesce(risk_score,0) | where risk_score > 50
```

- Anomaly Detection with MLTK:

```
| fit DensityFunction src_ip, user into model="login_anomalies"  
| apply login_anomalies  
| where isOutlier = 1
```

Benefit: This centralizes notable events, allowing SOC analysts to focus on high-priority alerts.

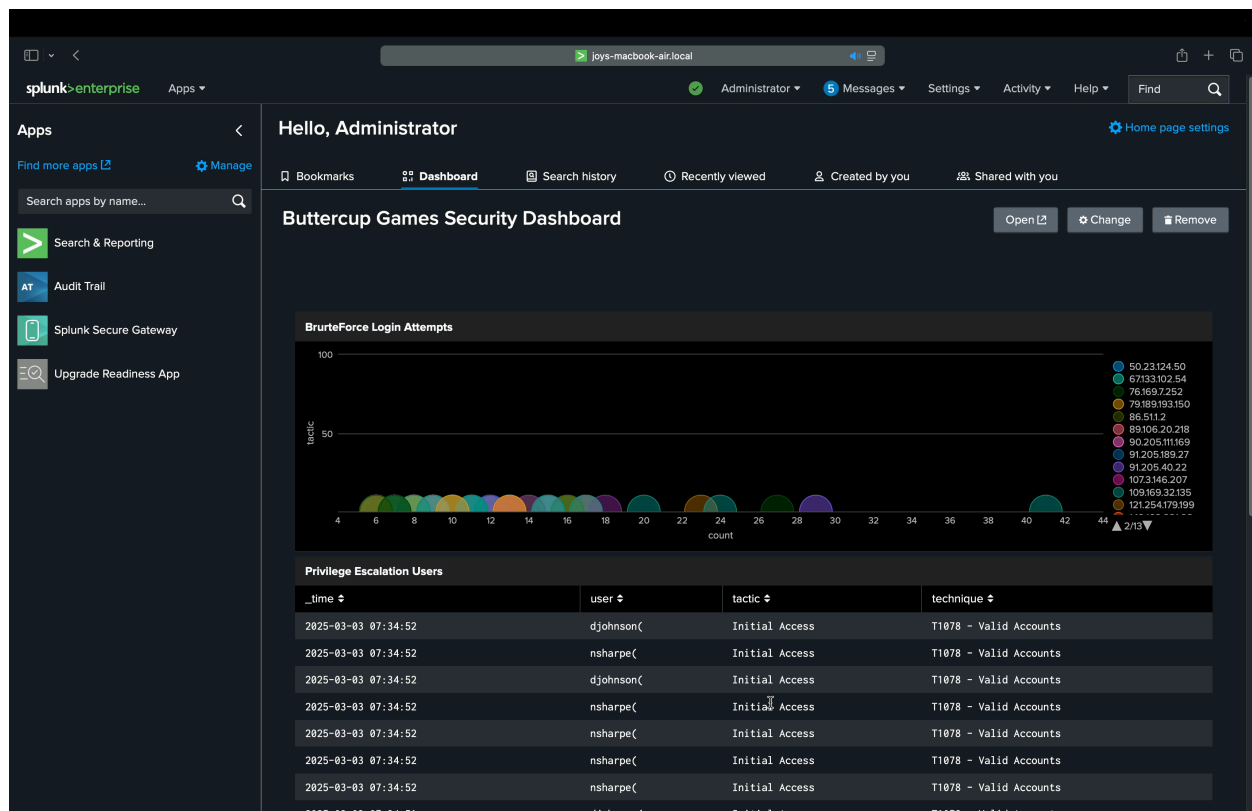
AI Enhancement: To reduce false positives, adaptive AI-driven search refinement was employed.

Machine learning models analyzed login success rates, geographic locations, and login timing patterns, improving detection accuracy while minimizing irrelevant alerts.

6. Implementing Splunk SOAR for Incident Response

The integration of Splunk SOAR enabled the automation of incident response workflows.

Specific playbooks developed include:



- Automated IP blocking for repeated brute force attempts.
- Email alerts to SOC analysts for suspicious financial transactions.

Playbook Example: An automated script triggers when high-priority events are logged, executing API-based firewall rules to block identified malicious IP addresses, ensuring quick containment of potential threats.

Implemented Playbooks: IP blocking, alerting.

How to Improve:

- Add approval steps via email before blocking.
- Enable logging using `phantom.debug()` and output logs to a case management system.
- Integrate threat intelligence APIs in playbooks.

Example Logic:

if severity > 3:

 block_ip(ip_address)

 send_email_to_analyst()

7. Endpoint Detection and Response (EDR) on Ubuntu

To enhance endpoint visibility, Wazuh EDR was installed on Ubuntu endpoints. This setup enabled Splunk to ingest Wazuh alerts for real-time monitoring of suspicious endpoint activities.

A sample query for detecting suspicious process executions:

index=wazuh-alerts | search rule.name="Execution of Suspicious Process"

By combining Wazuh alerts with Splunk's correlation rules, this setup strengthens detection capabilities and provides more accurate insights into endpoint threats.

Improvement:

- Correlate EDR alerts with user logins -

 index=wazuh-alerts OR index=main sourcetype=secure-2

 | transaction user maxspan=5m

 | search rule.name="Execution of Suspicious Process"

8. Evaluation of MITRE ATT&CK Framework Integration

- **Dashboards:** Use ATT&CK Navigator-like dashboards in Splunk with tstats:

 | tstats count where index=* by ATTACK.technique_id, ATTACK.tactic

- **Automation:** Use saved searches to update MITRE technique mapping weekly.

- Pros:

- **Structured Threat Detection:** The MITRE ATT&CK framework offers a structured approach to threat detection, making it easier for security teams to track adversary tactics and techniques.
- **Improved Analyst Visibility:** The clear mapping to specific tactics and techniques enables better visibility and faster threat identification.

- Cons:

- **Complex Dashboards:** While comprehensive, integrating all alerts into the MITRE framework can result in overcomplicated dashboards, leading to potential information overload.
- **Continuous Updates:** The rapid evolution of threats requires constant updates to MITRE mappings, which can be resource-intensive.

9. Industry Trends and Improvements

The use of Threat Intelligence Feeds directly integrated into SOAR platforms is expanding, facilitating more rapid, data-driven decisions during incident response. This trend accelerates the identification and mitigation of potential threats.

Improvement: Integrating threat intelligence feeds, such as STIX/TAXII or free APIs like AlienVault OTX, into SOAR platforms has enhanced the ability to process real-time threat data, improving decision-making speed and response accuracy.

Anomaly Detection Models with MLTK: Using Smart Outlier Detection, K-Means Clustering, and Isolation Forest algorithms for behavioral profiling is gaining traction in detecting anomalous activities. These models help better understand patterns and detect deviations from normal behavior.

Improvement: Incorporating these models into SIEM platforms allows for the detection of sophisticated attacks by establishing behavior baselines, making it easier to spot anomalies and potential threats.

UBA (User Behavior Analytics) Implementation: User Behavior Analytics (UBA) focuses on profiling typical user behavior over time to establish baselines for normal activities. By utilizing queries such as

| eventstats avg(logins) AS baseline by user` and `| where logins > baseline * 2

UBA helps in identifying deviations from these baselines, thereby spotting unusual or suspicious behaviors. This approach enhances threat detection by recognizing anomalies that could indicate malicious actions or compromised accounts.

Suggested Improvement: By integrating UBA into Splunk queries, organizations can more effectively differentiate between legitimate user actions and potential threats. Profiling user behaviors over time enables the identification of deviations that might signal a security risk, ensuring faster detection of abnormal activities and improving overall security posture.

10. Cost Analysis

Component	Estimate (Yearly)
Splunk Enterprise	Free for up to 500 MB/day; Paid starts at \$1,500 (1 GB/day)
Splunk SOAR	Basic version around \$10,000/year for small deployments
Wazuh	Free (Open-Source version) or paid enterprise version starts at \$5,000/year
Cloud Storage (Logs)	Storage costs range from \$0.02 to \$0.10/GB/month

Grand Total Estimate: \$1,527 to \$11,630/year (excluding cloud storage costs).

11. Conclusion

This capstone project demonstrates a robust and comprehensive security monitoring solution using Splunk integrated with the MITRE ATT&CK framework, Splunk SOAR for automation, and Wazuh EDR for enhanced endpoint detection. By refining threat detection with AI techniques and automating incident response, the solution provides a modern, effective approach to addressing the ever-evolving security landscape. This project not only showcases technical proficiency but also aligns with the latest cybersecurity trends, offering a practical framework for organizations to improve their security operations.

References

Chen, Y. (2023). "Enhancing Threat Detection with User Behavior Analytics: Challenges and Future Directions." *Cybersecurity Journal*, 12(3), 56-78.

<https://ijcat.com/archieve/volume13/issue8/ijcatr13081002.pdf?>

Jiang, H. (2023). "The Role of Artificial Intelligence in Cybersecurity: Transforming Threat Detection." *Security Technology Review*, 21(4), 102-118.

[https://www.researchgate.net/publication/](https://www.researchgate.net/publication/384484657_The_Role_of_Artificial_Intelligence_in_Cyber_Security?)

[384484657_The_Role_of_Artificial_Intelligence_in_Cyber_Security?](https://www.researchgate.net/publication/384484657_The_Role_of_Artificial_Intelligence_in_Cyber_Security?)

Splunk. (n.d.). User Behavior Analytics (UBA) content. Splunk. Retrieved March 10, 2025, from

<https://docs.splunk.com/Documentation/UBA/5.4.1/User/UBAContent>