SOC & Automation Report

Introduction

The selected Indicator of Compromise (IOC) for this simulation is a known malicious IP address (45.55.45.24) identified through the AlienVault OTX platform. This IP has been flagged in multiple threat intelligence sources due to its involvement in malicious activities such as distributing malware and conducting unauthorized access attempts on vulnerable systems.

Key Characteristics

The IOC is primarily associated with malware distribution and attempts to exploit vulnerabilities in various systems. It represents a significant threat to organizational security, particularly by targeting unpatched systems through malicious network traffic. The IP address is notable for its consistent appearance in threat reports, demonstrating its involvement in coordinated attacks. Blocking communication with this IP is critical to mitigating potential threats.

Setting up Wazuh and Creating a Rule

Installation and Configuration

Wazuh was installed and configured in a virtual machine (VM) environment provided by the assignment template. The steps involved setting up the Wazuh manager and agent in a virtualized environment. The Wazuh dashboard was accessed via a web browser using the virtual machine's IP address(https://192.168.64.4/app/login?). Basic settings, such as network interfaces and security configurations, were established to ensure proper monitoring of network activities.

Rule Creation

A custom rule was created in Wazuh to detect any activity related to the malicious IP address (45.55.45.24). The rule was added to the "local_rules.xml" file and configured to trigger whenever this IP appeared in network traffic. The rule specifies:

- **Rule ID**: 100001

- **Level**: 10 (high severity)

- **Condition**: Detect traffic from or to the IP "45.55.45.24"

- **Action:** Trigger an alert when traffic is detected involving the specified IP address.

The Wazuh service was restarted after editing the configuration file to apply the changes.

Shuffler.io Configuration for Automated Response

Integration with Wazuh

Shuffler.io was integrated with Wazuh by creating a webhook in Shuffler.io and adding its URI to the Wazuh "ossec.conf" file. The webhook was configured to trigger whenever an alert related to the identified IOC was generated. Steps taken included:

- Creating a webhook trigger in Shuffler.io to receive alert data from Wazuh.

- Configuring the Wazuh server to forward relevant events (related to rule ID 100001) to Shuffler.io.

- Restarting the Wazuh manager to activate the webhook connection.

Automated Response Setup

In Shuffler.io, a workflow was created to automate the response to the detection of traffic related to the IOC. The workflow was configured to:

- Send an email notification to the SOC team upon detection of the IOC.

- Execute an API call to update the firewall, blocking the malicious IP in future traffic attempts.

- Log the incident in the incident response system for further analysis.

Results and Observations from Threat Simulation

Threat Simulation Scenario

The threat scenario was simulated by manually triggering a connection to the malicious IP (45.55.45.24) using the “curl” command from a terminal within the environment:

```
curl http://45.55.45.24
```

This simulated a legitimate user unknowingly accessing a malicious server.

Detection and Response

Wazuh successfully detected the connection attempt to the malicious IP, triggering an alert based on the custom rule created earlier. The alert was forwarded to Shuffler.io via the configured webhook, which triggered the automated workflow:

- An email alert was sent to the SOC team, detailing the connection attempt.

- The IP address was automatically blocked in the firewall to prevent further malicious traffic.

Observations and Improvements

The overall detection and response worked as expected, with Wazuh detecting the IOC and Shuffler.io responding automatically. However, there were some delays in triggering the firewall update, which could be optimized for faster reaction times. Additionally, the workflow could be enhanced to include more detailed logging and reporting on the actions taken, improving traceability for future incidents.

Conclusion

The simulation successfully demonstrated the integration of threat intelligence (AlienVault OTX), Wazuh), and Shuffler.io to create an automated security response to an identified IOC. Wazuh effectively detected the malicious IP address, and Shuffler.io automated the response, showcasing the value of SOC automation in improving response times and reducing manual intervention.