SOC & Automation Report

1. Overview of the Selected IOC

1.1 Introduction

The selected Indicator of Compromise (IOC) is the IP address 185.220.101.52. This IP is associated with malicious activity, specifically related to anonymization services and potential Command and Control (C2) infrastructure. Monitoring and responding to traffic from this IP address is critical to safeguarding the organization's network from external threats.

1.2 Key Characteristics

- **Type**: IP Address
- **Threat**: The IP is known to be part of the Tor network, often used to anonymize malicious activities. Traffic from this IP could indicate attempts to bypass security controls or communication with a C2 server.
- **Attributes**: High association with malware distribution, phishing, and C2 activities.

2. Setting up Wazuh and Creating a Rule

2.1 Installation and Configuration

- **Wazuh Installation**: Wazuh was installed on a virtual machine using the provided image. The installation included setting up the Wazuh manager and agent, which were configured to communicate over the network.
- **Configuration**: The Wazuh server was configured by accessing it via SSH with the provided credentials. The IP address of the non-loopback interface was determined using the ip a command, and the Wazuh web interface was accessed using this IP.

2.2 Rule Creation

- **Creating a Rule for IOC**: A custom Wazuh rule was created to detect traffic involving the IP address 185.220.101.52. The rule was configured as follows:

```
<group name="alienvault_otx">
  <rule id="100001" level="10">
    <decoded_as>json</decoded_as>
    <field name="data.srcip">185.220.101.52</field>
    <description>Suspicious IP detected from Alienvault OTX IOC:
```

```
185.220.101.52</description>
  </rule>
</group>
```

- **Testing the Rule**: The rule was tested by simulating network traffic from the IP address 185.220.101.52 within the environment. The Wazuh agent successfully detected the IOC and generated an alert.

3. Shuffler.io Configuration for Automated Response

3.1 Integration with Wazuh

- **Account Setup**: A Shuffler.io account was created, and a new workflow was initiated. A webhook trigger was set up in Shuffler.io to receive alerts from Wazuh.
- **Integration**: The Wazuh server configuration (ossec.conf) was edited to include the Shuffle webhook URI. The following configuration was added:

```
<integration>
  <name>custom</name>
  <hook_url>https://shuffler.io/webhook/your-webhook-url</hook_url>
  <alert_format>json</alert_format>
</integration>
```

- **Wazuh Server Restart**: The Wazuh manager service was restarted to apply the configuration changes.

3.2 Automated Response Setup

- **Workflow Configuration**: In Shuffler.io, a complete workflow was created to automatically respond to alerts triggered by the detected IOC. The workflow included steps to isolate the affected machine, notify the SOC team, and update threat intelligence databases.

4. Results and Observations from Threat Simulation

4.1 Threat Simulation Scenario

- **Simulation Setup**: A simulated threat scenario was created by injecting traffic from the IP address 185.220.101.52 into the environment. This involved generating network activity that matched the criteria specified in the Wazuh rule.

4.2 Detection and Response

- **Results**: Wazuh successfully detected the malicious traffic from the IOC, triggering an alert that was forwarded to Shuffler.io. The automated response workflow was activated, isolating the affected endpoint and notifying the SOC team.

4.3 Observations and Improvements

- **Insights**: The integration between Wazuh and Shuffler.io worked seamlessly, allowing for a quick and effective automated response to the detected threat. One potential improvement could be refining the rule to include additional context, such as the nature of the traffic or time of day, to reduce false positives.

5. Conclusion

The integration of Alienvault OTX, Wazuh, and Shuffler.io proved effective in automating the detection and response to IOCs within the environment. The selected IOC, 185.220.101.52, was successfully detected, and the automated workflow in Shuffler.io responded as expected. This process demonstrated the value of SOC automation in enhancing an organization's security posture by reducing response times and improving accuracy.