**Nwachukwu Edumanichukwu**

**Bellevue University**

**CYBR 445 - Advanced Incident Detection and Response  
  
Module 10 Lab – SOAR with Shuffle**

**Professor Chelsie Thompson**

**July 16, 2023**

**What is the benefit of using a SOAR over simply programming workflows or playbooks in a script or program?**

**Using a SOAR offers a major advantage in terms of centralized management, automation, and integration of security tools like SIEM, threat intelligence platforms and EDR systems.**

**Go to** [**https://shuffler.io/search**](https://shuffler.io/search)**. Find three integration applications you find interesting. Describe what they do and how they could be useful.**

**Microsoft 365 Defender – This application coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. It can be useful for investigating a security incident, view logs, events. IT improves visibility, collaboration, reporting and automates responses.**

**Sentinel One – This application helps to monitor endpoints for suspicious activities and threats. It automates responses actions to threat detections that helps the Mean Time to Respond which minimizes the impact of security incidents.**

**Palo Alto firewall – This application helps to provide real-time threat detection and prevention capabilities. It automates response actions when specific threat indicators or events are detected.**

**Paste a screenshot of your Workflow with all nodes and flow lines marked as green.A screenshot of a computer

Description automatically generated**

**Paste a screenshot of your Execution dialog showing a successful execution (note that you don’t have to show all the results of each node.A screenshot of a computer

Description automatically generated**

**Take the result you received from each node (the full JSON and paste them below). It’s okay if your indicator was not found if the node correctly contacted service and show a valid not found response.**

**Virus Total:**

**"Results for VirusTotal\_Domain\_Check":{11 items**

**"scan\_id":"8438093d94c8071acb051034dbabe8012288c969500764f91597a767986d286e-1688524877"**

**"resource":"clcr.me"**

**"url":"http://clcr.me/"**

**"response\_code":1**

**"scan\_date":"2023-07-05 02:41:17"**

**"permalink":"https://www.virustotal.com/gui/url/8438093d94c8071acb051034dbabe8012288c969500764f91597a767986d286e/detection/u-8438093d94c8071acb051034dbabe8012288c969500764f91597a767986d286e-1688524877"**

**"verbose\_msg":"Scan finished, scan information embedded in this object"**

**"filescan\_id":NULL**

**"positives":3**

**"total":90**

**"scans":{...}90 items**

**}**

**URLScan:**

**"Results for URLScan\_Domain\_Check":{4 items**

**"results":[...]100 items**

**"total":600**

**"took":61**

**"has\_more":false**

**}**

**Alienvault OTX:**

**"Results for AlienvaultOTX\_Domain\_Check":{10 items**

**"sections":[...]7 items**

**"whois":"http://whois.domaintools.com/clcr.me"**

**"alexa":"http://www.alexa.com/siteinfo/clcr.me"**

**"indicator":"clcr.me"**

**"type":"domain"**

**"type\_title":"Domain"**

**"validation":[]0 items**

**"base\_indicator":{...}8 items**

**"pulse\_info":{...}4 items**

**"false\_positive":[]0 items**

**}**

**Paste a screenshot of your Email Phishing Compromise workflow below. If your workflow is not legible when pasted in, you can also submit an image file of your workflow as an attachment to your assignment.**

**A screenshot of a computer

Description automatically generated**