Demonstrating the Use of OpenC2 and SOAR

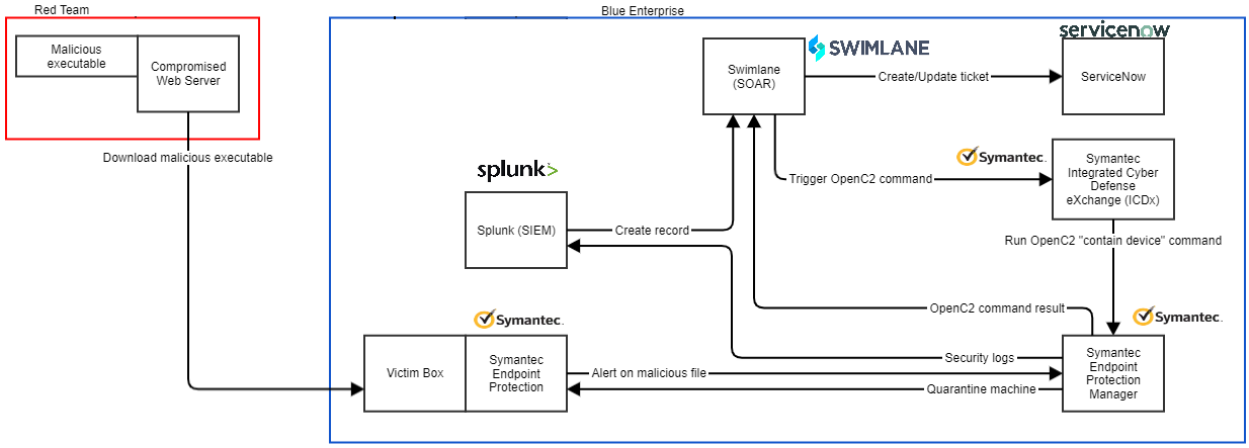
SOAR (Security Orchestration, Automation, and Response) technology enables orchestration and automation of security actions in response to cyber threat intelligence (CTI) and security alerts. SOAR products orchestrate the activity of other security products, such as firewalls and endpoint security clients. Each SOAR product and security product that work together must implement a connector interface using vendor- and product-specific commands.

OpenC2, or Open Command and Control, is a vendor-agnostic machine-to-machine language specification for cybersecurity tools. OpenC2 enables the automation and interoperability of cybersecurity tools, facilitating machine-speed cyber defense (OASIS Open Command and Control (OpenC2) TC, 2019). The OpenC2 standard is maintained by the Organization for the Advancement of Structured Information Standards (OASIS) Technical Committee with participation and support from industry and government organizations around the world. Using OpenC2, organizations can design processes for mitigating threats and share those methods with the security community in precise, machine-readable terms. Because OpenC2 is platform- and product-agnostic, other organizations can apply the mitigations directly to their environments without having to worry about interoperability (OASIS, 2017).

The Integrated Adaptive Cyber Defense (IACD) initiative demonstrated the use of OpenC2 and SOAR technology together during a threat feed experiment and proof-of-concept demonstration. In the experiment, the IACD team created a virtual enterprise, called the Blue Enterprise, that included the following technologies:

- Splunk Security Information and Event Management (SIEM)
- Symantec Endpoint Protection client security and management software
- ServiceNow service ticket management
- Swimlane SOAR product for security orchestration and automation

The experiment scenario involved a user in the Blue Enterprise accidentally downloading malicious software from a compromised web server owned by a Red adversary, as depicted in the figure below.



When the Symantec Endpoint Protection (SEP) anti-virus software on the Victim Box detects the malware download, the SEP alert is sent to Symantec Endpoint Protection Manager. The SEP Manager creates an alert in Splunk, which creates a record and initiates an automated workflow in the Swimlane SOAR product. The Swimlane orchestrator begins its workflow by creating a record and obtaining the relevant

information about the affected device from the Splunk alert and Symantec products. Swimlane generates a ServiceNow ticket and sends an OpenC2 command to Symantec's Integrated Cyber Defense Exchange (ICDx). Symantc ICDx is a software layer that standardizes interfaces and enables integration across Symantec products, implementing action orchestration using the OpenC2 standard (Symantec, 2019). Symantec ICDx supports OpenC2 commands by translating them to Symantec API commands that the SEP Manager can implement. Swimlane sends an OpenC2 "contain device" command to Symantec ICDx, which triggers an action within SEP to quarantine the affected machine. After Swimlane receives the command's results from SEP Manager, the workflow updates the Swimlane record and ServiceNow ticket.

This experiment demonstrated the ability of OpenC2 to implement one response action to a security event using SOAR technology. The OpenC2 standard provides a wide array of response actions, and support within the OpenC2 community continues to grow (OASIS-TCS, 2020). Because OpenC2 enables the description of response actions in vendor-agnostic terms that can then be used by SOAR technology, the use of OpenC2 by SOAR to control security products helps mitigate issues of vendor lock-in while speeding automated response to security events.

For more information on SOAR technologies, OpenC2, and other experiments, please visit https://www.iacdautomate.org .

References

[1] OASIS Open Command and Control (OpenC2) TC. (2019, November 24). Open Command and Control (OpenC2) Language Specification Version 1.0. (J. Romano, & D. Sparrell, Editors) Retrieved from OASIS: https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs02/oc2ls-v1.0-cs02.html

[2] OASIS. (2017, September 5). "International Community Comes Together at OASIS to Advance OpenC2 Standard for Automated Defense Against Cyber-Attacks". Retrieved from OASIS: https://www.oasis-open.org/news/pr/international-community-comes-together-at-oasis-to-advance-openc2-standard-for-automated-def

[3] Symantec. (2019). Symantec Integrated Cyber Defense Exchange. Retrieved from Symantec/Broadcom: https://docs.broadcom.com/doc/icdx-partner-en

[4] OASIS-TCS. (2020). "Plugfest-Outcomes.md". Retrieved from https://github.com/oasis-tcs/openc2-usecases/blob/master/Cybercom-Plugfest/Plugfest-Outcomes.md