



OpenC2 Parser for Cisco Security Responses DevNet Gurus' SXO Hackathon Submission

Krishan Veer, Kareem Iskander, Pieter van Schaik and Christopher van der Made Developer Advocates 17th of April 2021



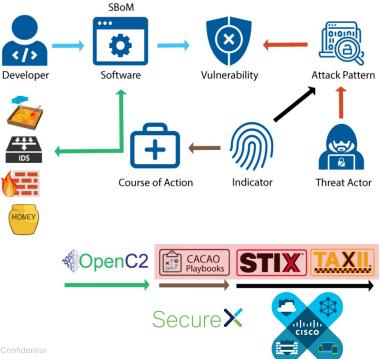
Business Case OpenC2

- OpenC2 is a <u>standardized language for the command and control</u> of technologies that provide or support cyber defenses.
- By providing a common language for machine-to-machine communication, OpenC2 is <u>vendor and application agnostic</u>, enabling interoperability across a range of cyber security tools and applications.
- The use of standardized interfaces and protocols enables <u>interoperability of different tools</u>, regardless of the vendor that developed them, the language they are written in or the function they are designed to fulfil.

Business Case Cisco SecureX OpenC2 Parser ("OpenC2Cisco" or "OC2C")

- Important for Cisco to be interoperable with open-source initiatives.
- Important for Cisco to be <u>interoperable with third-party</u> solutions.
- The use of SecureX orchestration will introduce customers to <u>simple</u> and <u>effective automation</u>.
- Central OpenC2 parser in SecureX orchestration allows for scalability to many Cisco Secure responses.
- Due to the many response actions, customers will be <u>introduced to</u> <u>Cisco Secure solutions</u> that they did not have yet.

Position of OpenC2, SecureX Orchestration and Cisco Secure portfolio...



Overview SXO Atomics Current: Secure HashiCorp -> Add/Remove ₩ **Vault** SHA256 from Custom Detector List Endpoint Roadmap: -> Isolate Endpoint [OPTIONAL] Retrieve API Current: Secure Add/Remove kevs IP from Dynamic Firewall Obiect Roadmap: SXO Main SXO Remote -> URL Group Object OpenC2 OpenC2 JSON SXO command via Source webhook trigger Current: ≪ OpenC2 -> Add/Remove **Domain** from Custom Umbrella Block List A.1 Example 1 Roadmap: This Command would be used to guarantine a device on the network. -> Destination Lists -> Cloud Delivered "action": "contain", "target": { Firewall "device": { "device_id": "9BCE8431AC106FAA3861C7E771D20E53" } SXO Atomics Current: More examples: -> Create Webex Teams Alert -> Create SecureX More... Casebook Roadman: -> ISE Quarantine -> Much more..

Features details

- SXO workflow triggers based on webhook with <u>OpenC2 command in request body</u>;
- Parses OpenC2 command and takes action on: <u>deny, allow, contain and restore OpenC2 action types</u>;
- Depending on the OpenC2 target specific Cisco Security solutions are triggered:
 - deny and allow actions with IPv4 or IPv6 targets will trigger Cisco Secure Firewall (Firepower);
 - deny and allow actions with domain targets will trigger Cisco Umbrella;
 - deny and allow actions with sha256 targets will trigger Cisco Secure Endpoint (AMP);
 - contain and restore actions with IPv4 or IPv6 targets will trigger Cisco Secure Endpoint (AMP) and/or Cisco Identity Services Engine.
- [OPTIONAL] Uses Hashicorp Vault to securely retrieve API keys for various Cisco solutions;
- Creates Webex alerts messages for Security Operations Center (SOC) or other help desk;
- Creates case in <u>SecureX casebook</u> for Security Operations Center (SOC) or other help desk.

Roadmap (6-12 months)

- Add query action support for <u>Cisco Identity Services Engine</u> and Microsoft Active Directory;
- Add domain target support for Cisco Secure Firewall (Firepower);
- Add IPv4 and IPv6 target support for <u>Umbrella Cloud Delivered</u> <u>Firewall</u>;
- Add mac_address and hostname target support for Cisco Secure Endpoint (AMP) and/or Cisco Identity Services Engine;
- More to be announced...



Try it now!

https://github.com/chrivand/securex_openc2cisco