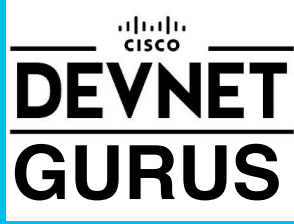


OpenC2 Parser for Cisco Security Responses

DevNet Gurus' SXO Hackathon Submission

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

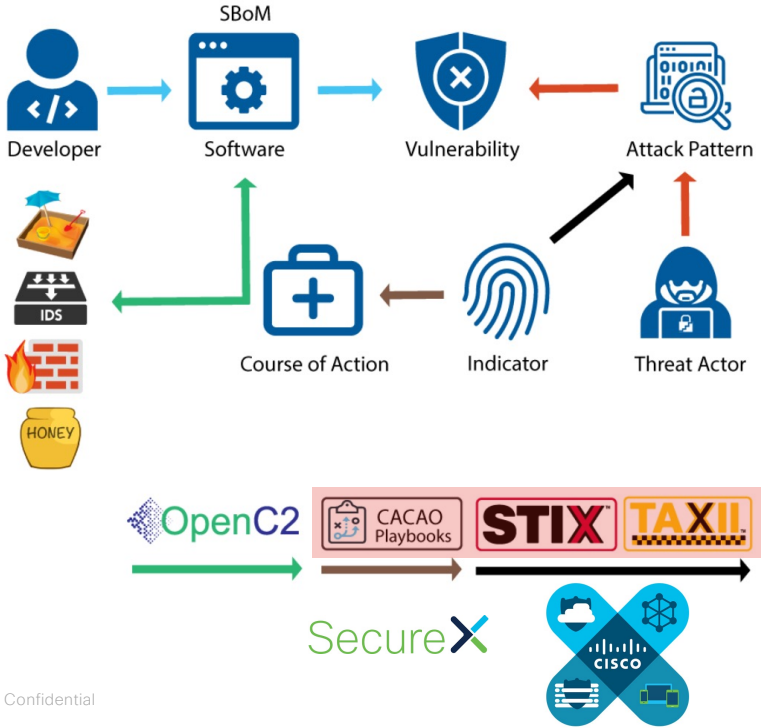
Business Case OpenC2

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

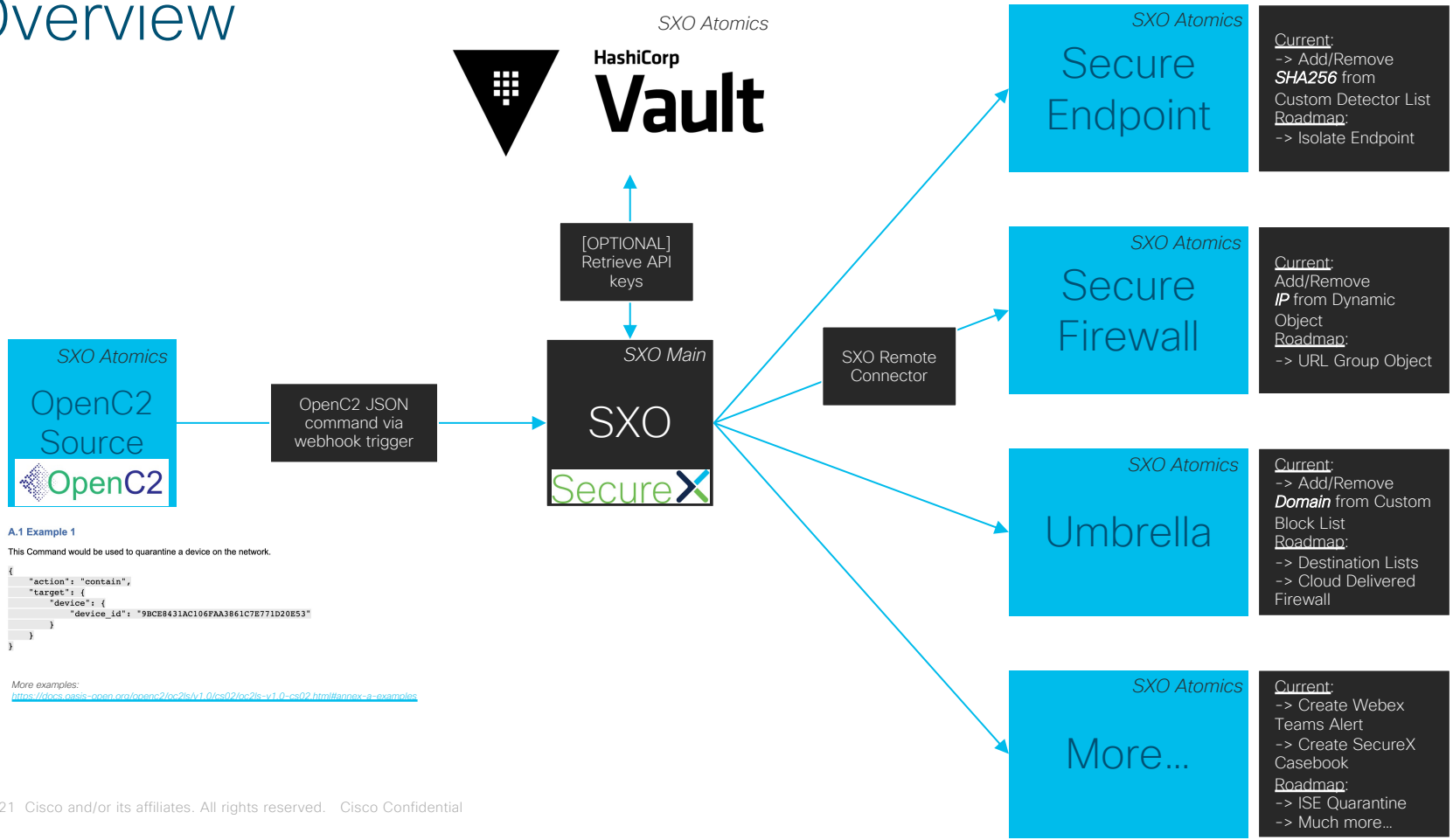
Business Case Cisco SecureX OpenC2 Parser ("*OpenC2Cisco*" or "*OC2C*")

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

Position of OpenC2, SecureX Orchestration and Cisco Secure portfolio…



Overview

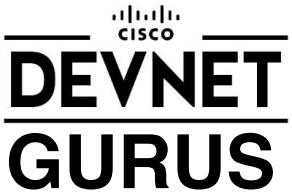


Features details

- SXO workflow triggers based on webhook with OpenC2 command in request body;
- Parses OpenC2 command and takes action on: *deny*, *allow*, *contain* and *restore* OpenC2 action types;
- 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 SecureX casebook for Security Operations Center (SOC) or other help desk.

Roadmap (6-12 months)

- Add *query* action support for Cisco Identity Services Engine and Microsoft Active Directory;
- Add *domain* target support for Cisco Secure Firewall (Firepower);
- Add *IPv4* and *IPv6* target support for Umbrella Cloud Delivered Firewall;
- 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