OpenC2

BIWEEKLY FORUM MEETING

16 March 2017

Agenda

□ Welcome New Members

□ OASIS Transition Q&A

□ OASIS Charter, Non-Normative Document

□ May 19th Face-to-Face Agenda Topics

□ Actuator Profile Subgroup Report

□ Upcoming Events of Interest

OpenC2 TC Charter

- A draft TC charter has been submitted to establish the OASIS Open Command and Control (OpenC2) Technical Committee. In accordance with the OASIS TC Process Policy section 2.2: (https://www.oasis-open.org/policies-guidelines/tc-process#formation) the proposed charter is hereby submitted for comment. The comment period shall remain open until 23:59 UTC on 27 March 2017.

May 19th Face to Face

Agenda

- Prototype Implementations
- JAEN and Data Modeling
- OASIS Transition
- Implementation Considerations
- Future of the "Forum"
- Cyber Security Considerations

5 Actuator Profile Subgroup Update

Actuator Profile Update

- Current LDD is device or technology centric
  - Endpoint
  - Network
  - Process
  - Redundancy in profiles (example, host based, perimeter and network firewalls)
- Proposal: Actuator Profiles should be functional
  - Firewall specifiers and modifiers apply to both network and host based firewalls
  - Use of actuator specifiers to identify a particular firewall if needed
- General Agreement at the March 9 2017 Firewall Profile teleconference

Proposed List

(Based on industry feedback. Not in priority order)

- Directory Service
- Email
- Firewall
- Forensic
- Generic
- Informative
- Investigative
- Network Access Controls

- Reputation
- Router
- Sandbox
- SIEM
- Threat Intel
- Ticketing
- Virtualization
- Web Proxy

Proposed Definitions, page 1 of 2
(Gleaned from Slack)

Type	Description
compute-platform	any general purpose computing device, be it user-oriented (e.g., desktop, laptop, mobile), infrastructure-oriented (e.g., server), or special-purpose (e.g., IoT devices)
malware-detection	Provides detection and notification of malware (e.g., viruses, ransomware)
malware-remediation	Provides removal of malware and restoration of secure system state
malware-analysis	Performs static (e.g., code inspection) and dynamic (e.g., detonation chamber) analysis and characterization of suspected malware
traffic-capture	Performs full / raw capture of network traffic (i.e., pcap)
traffic-characterization	Performs traffic metadata capture (e.g., netflow)
intrusion-detection	Network- or host-based intrusion detection
intrusion-prevention	Network- or host-based intrusion prevention

Page 2 of 2

packet-filtering	Traffic filtering based on packet / protocol characteristics (e.g., 5-tuple)
packet-routing	Traffic routing based on packet / protocol characteristics (e.g., 5-tuple)
content-inspection	Inspection of network traffic at the application level (e.g., email content scanning); may require "break & inspect" capabilities
content-filtering	Traffic filtering based on content characteristics (e.g., email content); may require "break & inspect" capabilities
content-routing	Traffic routing based on content characteristics (e.g., email subject, attachments); may require "break & inspect" capabilities
network-characterization	Determination of network characteristics through a mixture of techniques that may include active scanning and passive traffic and host characterization
vulnerability-scanning	Identification of network and/or software vulnerabilities through scanning

‘Red on Black’

- Human Interaction (Alarm)
  - Means to involve humans (either in the loop or on). Combine email, ticketing, SMS, etc.?
- Access Controls
  - Means to elevate or retract privileges to the system, files or whatever. Combine Network Access Controls and Directory Services?
- Task Analytics
  - Means to analyze data to gain information. Combine Informative, Investigative, Reputation, Forensic and Threat Intel?
- Generic; Equivalent to ‘User Defined’?
- Combine Sandbox and Virtualization?
- Are Firewall, Router, Sandbox, SIEM and Web Proxy OK?

More Red on Black

Type	Description	Questions
compute-platform	any general purpose computing device, be it user-oriented (e.g., desktop, laptop, mobile), infrastructure-oriented (e.g., server), or special-purpose (e.g., IoT devices)	Is this an actuation function?
malware-detection	Provides detection and notification of malware (e.g., viruses, ransomware)	Are malware detection and analysis separate functions?
malware-analysis	Performs static (e.g., code inspection) and dynamic (e.g., detonation chamber) analysis and characterization of suspected malware	
malware-remediation	Provides removal of malware and restoration of secure system state	Is this a single function?
traffic-capture	Performs full / raw capture of network traffic (i.e., pcap)	Are these separate functions?
traffic-characterization	Performs traffic metadata capture (e.g., netflow)	
intrusion-detection	Network- or host-based intrusion detection	
intrusion-	Network- or host-based intrusion prevention	

Even More Red on Black

packet-filtering	Traffic filtering based on packet / protocol characteristics (e.g., 5-tuple)	Distinct from Firewall?
packet-routing	Traffic routing based on packet / protocol characteristics (e.g., 5-tuple)	Distinct from Router? Why limit it to Layer 3?
content-inspection	Inspection of network traffic at the application level (e.g., email content scanning); may require "break & inspect" capabilities	Distinct from Analysis?
content-filtering	Traffic filtering based on content characteristics (e.g., email content); may require "break & inspect" capabilities	
content-routing	Traffic routing based on content characteristics (e.g., email subject, attachments); may require "break & inspect" capabilities	
network-characterization	Determination of network characteristics through a mixture of techniques that may include active scanning and passive traffic and host characterization	Distinct from Traffic characterization?
vulnerability-scanning	Identification of network and/or software	Subset of Configuration

Status/ Way Forward

- □ First Generation Firewall profile underway
- □ Router profile pending
- □ Identify and prioritize Other Actuator Profiles

Upcoming Events of Interest

- □ openc2 and ocas at EEF17 in San Francisco (March 23) Duncan Sparrell http://www.erlang-factory.com/sfbay2017/duncan-sparrell.html
- □ IACD Community Day (March 23) http://www.cvent.com/events/iacd-community-day/custom-20-d4bb79bacefd4c1798ede27d28dc10dc.aspx
- □ OpenDXL Kickoff (April 5) Neal Z on Panel
- □ EICC in Munich (May 9-12) Joe B and a TBA briefer will brief OpenC2.
- □ OASIS Borderless Cyber NYC (June 21-22) (http://us17.borderlesscyber.org/en/)