(U) Open C2 Proof of Concept

(U) Deny at Perimeter

29 September 2016
Presented by
Joe Brule
Larry Salazar

CONFIDENCE IN CYBERSPACE

The overall Classification of this video is Unclassified//For Official Use Only

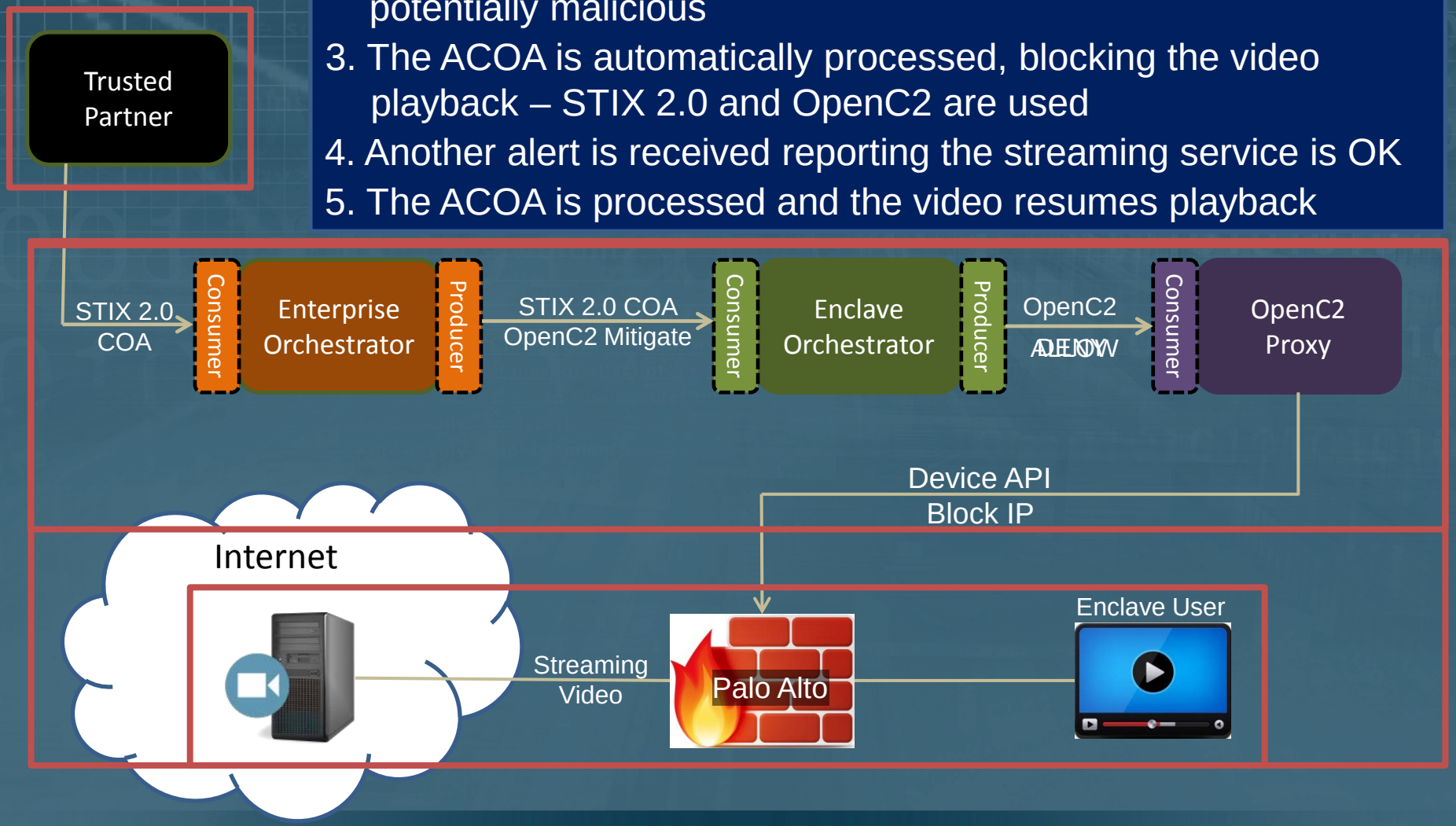
Introduction

- Modern network defenses :
  - Striving to share threat data between enclaves
  - Need uniform communications to end points

- This video shows:
  - Shared threat information via STIX 2.0
  - Uniform communications via OpenC2

Architecture / Use Case

1. User starts streaming a video from the internet
2. The enterprise receives an alert stating the streaming service is potentially malicious
3. The ACOA is automatically processed, blocking the video playback – STIX 2.0 and OpenC2 are used
4. Another alert is received reporting the streaming service is OK
5. The ACOA is processed and the video resumes playback



Face to Face Reference ArchitectureFinal.mp4

Closing

- This video demonstrated sharing threat data with mitigations down to the end points with OpenC2.
- OpenC2 resources are found at:
  - https://github.com/OpenC2-org
  - http://openc2.org/
- Contact Joe Brule (jmbrule) for more information or to schedule a live demo.