|  |
| --- |
|  |
|  |
| XSOAR Hackathon  Threat Detection and Containment in IT-OT Converged Network - Playbook  NTT CoE |
|  |
| 21 September 2020 Document Version 1.0 |
|  |

Table of Contents

[1. Problem Statement 3](#_Toc52140399)

[2. Lab Environment 4](#_Toc52140400)

[3. Playbook Summary 5](#_Toc52140401)

[4. Playbook High Level Workflow 6](#_Toc52140402)

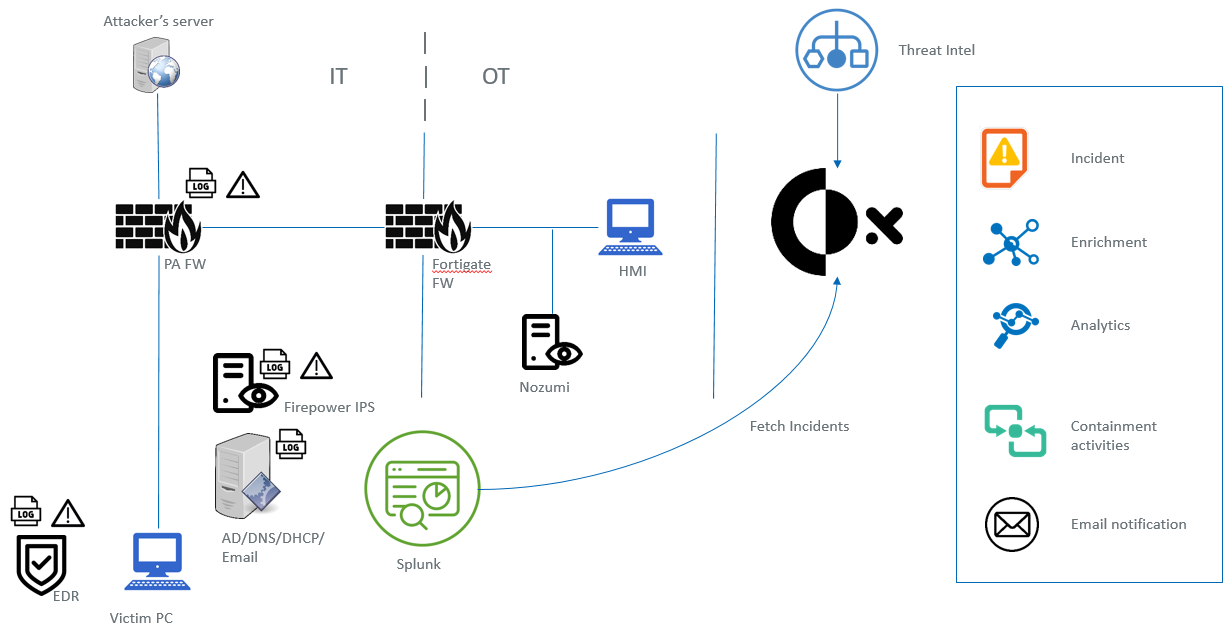
[5. The Team 7](#_Toc52140403)

# Problem Statement

We see more and more IT-OT converged networks, as manufacturing and critical infrastructure organizations try to achieve their digital transformation goals. These converged networks increase the attack surface by exposing the OT environment to always connected internet accessible networks against the traditional well controlled (sometimes separated by an air gap) OT network boundaries. Over the last few years we have seen some targeted attacks intentionally using the IT environment as a pivot point to enter OT networks to achieve their objective but most of the time incidents are generated by threats built to target IT environments, unintentionally impacting OT networks. There are fundamental differences between handling an IT security alert vs OT security alert, where IT world focuses on confidentiality/Integrity while OT world’s main focus being availability. Although there are lot of differences between IT & OT worlds in many ways such as CIA priority and protocols used, more and more fusion SOCs are being built to monitor these converged networks for threats and compliance.

Primary challenge is to correlate the alerts generated by both IT and OT point security products, identify the malwares that could have moved across IT-OT boundary impacting the critical OT assets and contain them preventing further damage to the organization in a structured manner. Secondary challenge being optimizing the analyst efforts spent on manually gathering, enriching indicators and evidence.

# Lab Environment



XSOAR Integrations:

Firewalls : Palo Alto Firewall, Fortigate Firewall

IPS/IDS : Firepower (IT), Nozumi (OT)

Servers : Active Directory, MS Exchange

Log Server : Splunk

Threat Intel : Virus Total (Public), IPinfo, Phishtank

Tasks to Achieve via Playbook

* Streamline threat detection activities
* Assist all analyst to provide high quality resutls
* Automate incident creation
* Automate indicator extraction
* Automate evidence fetching
* Automate enrichment
* Assist event driven threat hunt activities to be more efficient
  + Find related incidents generated other IT/OT security controls
  + Provide latest OT alerts
* Automate containment activities and notification
* Assist confirmation of eradication and recovery

# Playbook Summary

* Log Collection: Firewalls, IPS/IDS and Servers are forwarding logs to the splunk
* Incident Fetch: Splunk integration on XSOAR is configured to fetch incidents from splunk using a query crafted to select logs with sourcetype:panthreat and specific labelled fields required for analysing the incident
* Enrichment: Playbook initially confirms that required field are populated (PCAP, URL, IP addresses, User), followed by enriching the information with integrated threat feeds and servers
  + PCAP – Extract Indicators
  + IP addresses,URL – Enrich using Virus Total, IPinfo
  + User – Enrich using Active Directory
  + Confirm presence of malicious indicators
* Event Driven Threat Hunt: ML automation is used to find incidents that are similar, generated by IT (FW, IPS) and OT(IDS) security controls in order to confirm lateral movement within converged network.
* Incident Validation and Containment action confirmation by Analyst: Analysts validate the incident and confirm containment actions by analysing the enriched indicators/evidence and similar incidents that has taken place during a windows of time.
* Containment actions:
  + User – Account disabled temporarily and notify user’s manager/ IT service desk via email
  + Endpoint – Isolating the endpoint/endpoints involved in the incident using EDR and notify user’s manager/IT service desk via email
  + OT – Fetch latest alerts from Nozumi IDS using query automation, update incident with query results to be used by analyst to asses on going activities in OT network, assess and submit a the impact report. The impact report is emailed to the OT management team aiding the containment action decision making process.
* Review success of containment, eradication & recovery activities: Analysts evaluate on-going activities/alerts and confirm the effectiveness of action taken. If involved endpoints users are confirmed to clean go ahead and close the incident, if related activities are continue to be observed update user’s manager and IT service desk. If containment, eradication and recovery actions are found to be ineffective, incident has to be escalated to major incident management team.

# Playbook High Level Workflow

Analyst validates effectiveness of remediation actions, monitor further related activities and based on observation make the decision to close incident or escalate.

Based on Analyst decision

OT – Evaluate impact on OT environment

Endpoint – Isolate endpoint using EDR

User – Temporary disable AD access

Notification – Email notification

Analyst validates the incident by evaluating the OT/IT incident generated during the time window and confirms the containment actions.

XSOAR looks for similar incident over last “X” hours, using ML automation (Incidents generated by OT and IT security controls)

XSOAR validates the available indicators and enrich them (IP, user, PCAP, URL)

XSOAR monitors splunk for specific logs with sourcetype:panthreat, fetches alert logs and create incident.

Splunk receives logs from Firewalls, IPS, servers, including the alert logs from Palo Alto Firewall

Palo Alto Firewall generates threat alerts based on the traffic inspected and forward the logs to splunk

# The Team

Weranga Kumaradasa

John Kiac

Ashish Bansal

Phil Jeon

Yousuf Faizal

Jay Kar

# Playbook Screen capture

