FloCon 2021

Using Data to Defend

An Architecture for Situational Awareness

Timothy Shimeall, Ph.D.

CERT Situational Awareness Group

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0015

FloCon 2021

An Architecture for Situational Awareness

Overview

Motivation

Elements

Architecture

Summary

Motivation

- Experience in fielding awareness for network security, particularly methods that scale to and above Internet security providers
- Desire to provide methods of use in realistic security defense of networks
- Inclination for awareness that can generalize across networks and attacks
- Recognition of the changing nature of awareness

Scalability

Providing sufficient detail for utility vs. confusing results

Showing data displays too crowded to display data (plot goes grey)

Representing multiple axes of variation effectively

Generating results in reasonable amounts of time

Back-hauling data to central point for processing vs. federating distributed data sources processed locally

Ensuring known provenance of results (data goes brown)

Unclean Data

Network attackers (and defenders) don't produce clean data

- Traffic artifacts (exponential back off, repeated termination, scanning, distraction)
- Deception and concealment engineered in (protocols, ports, endpoints)

Data is almost never normally distributed

- Network behaviors driven by work cycle and network stacks, not individuals
- Attack behaviors: noisy or invisible

Power-law distributions are often not useful

Often need to transform data before it can be effectively used or displayed

- Clean and regularize
- Scale and measure

Elements

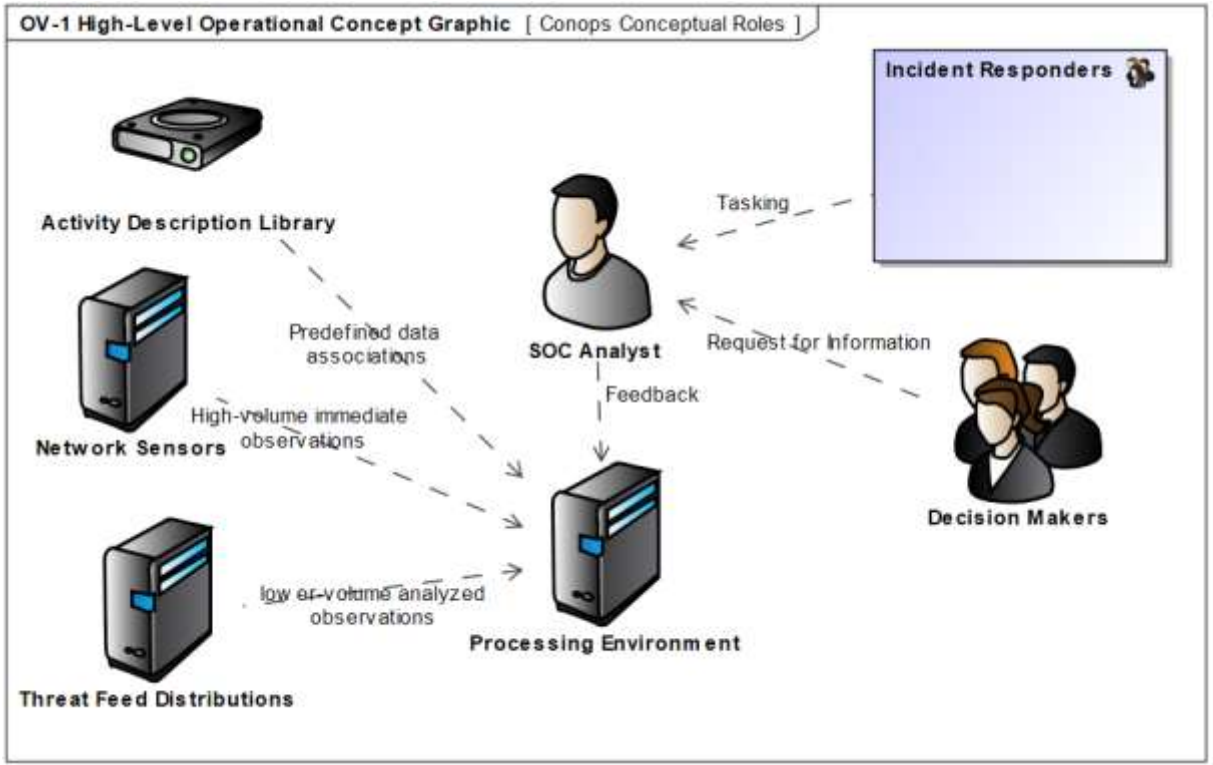
Hybrid Implementation (Cloud/Organization local)

Diverse data sources (Traffic, alert, routing, threat intel, logs)

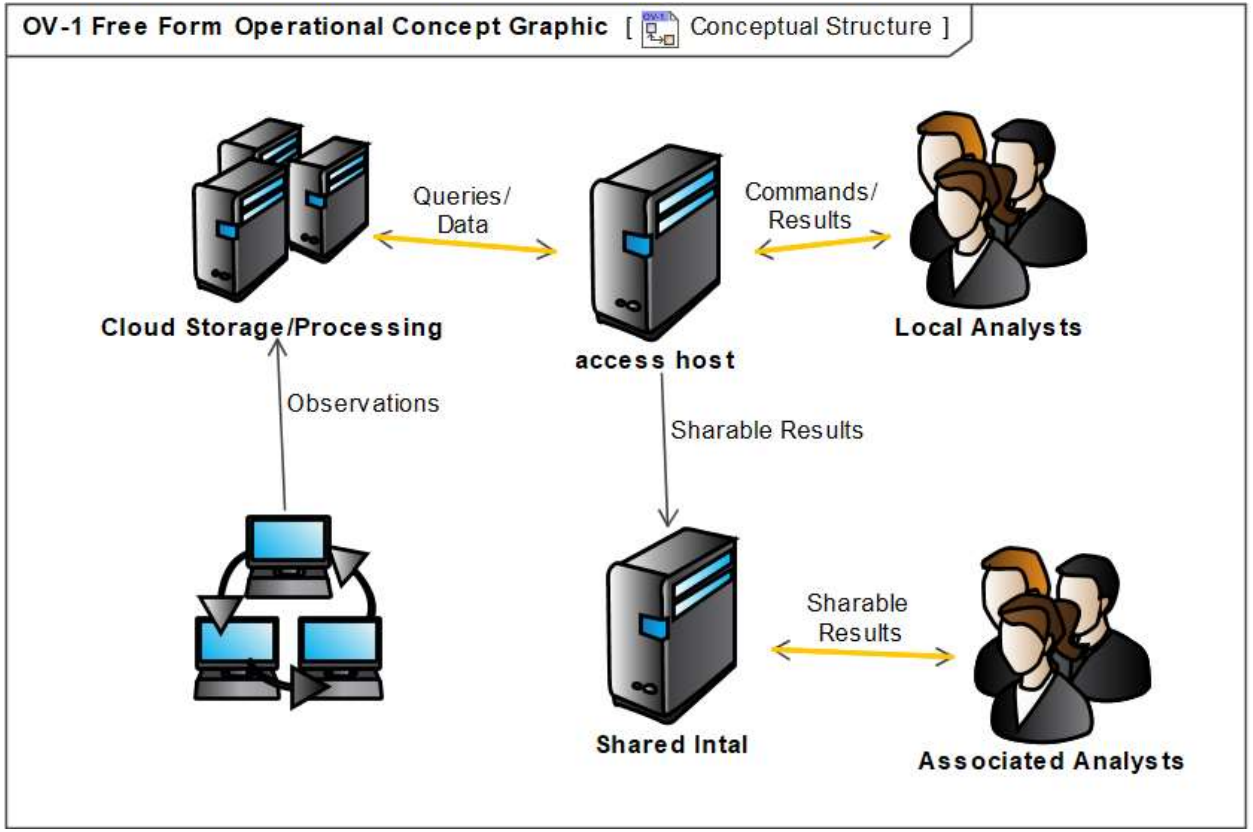
Semi-coordinated teams

Communication environment (Site, enterprise, supra-enterprise)

Architecture



Team Connections



Summary

Current high-level architecture being refined

Providing solutions applicable to real networks of scale

Finding the threat where it is, not where we'd like to look