Exploring the Interactions Between Network Data Analysis and Security Information/Event Management

Timothy J. Shimeall
CERT® Network Situational Awareness (NetSA) Group
January 2011

Overview

Network Data

Security Information/Events

The Problem

Events, Revisited

Analysis leading to Events

The Problem, Revisited

Summary

Network Data

larger network, more security data

Data: Packets, Flows, DNS resolutions, host log entries, firewall log entries, etc.

Data (in general) -> Low security information density

Analysis (in part) -> Use goal/context to focus on higher-density data subsets, convert to aggregated form

Security Information/Events

Commonly: “Event: Something that happens”

SIEM: Event:

- Something describable via the schema
- Instance of security-sensitive activity observed at a device
- Aggregations of security-sensitive activity
- Chains of security-sensitive activity

Information: Context for analyzing or processing events

The Problem

If “generation of data instance” = “event”, too many events

- For collection and processing
- For human analysts

Candidate solutions:

- Sampling
- Reduce data on arrival
- Restrict scope
- Restrict classes of data

Events, Revisited

Definition: “Security sensitive event -- instance of activity that, in context, is associated with a threat to the network or with its defensive strategy.”

Security sensitivity depends on context

Effective security depends on strategy

Edge devices (router, firewall, proxy, etc.) can not have that context (or time to process it)

Analysis as Event Mediator

Event mediator: Automated actors receiving instances of network activity and applying context and strategy information to filter for security-sensitive events.

Application:

- Process-mapping approach, isolating critical “tipping points” sensitive for security
- Rule-based approach, identifying specific events with high security sensitivity
- Learning approach, using historical data to build indicators of security sensitivity

All three approaches are based on analysis.

Moving Closer to Reality

Mediators provide more achievable information distribution

- Core-outward: context information, strategy rules
- Edge-inward: filtering (and re-filtering) event stream to isolate security sensitivity.

Mediators simplify handling

- By automation: fewer intervening cases
- By humans: lower event rates

The Problem, Revisited

How often to publish context

- Rule updates
- Repeated training

How to incorporate strategy

- Deception
- Frustration
- Resistance
- Isolation/Recovery

Summary

Initial definition of security sensitive event

Decomposition of problem

Strategies for further development

Experience and experimentation needed