Security Automation –
Tips, Tricks and Techniques

Henk Birkholz (henk.birkholz@sit.fraunhofer.de)

Chip-To-Cloud September 23rd 2014

Security Automation (examples of application)

- Network Access Control (**NAC**) / Trusted Network Connect (**TNC**)
- Continuous Monitoring (**CM**)
- Security Information and Event Management (**SIEM**)
- Virtual Infrastructure Management **(VIM**) / Orchestration

Basis for Automated Assessments/Assertions/Decisions

- **NAC**: system state, endpoint identification, policies
- **CM**: inventory catalog, topology, maintenance schedule
- **SIEM**: event correlation, asset catalogs, incident categories
- **VIM**: SLA, state of resource consumer / provider, optimization

Roles in Security Automation

- **Consumer of Information**
  - NAC, CM, SIEM, VIM, etc.
- **Producer of Information**
  - Clients, Server, network components, etc.
  - IDS, netmon/netflow, Icinga, etc.
  - Logfiles, SNMP/MIBs, CLI, SOAP, REST, websockets, etc.

Key Factor for Security Automation

- The **basis** for decision-making has to be **provided** for security automation
- This **basis** is also **acquired** via automated procedures
- The **quality** of this basis is the **key factor** to security automation

- „To know what to do, you have to know **what you have**“
- Assets with **interconnected** relationships that produce information
- **Context** is everything

Pro-Active vs. On-Demand

- Having the right information at the **right time**.
  - Aggregation & correlation **takes time**.
  - Collecting context information without corresponding requirements…
    - … can violate privacy requirements or compliance guidelines.

- Having **up-to-date** information…
  - requires a well maintained / managed **acquisition process**.
  - can fail if it is not available **ad-hoc**.
    - requires a **fallback**.

- You can do **both** to double check (and reveal inconsistencies).

Quantity vs. Quality

- Producer of Information produce a **default set** of security related information
  - that is most of the time…
    - unstructured
    - incomplete
    - in dire need of refinement
  - that **does not scale** well if aggregated blindly

- **Documentation** is the basis for **quality**.
  - Security Goals
  - Producer, Consumer, and a well structured information **flow between** them.

Configuration vs. State

- A matter of scalability…
- …and feasibility.

- Configuration and state are sometimes difficult to distinguish.
  - Sometimes an endpoint attribute can be both…
    - …depending on the context.

- Both are an important basis for determining identity
  - Identity is an assertion.
  - Unique identifier are therefore valuable.

Attributes vs. Events

- An endpoint attribute has a **value** that can be acquired (via automatic procedures).
- An event is the **change** of an attribute **value** at a specific time.

- Multiple attributes can be converted into events
- Events can be converted into multiple attributes

- **Events** are typically processed in **streams** and require the continuous availability of processing capacity.
- **Attributes** are typically processed in **bulks** (collections/bundles/bursts) that can be processed

Integration into Business Processes

- Structured Security Information is a **commodity**.
  - Producing security events & Collecting endpoint attributes.
  - Providing a **standardized** communication schema**.**
- Producing security information requires a **management** process.
  - Risk Management
  - Asset Management
  - Configuration Management
- Security information needs a **purpose** to provide a benefit.
  - Understanding produced and consumed information.
  - Homogenizing / aggregating it requires understanding it.

Creating Context

- Homogeneity
  - Event Transport
  - Attribute Collection
  - Security Information Repositories

- Lingua Franca
  - To fit the puzzle pieces, there has to be a pattern,
    - a common understanding, a common language.
  - Examples: IDMEF, SCAP, IF-MAP, SACM

- …and the flexibility to do what you need to do.

What do I have to to do?

- Gap-Analysis
  - What do you have?
  - What do you need to satisfy your requirements?
  - Typical goals: compliance, resilience, confidentiality.

- Create more than a list of things / checklists.
  - Relationships and dependencies
  - Service graphs
  - Supported business processes