Compare and Contrast Automation Concepts and Technologies

Chapter 14

Episode 14.01

Workflow and Scripting

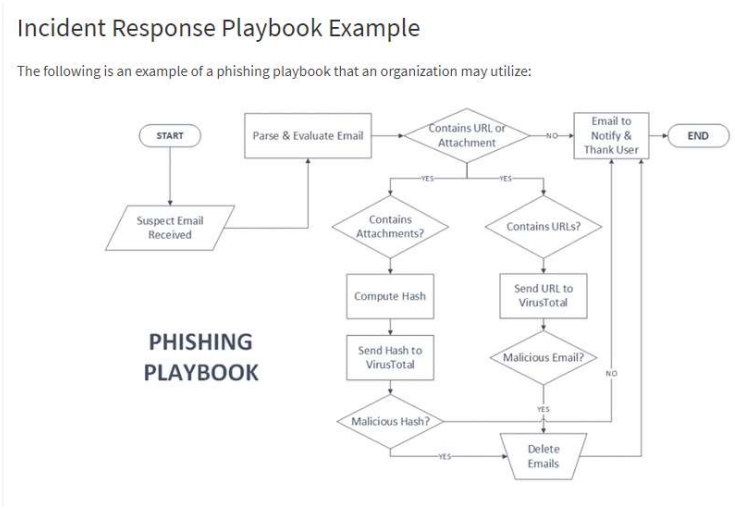
Objective: 3.4 Compare and contrast automation concepts and technologies.
• Workflow orchestration
- Security Orchestration, Automation, and Response (SOAR)
• Scripting
• Data enrichment

Workflow Orchestration

- Security orchestration, automation, and response (SOAR) platforms
  - Automate common tasks
  - Standardize incident response
  - Organize flow to help catch mistakes and repeat processes easily
  - Example: Splunk Phantom (formerly Phantom Cyber)

Workflow Orchestration

- Playbooks
  - Visualizations of workflows



Source: https://securityboulevard.com/2019/09/how-to-build-an-incident-response-playbook/

Data Enrichment

- Transform raw data into actionable information
- Enrichments lead to additional insights
- Process is to correlate known data with additional details
- Example
  - Detected newly opened RDP ports on monitored computers
  - Vulnerability feed queries of RDP ports being opened result in hits for Sarwent malware
  - Alert created for potential Sarwent malware infection

Scripting

- Automate the repetitive stuff
- Administrators have known about the power of scripting for decades
- Great for standardizing any mundane tasks
- Common scripting environments:
  - Python
    - Check out Violent Python book
  - PowerShell (not just for Microsoft Windows)

Episode 14.02

API and Malware Signature Creation

Objective: 3.4 Compare and contrast automation concepts and technologies.
- Application programming interface (API) integration
- Automated malware signature creation

Application Programming Interface (API)

- Gives the ability to reach out and consume services created by others
  - Link your code and scripts to someone else's software with minimal overhead
- Representational State Transfer (REST) method
  - Quick and easy way to consume remote services
  - Create HTTP request, send to Web server; Web server translates request into a function call

Application Programming Interface (API) Integration

- Representational State Transfer (REST) method
  - Entire architecture is client/server
  - Stateless
  - Cacheable
  - Uniform interface
    - Manipulation of resources through representations
    - Self-descriptive messages
    - Hypermedia as the engine of application state
  - Layered system
  - Code on demand (optional)

Application Programming Interface (API) Integration

- Representational State Transfer (REST) method
  - Embed in any language
  - Call from command line
    - curl (character-based URL)
    - curl --request GET \ --url https://www.virustotal.com/api/v3/domains/{domain} \ --header 'x-apikey: <your API key>'

Error Codes

Error Code	HTTP Code	Description
AlreadyExistsError	409	The resource already exists.
AuthenticationRequiredError	401	The operation requires an authenticated user. Verify that you have provided your API key.
BadRequestError	400	The API request is invalid or malformed. The message usually provides details about why the request is not valid.
ForbiddenError	403	You are not allowed to perform the requested operation.
QuotaExceededError	429	You have exceeded one of your quotas (minute, daily, or monthly). Daily quotas are reset every day at 00:00 UTC.

Automated Malware Signature Creation

- Useful to keep up with rapidly changing malware threat
- YARA
  - Identify and classify malware samples
  - virustotal.github.io/yara/

Episode 14.03

Threat Feeds and Machine Learning

Objective: 3.4 Compare and contrast automation concepts and technologies.

- Threat feed combination
- Machine learning

Threat Feed Combination

- Aggregating disparate data streams is always difficult
- Threat feeds may provide data in different formats
- Scripting can help automate transforming data into a single format
  - Easier to read, understand, and respond

Machine Learning

- Field of computer science
- Algorithms examine datasets to reveal trends and indicators that can predict future behavior
- An algorithm “learns” by using historical data to make predictions
- Similar fields
  - Machine learning
  - Data mining
  - Data science
    - Involves process, business side, machine learning, analysis

Machine Learning

- Data mining
  - Looking at large data sets to extract previously unidentified valuable data
- Machine learning
  - Looking for trends

Machine Learning

- Useful in security analysis
  - Past attack behavior can predict what's next
- Based on the natural tendency to stabilize
- Supervised vs. unsupervised learning
- Examples: neural networks, decision trees, SVM, regression, etc.

Episode 14.04

Protocols, Standards, and Software Engineering

Objective: 3.4 Compare and contrast automation concepts and technologies.

- Use of automation protocols and standards
- Security Content Automation Protocol (SCAP)
- Continuous integration
- Continuous deployment/delivery

Automation Protocols and Standards

- Security Content Automation Protocol (SCAP)
  - Great place to start to automate cybersecurity analysis tasks
  - Languages
  - Reporting formats
  - Identification schemes
  - Measurement and scoring systems
  - Integrity
  - Example: OpenSCAP

Software Engineering

- Continuous integration
- Continuous delivery
- Continuous deployment