Use Case Scenario Development & the ARECI Chart

Nathan Clarke
APAC ASOC Manager
Let’s set this up...

The problem this is trying to solve...

Scope / not in Scope

Time up front...

Not a panacea...

Use Case Development

- Use Case Concept & Scenario Development
- System Context & Normality
- Threats
- Charting Data, Availability (ARECI), & Feasibility

Engineering

The hard stuff engineers do
Top 5 Global Risks in Terms of Likelihood

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks


Compromised Data Varieties

- Internal
- Credentials
- Personal
- Medical
- Payment
- Secrets

Source: Verizon Data Breach Report 2019

Use Case Concept & Scenario Development
System Context & Normality
Threats
Charting Data, Availability (ARECI), & Feasibility
Use case development should be a team sport. Analysts and SIEMS Engineers both have unique perspectives to bring into use case & detection development.

- Incident Scenario
- Event Analysis
- Evidence Validity
- Handling Difficulty
- Playbook Guidance
- Clear Determinations
- Response Actions

- Use Case Analysis
- Data availability
- Correlation Logic
- Resource Conservation
- Alert Engineering
- Testing & Deployment
- Further tuning & On boarding

*Side note: Awesome Teamwork 😊
Get your facts first, and then you can distort ‘em as much as you please.
A use case scenario needs good constraints in order to ensure that the development leads to the SIEMS presenting good work to analysts. Good constraints include principles for presentation, careful interpretation of what defines an incident and thresholds to action for the organisation.

1. Must be security relevant
2. Must be actionable
3. Must be presented with enough information
Start documenting

Use Case
Concept & Scenario Development

System Context & Normality

verizon
This use case/correlation rule will alert the analyst that a potential security incident has resulted from the detection of a local interactive login/authentication on a critical host from an unusual/unauthorised source and/or at an unusual date and time.
This part of the development will establish relative norms in the environment. (In this example, authentication).

The section of use case development documentation can contain or reference:

- Diagrams / Architecture
- Statements / SOPs
- Past observations by analysts
- Controls / Preventions in play
- Information pertaining to humans (how many, groups/roles in scope, working hours, locations, etc)
Not intended to be an exhaustive analysis of threats, but focused on the deviant behaviour expected in this scenario.

The section can include:

- References to past incidents related to this scenario
- Links to intelligence reports & resources
- Links to Pre/ATT&CK Matrix entries
- Models demonstrating detections and control/response pairing (Kill Chain COA)
This use case/correlation rule will alert the analyst that a potential security incident has resulted from the detection of a local interactive login/authentication on a critical host from an unusual/unauthorised source and/or at an unusual date and time.

<table>
<thead>
<tr>
<th>Type</th>
<th>Source Data</th>
<th>Utility / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Points</td>
<td>HTTP Logs</td>
<td>Records methods and requests including deviant requests like SQLI</td>
</tr>
<tr>
<td></td>
<td>WAF Logs</td>
<td>Alerts on known deviant requests that are blocked and/or logged</td>
</tr>
<tr>
<td></td>
<td>Web Server Host/SQL Logs</td>
<td>Records host activity and other service's events. Will show deviations from norms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>if host breached. Example: File mod, new procs, etc</td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td>Web Load Balancer Logs</td>
<td>Provides records of mapping external source to web host for alert enrichment</td>
</tr>
<tr>
<td></td>
<td>Ext Firewall</td>
<td>DMZ-&gt;External logs capture unusual attempts to call out on disallowed ports</td>
</tr>
<tr>
<td></td>
<td>DMZ Firewall</td>
<td>DMZ-&gt;Internal logs capture unusual attempts to connect internally</td>
</tr>
<tr>
<td>Asset &amp; Config</td>
<td>Public facing web host</td>
<td>CMDB events advising of changes in web host configuration</td>
</tr>
<tr>
<td>Management DBs</td>
<td>entries in CMDB</td>
<td></td>
</tr>
<tr>
<td>Traffic &amp; Flow</td>
<td>Netflow Logs</td>
<td>Flow records current and historical connection</td>
</tr>
<tr>
<td></td>
<td>PCAP</td>
<td>Recording traffic contents (C2)</td>
</tr>
<tr>
<td></td>
<td>ZEEK</td>
<td>Connection records and protocol parsers - Detect SQLi Script</td>
</tr>
<tr>
<td>Threat Intel</td>
<td>VTRAC TI Feed</td>
<td>Contains indicators related to web attacks occurring in current campaigns</td>
</tr>
<tr>
<td>Org Data</td>
<td>RBA</td>
<td>Directory containing authorised web administrators</td>
</tr>
</tbody>
</table>
List everything required for both correlation and investigation*

Then work on the availability*

Feasibility informs prioritisation of effort

Warning #1: Do not exclude anything required for the scenario!
Data Availability & Gaps

- **In SIEMS**: It’s there and ready for use in correlation or as part of an investigation.

- **In Env**: It’s in the system, but not yet joined to the logging architecture.

- **Not Avail**: It isn’t there or source doesn’t have an ability to send logs.

A basic feasibility will start to establish itself here. Some deeper analysis may be required in engineering*

This is a good point to decide if moving forward is worth the effort, or move onto to another use case.
Collate similar use cases (same type of host or attack). They probably share similar requirements.

Establish data availability / non-availability across multiple use cases.

**Capability Needs:**
- Netflow: 5
- Taps: 4

**On Boarding Needs:**
- WAF Logs: 5
- Host Logs: 4
- EDR Logs: 3
- RBA/LDAP: 2
Own the gaps (and use them)

Don’t discard the scenario if you don’t have data to achieve good correlation

Keep a ledger of all detection requirements that aren’t met and how many use cases they effect, and use it!

If a use case is not feasible, and that use case is based on an organisational risk, let the risk manager know!
If you don’t have gaps....

- Schedule the use case for engineering!
- The collaboration isn’t over!
- Presentation matters.
- Continual improvement: Keep the analyst/engineer feedback loop & team work happening through to testing and into production.
LET THE TUNING COMMENCE!
Assess your data potential with ATTACK Datamap

<table>
<thead>
<tr>
<th>Instance</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Brute Force</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Application Deploy Software</td>
</tr>
<tr>
<td>Account Manipulation</td>
<td>Accessibility Features</td>
<td>Credential Dumping</td>
<td>Credentials in Files</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Compo Object Model</td>
</tr>
<tr>
<td>Cert DLLs</td>
<td>AppCert DLLs</td>
<td>Credentials in Registry</td>
<td>Credentials in Registry</td>
<td>Exploitation of Rem Services</td>
<td>Exploitation of Object Control Services</td>
</tr>
<tr>
<td>Init DLLs</td>
<td>Asperm DLLs</td>
<td>Exploitation for Credential Access</td>
<td>File and Directory Discovery</td>
<td>File and Directory Discovery</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>Application Shimming</td>
<td>Application Shimming</td>
<td>Forced Authentication</td>
<td>Network Service Scanning</td>
<td>Network Service Scanning</td>
<td>Network Service Scanning</td>
</tr>
<tr>
<td>Authentication Package</td>
<td>Bypass User Account Control</td>
<td>Hooking</td>
<td>Network Share Discovery</td>
<td>Network Share Discovery</td>
<td>Network Share Discovery</td>
</tr>
<tr>
<td>Jobs</td>
<td>Dll Search Order Hijacking</td>
<td>Input Capture</td>
<td>Password Policy Discovery</td>
<td>Password Policy Discovery</td>
<td>Password Policy Discovery</td>
</tr>
<tr>
<td>Jitkit</td>
<td>Exploitation for Privilege Escalation</td>
<td>Kerberos</td>
<td>Peripheral Device Discovery</td>
<td>Peripheral Device Discovery</td>
<td>Peripheral Device Discovery</td>
</tr>
<tr>
<td>User Extensions</td>
<td>Extra Window Memory Injection</td>
<td>LLMNR/NBT-NS Poisoning</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
</tr>
<tr>
<td>Component Default File Location</td>
<td>File System Permissions Weakness</td>
<td>Hooking</td>
<td>Query Registry</td>
<td>Query Registry</td>
<td>Query Registry</td>
</tr>
<tr>
<td>Component Object Model</td>
<td>Hooking</td>
<td>Password Filter DLL</td>
<td>Shared Webroot</td>
<td>Shared Webroot</td>
<td>Shared Webroot</td>
</tr>
<tr>
<td>File Account</td>
<td>Image File Execution Options Injection</td>
<td>Process Discovery</td>
<td>Taint Shared Conne</td>
<td>Taint Shared Conne</td>
<td>Taint Shared Conne</td>
</tr>
<tr>
<td>Search Order Hijacking</td>
<td></td>
<td>Remote Services</td>
<td>Third-party Software</td>
<td>Third-party Software</td>
<td>Third-party Software</td>
</tr>
</tbody>
</table>
Thank you.