A Use Case Framework for Intelligence Driven Security Operations Centres

Angelo Perniola
ACD Senior Consultant
RSA Advanced Cyber Defense EMEA
@AngeloPerniola

David Gray
ACD Practice Consultant
RSA Advanced Cyber Defense EMEA
@D4VID_GRAY
So ... what's a Use Case?
What we will talk about

- Context – background and history
- Our solution - “Use Case Framework”
  - Granular walkthrough of each step
- The benefits
- From “huuu?!?” to “yeah!!!”
Whoami

❖ Angelo Perniola, Sr. RSA ACD Consultant
  ❖ 10 years of Information Security
  ❖ Ex Italian Army Officer; in love with basketball, triathlon and infosecurity

❖ David Gray, Practice RSA ACD Consultant
  ❖ 8 years of Information Security
  ❖ Ex Royal Air Force Malware Team Leader

❖ The work presented today is based on experiences of the whole RSA ACD team
Use Case Framework at a glance
Use Cases 1.0 (or 0.1-beta 😊)

- End to End solution framework
- More Granularity
- Incorporates all information required to Create, Monitor and Test a Use Case (not only alerts/reports!!!)
- Puts together Detection AND Response
- Able to reflect the detection logic from different technologies/vendors
Objective

- Why we need the Use Case and what we want to accomplish
- Along with Threat, this is of major importance to a Manager
- Improves Effectiveness of SOC by targeting resources
Threat

- What we want to Defend against
- Should identify some scenarios we are looking to detect
- Give background to why the Use Case has been created
Stakeholders

- Stakeholders are not necessarily the owners of the Use Case
- They are analysts involved in detecting threats and responding to incidents
- Any external parties should be incorporated
  - IT OPS
  - Law Enforcement Contacts
  - MSSP’s
Data Requirements

◆ The raw Log/Packet/Flow/Endpoint Data sources that are required to be able to detect our Threat

◆ Consultation with local Content Team is key

◆ External feeds should be incorporated:
  ◆ Threat Intel (e.g. RSA Live, Open Source/Commercial …)
  ◆ Context (CMDB, VIP list, change requests, …)
Logic

- How we are going to detect our malicious behavior
- This can be a high-level overview
- More value comes from being as specific as possible
Logic [cont.]

- Example (high level):
- Example (technology dependant):

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Port 21 (FTP) or PORT 80 (HTTP)</td>
</tr>
<tr>
<td>ip_src</td>
<td>NOT IN list of authorized IP Addresses</td>
</tr>
<tr>
<td>Data Pattern</td>
<td>Port 21 AND &quot;put&quot; followed by Port 80 AND &quot;get&quot;</td>
</tr>
</tbody>
</table>

Threshold: 1 in 10 Minutes

```
DEFINE
  U as U.service = 21 AND 'put' = any (U.action),
  D as D.service = 80 AND 'get' = any (D.action)
);```
Testing

- How we know the Logic will produce a (reliable) alert
- Key to validating the Content Rules
- Should be tested first in a QA environment before being tested on a live network (with benign traffic)
- Results should be fed back into the Logic to ensure the greatest degree of confidence is achieved
Priority

- Provides guidance to SOC Analysts
- Dependent upon policies and business requirements
- Any changes to Priority as a result of asset value should be considered
  - i.e. An Active Directory Server would have a higher priority than that of a User’s workstation
Output

- Reports
- Dashboards
- Incident Response Procedures

"Failure to prepare is preparing to fail" gives clear guidance to analysts as to what they are looking for and what their next steps are.

Tasks
- Data to be collected
- Escalation and decision points

And what
## Workflow/Procedural Steps

<table>
<thead>
<tr>
<th>SecOPs Incident Response Task ID</th>
<th>Step Number</th>
<th>Task Name</th>
<th>Description</th>
<th>Required / Optional</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT-0010</td>
<td>0.10</td>
<td>Notification received of Insider Threat</td>
<td>Add all details of the Notification to the Incident Ticket. Ensure that all details of the detection or the member of staff reporting the incident are added to the case.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0020</td>
<td>0.20</td>
<td>Establish if a &quot;Confidential&quot; Incident</td>
<td>Establish if the case is to be classified as &quot;Confidential&quot; and who is to be allocated access.</td>
<td>Required</td>
<td>ACME: Analyst, ACME: Manager</td>
</tr>
<tr>
<td>IT-0030</td>
<td>1.10</td>
<td>Log relevant information from suspect system</td>
<td>Log system information from suspect system: • Employee Name (if known)  • Hostname  • Operating System with Service Pack (if known)  • System Type (if known)  • Location of Employee  • Employee's Role, Security Clearance and Privilege/access level.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0040</td>
<td>1.30</td>
<td>Set the Priority of the incident</td>
<td>Determine the impact and priority of the incident.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0050</td>
<td>1.40</td>
<td>Determine what assets have been accessed by Individual</td>
<td>Establish what other systems the Insider has had access to and what changes have been made. Record all assets associated with threat.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0060</td>
<td>1.50</td>
<td>Correlate findings</td>
<td>If there is evidence of similar incidents, correlate findings.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0070</td>
<td>2.10</td>
<td>Pull traffic logs of the incident</td>
<td>Acquire all relevant Network logs.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0080</td>
<td>2.20</td>
<td>Establish Threat</td>
<td>Confirm if this is a credible threat to ACME or a False Positive.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
<tr>
<td>IT-0090</td>
<td>3.10</td>
<td>Update ACME Manager</td>
<td>Update ACME Manager on the current state of the investigation. Seek approval for seizure of assets.</td>
<td>Required</td>
<td>ACME: Analyst</td>
</tr>
</tbody>
</table>
## Summary – The Big Picture

### Use Case Elements

<table>
<thead>
<tr>
<th>Objective</th>
<th>Threat</th>
<th>Stakeholder</th>
<th>Data Req.</th>
<th>Logic</th>
<th>Testing</th>
<th>Priority</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose and goal of the procedure</td>
<td>The threat which the logic seeks to identify</td>
<td>Those with responsibility relating to the procedure</td>
<td>Detection Info. sources e.g. logs, packets, host configuration, CTI, etc.</td>
<td>Content rules and filters, etc. to process data and identify threat</td>
<td>Logic validation process to confirm that it addresses the risk</td>
<td>Classification category and level for the threat based on impact and urgency</td>
<td>Workflow when responding to the threat</td>
</tr>
</tbody>
</table>

### Element Descriptions

**Example: Remote Access – C2 Communication**

- **Monitor and alert on web C2 malicious host**
- **Compromised host succumbing to attacker takeover**
- **L1, L2 Analysts SOC Manager, ITOPS**
- **FW, Web Proxy Pinchpoint FPC Context (CMDB, TI feeds)**
- **Reporting Engine; SA ESA Rules**
- **Connect to domain previously added to blacklist**
- **Host: P3 Critical System: P2**
- **Procedure to be followed when C2 is detected**
The Road Ahead

- Consolidate Framework
  - SLAs
  - UC fine tuning and improvement
  - IRPs scalability
  - Threat Indicators
- Create Use Case scenarios (focus on threats)
- Publicise the Framework and establish an industry standard
Benefits of ACD Use Case

- End 2 End Capability
- Granularity
- Adaptable to different platforms (SIEM and IMS)
- Plan on a Page
  - Each Use Case is complete in its own right
Apply What You Have Learned Today

Next week you should:
- Investigate if your organisation already utilises Use Cases
- Highlight any gaps in coverage

In the first three months following this presentation you should:
- Establish your most critical Use Cases and apply Framework

Within six months you should:
- Deploy your Critical Use Cases
- Have a Library of Use Cases and associated IRP’s
- Identify remaining Use Cases requiring deployment
Conclusions

- SOC’s can’t function effectively without properly designed Use Cases.
- A framework provides flexibility but still keeps Use Cases targeted.
- A Use Case is Detection AND Response.
Questions (and thanks for your resiliency 😊)

David.Gray@rsa.com

Angelo.Perniola@rsa.com