RSA® Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: **SOP-W10**

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

#RSAC

So … what’s a Use Case?

What we will talk about

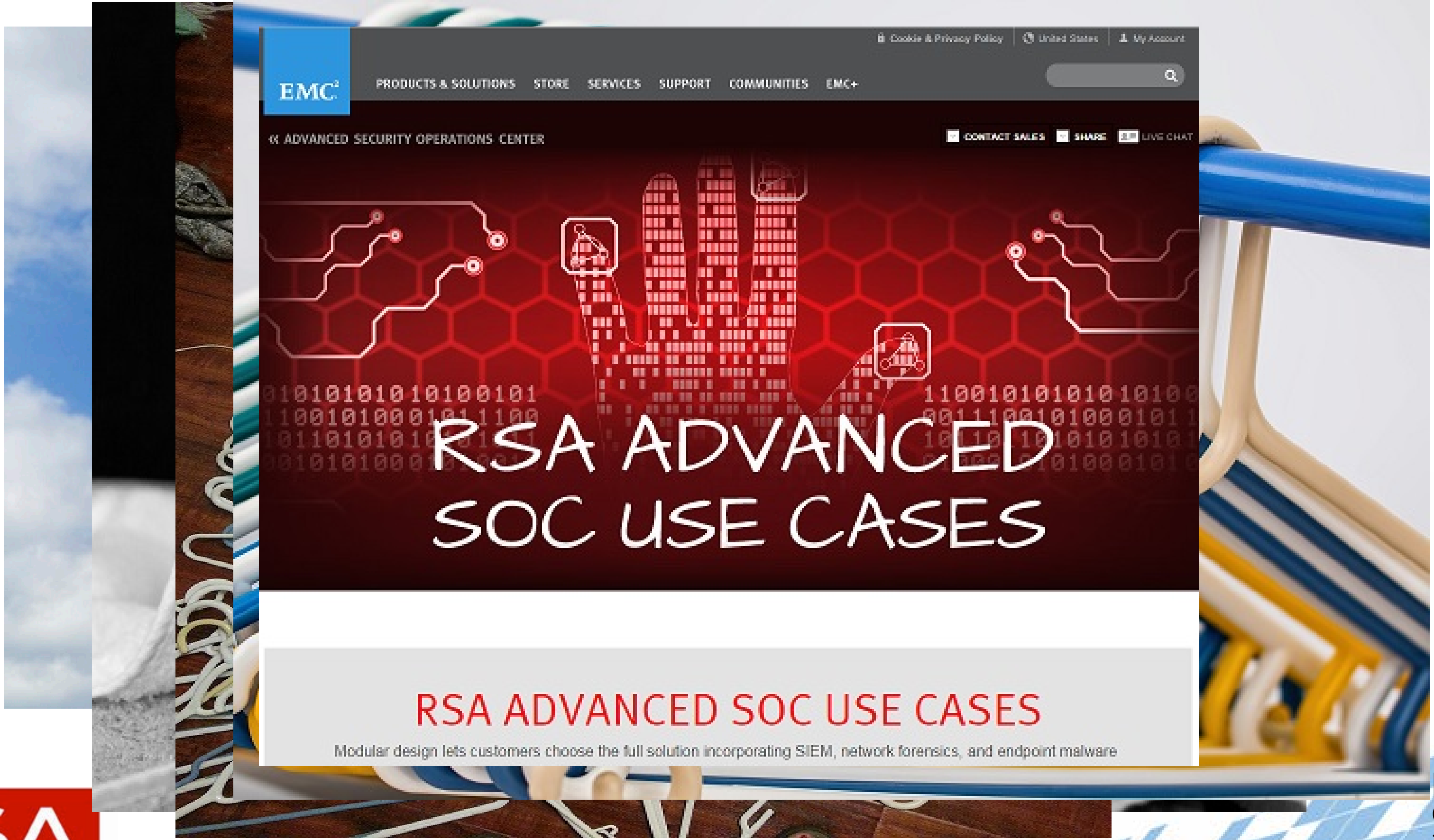
- Context – background and history
- Our solution - “Use Case Framework”
  - Granular walkthrough of each step
- The benefits
- From “huuu?!?” to “yeah!!!”

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**

Context

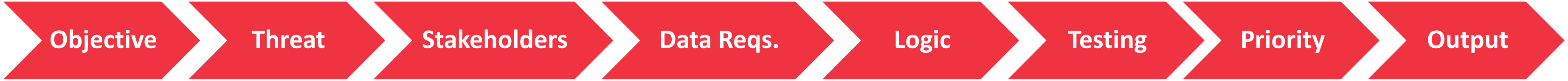


RSA ADVANCED SOC USE CASES

RSA ADVANCED SOC USE CASES

Modular design lets customers choose the full solution incorporating SIEM, network forensics, and endpoint malware

Use Case Framework at a glance



Objective → Threat → Stakeholders → Data Reqs. → Logic → Testing → Priority → Output

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

SOC Manager/ CISO

Incident Coordinator

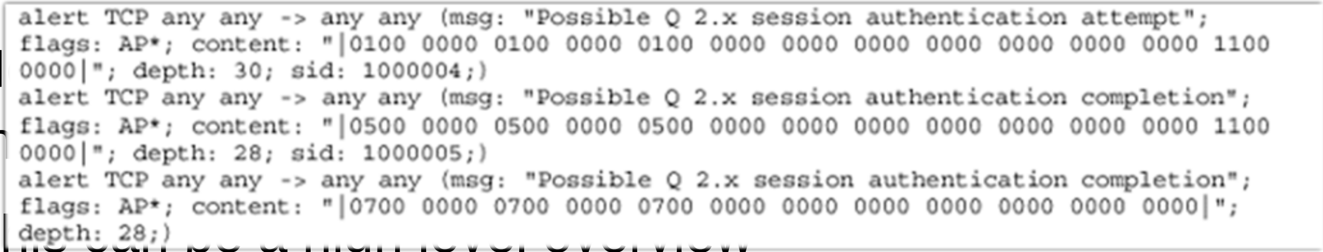
L1/L2 Analyst

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, …)

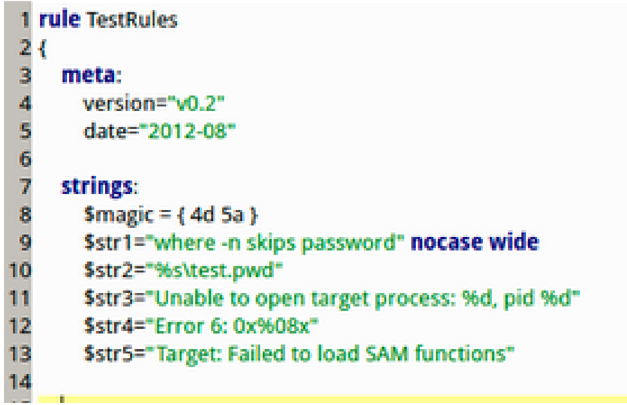
Logic

- H
beh



```
alert TCP any any -> any any (msg: "Possible Q 2.x session authentication attempt";
flags: AP*; content: "|0100 0000 0100 0000 0100 0000 0000 0000 0000 0000 0000 0000 1100
0000|"; depth: 30; sid: 1000004;)
alert TCP any any -> any any (msg: "Possible Q 2.x session authentication completion";
flags: AP*; content: "|0500 0000 0500 0000 0500 0000 0000 0000 0000 0000 0000 0000 1100
0000|"; depth: 28; sid: 1000005;)
alert TCP any any -> any any (msg: "Possible Q 2.x session authentication completion";
flags: AP*; content: "|0700 0000 0700 0000 0700 0000 0000 0000 0000 0000 0000 0000|";
depth: 28;)
```

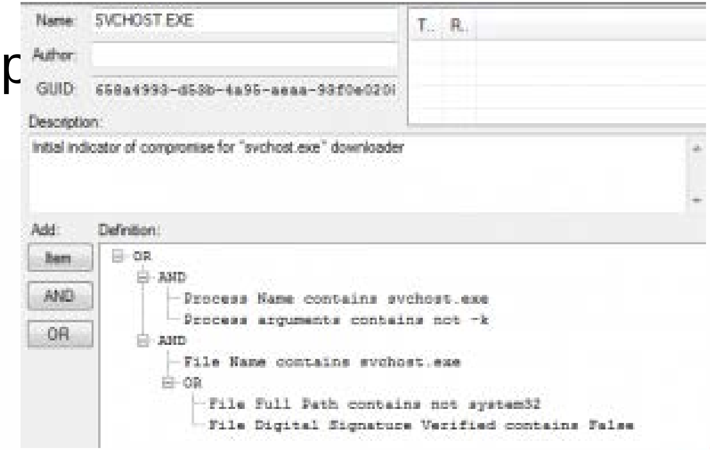
- This can be a high level overview
- M g as sp



```
rule TestRules
{
  meta:
    version="v0.2"
    date="2012-08"

  strings:
    $magic = { 4d 5a }
    $str1="where -n skips password" nocase wide
    $str2="%s\test.pwd"
    $str3="Unable to open target process: %d, pid %d"
    $str4="Error 6: 0x%08x"
    $str5="Target: Failed to load SAM functions"

```



Name: SVCHOST.EXE

Author:

GUID: 658a4993-d58b-4a96-aeaa-93f0e020(

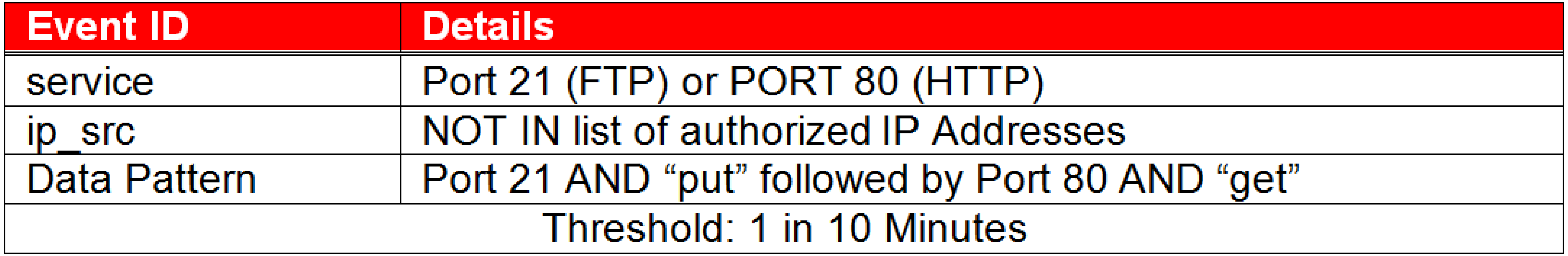
Description:

Initial indicator of compromise for "svchost.exe" downloader

```
OR
  AND
    Process Name contains svchost.exe
    Process arguments contains not -k
  AND
    File Name contains svchost.exe
    OR
      File Full Path contains not system32
      File Digital Signature Verified contains False
```

Logic [cont.]

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



Event ID	Details
service	Port 21 (FTP) or PORT 80 (HTTP)
ip_src	NOT IN list of authorized IP Addresses
Data Pattern	Port 21 AND “put” followed by Port 80 AND “get”
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

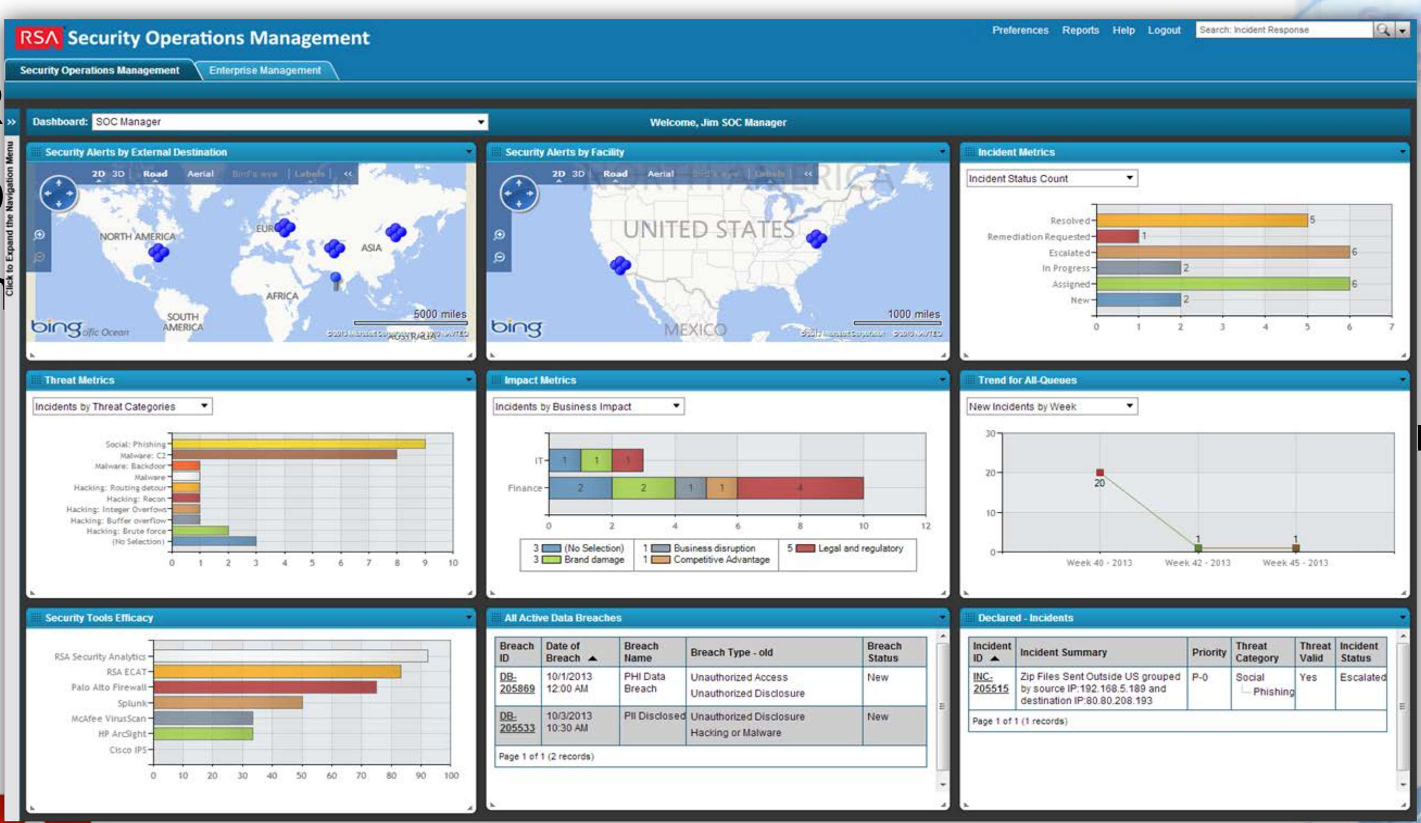
- How we know the Logic will produce a (reliable) alert
- Key to validating the Content Rules
- Should be tested first in a QA environment before being tested on a live network (with benign traffic)
- Results should be fed back into the Logic to ensure the greatest degree of confidence is achieved

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

- R
- D
- In
  -
  - nd what



All Active Data Breaches

Breach ID	Date of Breach ▲	Breach Name	Breach Type - old	Breach Status
DB-205869	10/1/2013 12:00 AM	PHI Data Breach	Unauthorized Access Unauthorized Disclosure	New
DB-205533	10/3/2013 10:30 AM	PII Disclosed	Unauthorized Disclosure Hacking or Malware	New

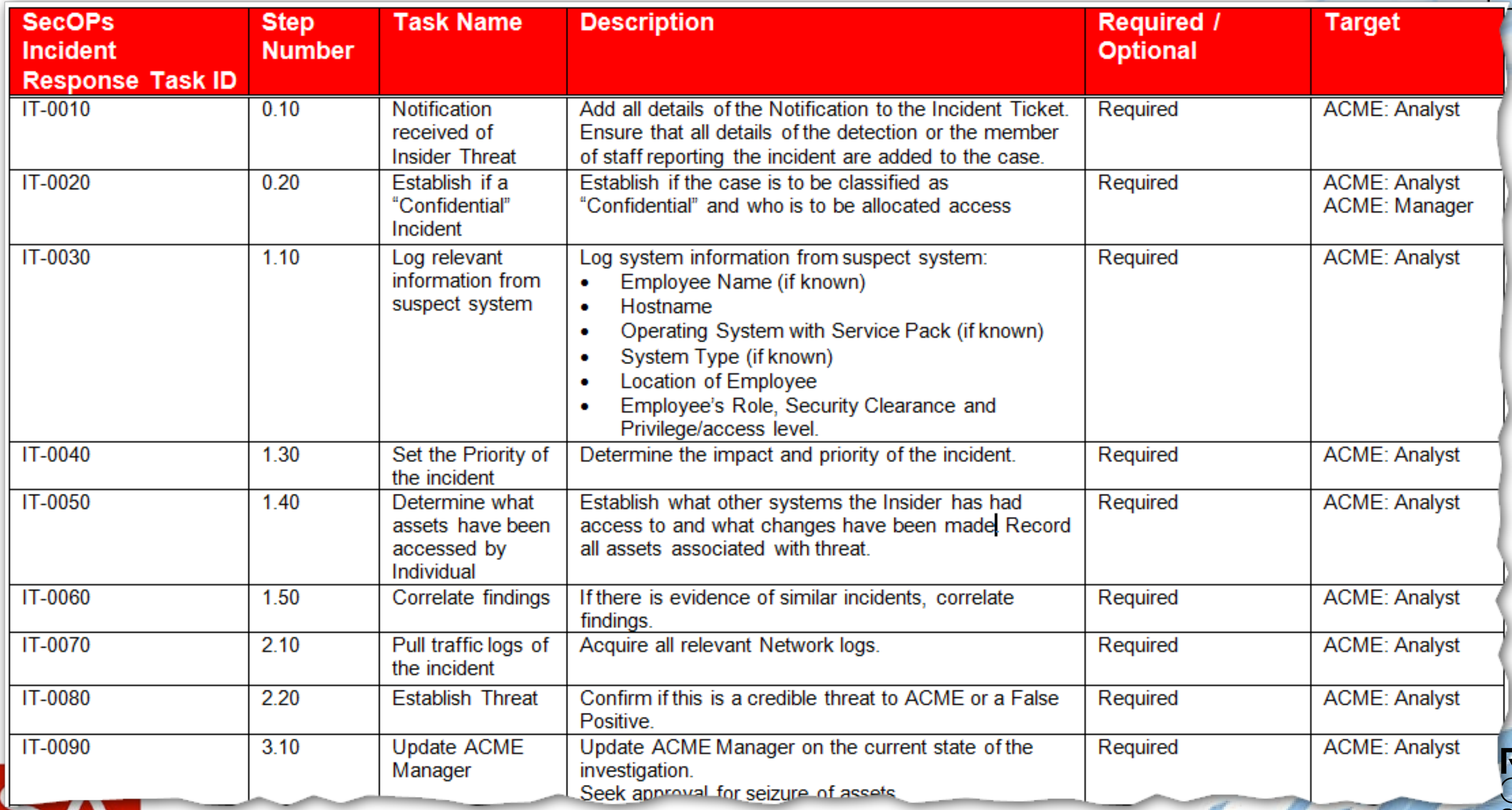
Page 1 of 1 (2 records)

Declared - Incidents

Incident ID ▲	Incident Summary	Priority	Threat Category	Threat Valid	Incident Status
INC-205515	Zip Files Sent Outside US grouped by source IP:192.168.5.189 and destination IP:80.80.208.193	P-0	Social Phishing	Yes	Escalated

Page 1 of 1 (1 records)

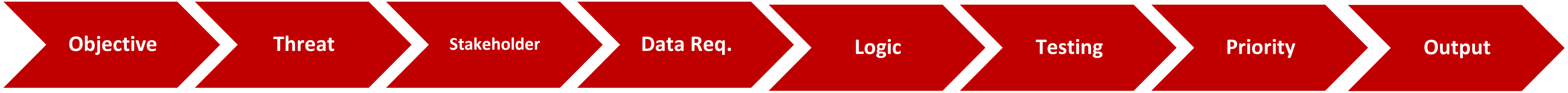
Workflow/Procedural Steps



SecOPs Incident Response Task ID	Step Number	Task Name	Description	Required / Optional	Target
IT-0010	0.10	Notification received of Insider Threat	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.	Required	ACME: Analyst
IT-0020	0.20	Establish if a "Confidential" Incident	Establish if the case is to be classified as "Confidential" and who is to be allocated access	Required	ACME: Analyst ACME: Manager
IT-0030	1.10	Log relevant information from suspect system	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.	Required	ACME: Analyst
IT-0040	1.30	Set the Priority of the incident	Determine the impact and priority of the incident.	Required	ACME: Analyst
IT-0050	1.40	Determine what assets have been accessed by Individual	Establish what other systems the Insider has had access to and what changes have been made Record all assets associated with threat.	Required	ACME: Analyst
IT-0060	1.50	Correlate findings	If there is evidence of similar incidents, correlate findings.	Required	ACME: Analyst
IT-0070	2.10	Pull traffic logs of the incident	Acquire all relevant Network logs.	Required	ACME: Analyst
IT-0080	2.20	Establish Threat	Confirm if this is a credible threat to ACME or a False Positive.	Required	ACME: Analyst
IT-0090	3.10	Update ACME Manager	Update ACME Manager on the current state of the investigation. Seek approval for seizure of assets	Required	ACME: Analyst

Summary – The Big Picture

Use Case Elements



Element Descriptions

Purpose and goal of the procedure	The threat which the logic seeks to identify	Those with responsibility relating to the procedure	Detection Info. sources e.g. logs, packets, host configuration, CTI, etc.	Content rules and filters, etc. to process data and identify threat	Logic validation process to confirm that it addresses the risk	Classification category and level for the threat based on impact and urgency	Workflow when responding to the threat

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
  designe
- A frame
  Cases
- A Use C

RSA Conference 2015
Abu Dhabi

Questions (and thanks for your resiliency ☺)

David.Gray@rsa.com

Angelo.Perniola@rsa.com