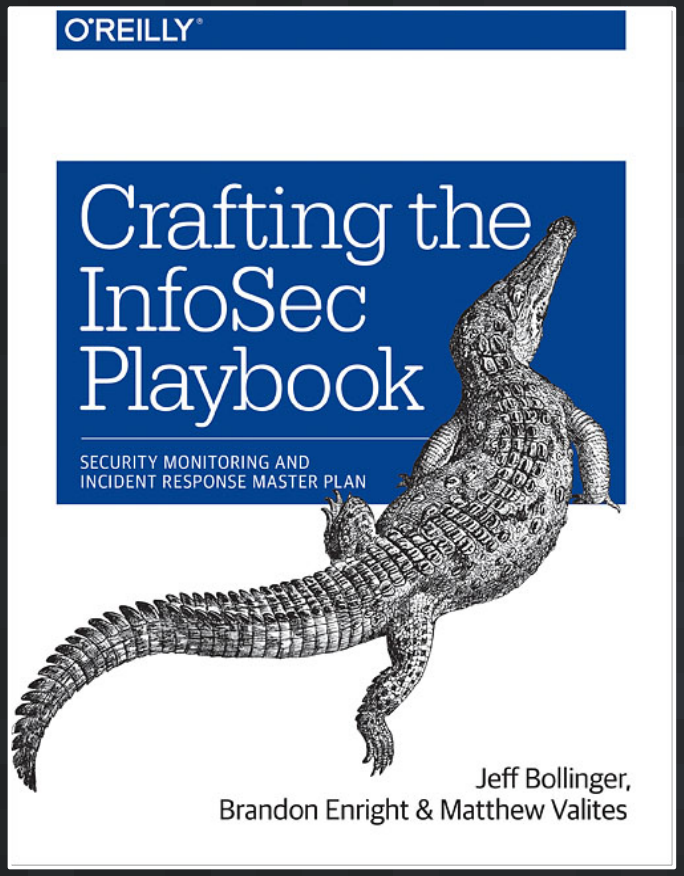
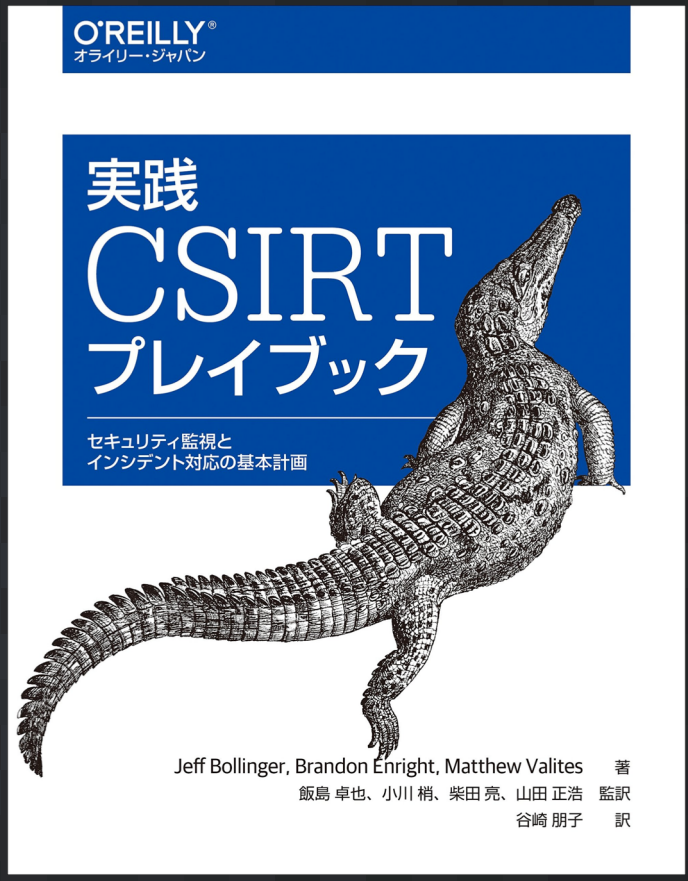
The Right Data At the Right Time

Jeff Bollinger | @jeffbollinger
Matt Valites | @matthewvalites

SANS SIEM Summit 2019


O'REILLY
Crafting the InfoSec Playbook
SECURITY MONITORING AND INCIDENT RESPONSE MASTER PLAN
Jeff Bollinger,
Brandon Enright & Matthew Valites


O'REILLY
オライリー・ジャパン
実践
CSIRT
プレイブック
セキュリティ監視と
インシデント対応の基本計画
Jeff Bollinger, Brandon Enright, Matthew Valites 著
飯島 卓也、小川 梢、柴田 亮、山田 正浩 監訳
谷崎 朋子 訳

Amsterdam 2020 FIRST Technical Colloquium

Amsterdam (NL), April 6th-8th, 2020

Is there an ideal set of data sources for Security Monitoring & Incident Response?

NETWORK

NETWORK SECURITY MONITORING

- IDS
- DNS
- Web
- NetFlow | Firewall Logs
- Email
- Remote Access
- Vulnerability Management

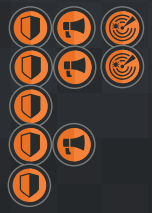
Detect
Prevent
Respond

HOSTED SERVICES

- Account Behavior
- Web App Firewall
- IaaS Logs
- Web & App Server Logs
- Custom App Logs

ENDPOINT

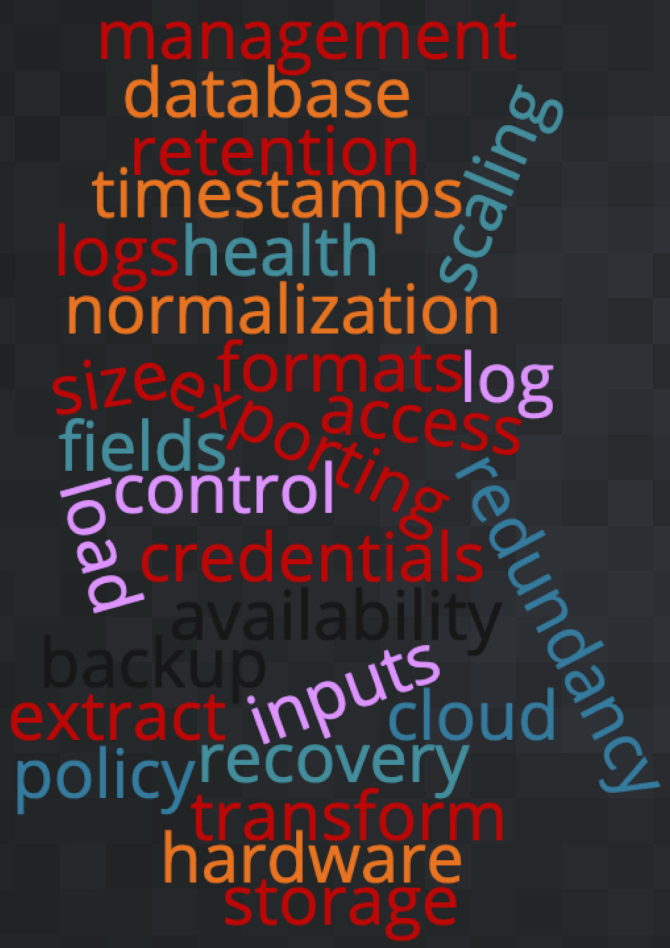
- Detection & Response Agent
- Anti-Virus
- Authentication & Access
- OS Logs



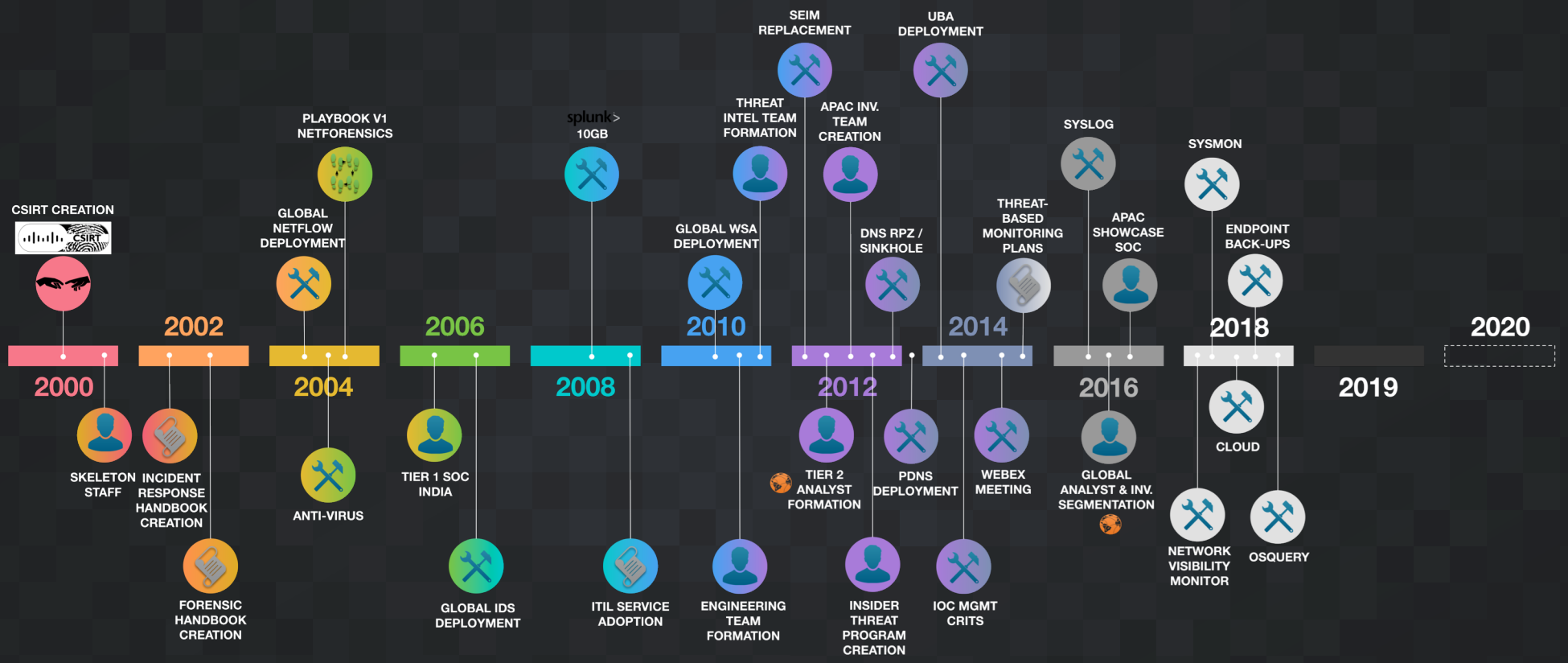
INFRASTRUCTURE

- Authentication & Access
- Active Directory
- Mobile Device Management
- ‘Data’

Capability Dependencies



Weaponizing Detection



Security Capabilities

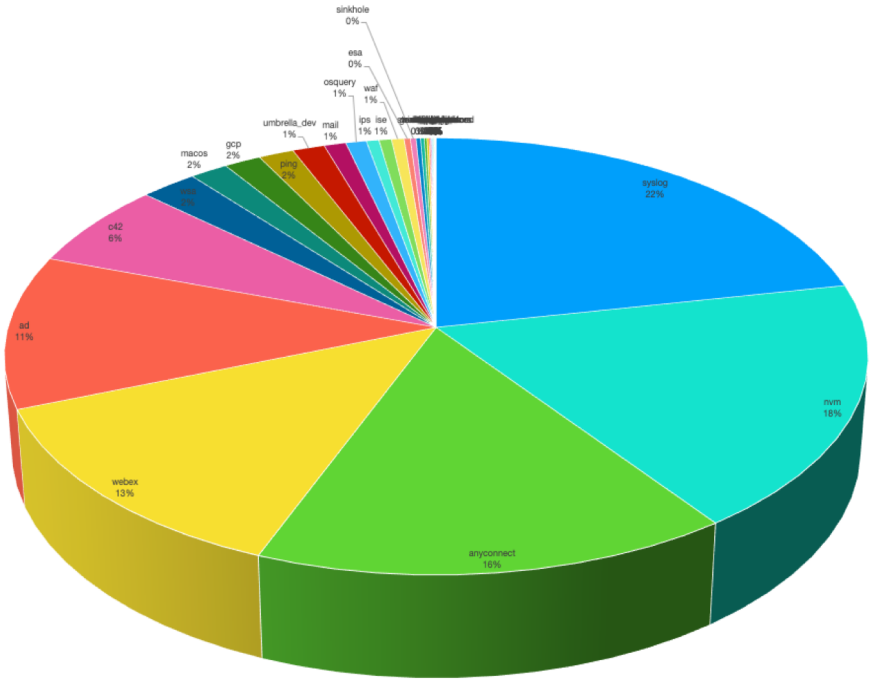
Visibility

e.g. Attribution

Control

e.g. Prevention

From Data to Detection

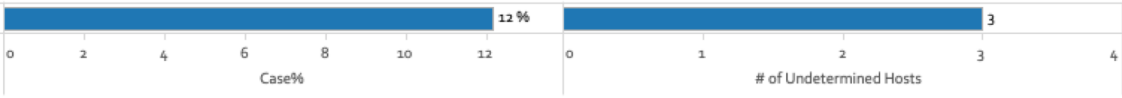


Top 10 Playbook Reports

Index	Playbook Title	
1	830167:Tier1:Non-Approved application installation/Execution on the servers	28
2	830171: Tier2: Monitoring Non-Admin Account Logon Activity	20
3	830174:Tier2: Monitoring Shared Folders on Tier1 Servers Accessed Remotely	18
4	810002: Data Exfil Ports	14
5	300142: TLP GREEN URL IOC	10
6	600030: Unable to Clean Threat	10
7	110037: SMB Attacks	8
8	110044: Coinminer Activity	8
9	830160:Tier1: Monitoring Shared Folders on Tier1 Servers Accessed Remotely	8
10	830166:Tier1: Application Crashes	8

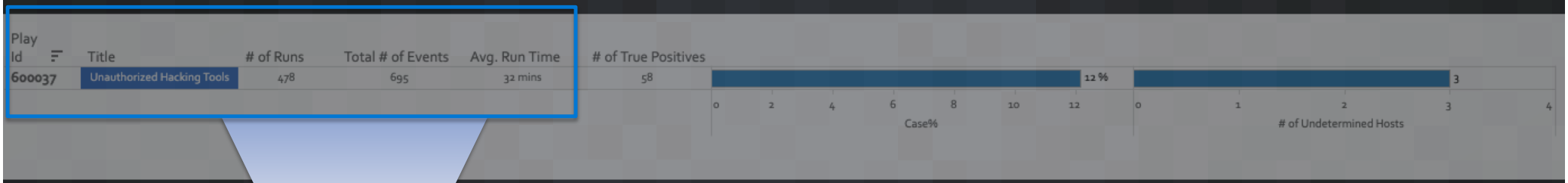
From Data to Detection

Play Id	Title	# of Runs	Total # of Events	Avg. Run Time	# of True Positives
600037	Unauthorized Hacking Tools	478	695	32 mins	58



From Data to Detection

Play Details

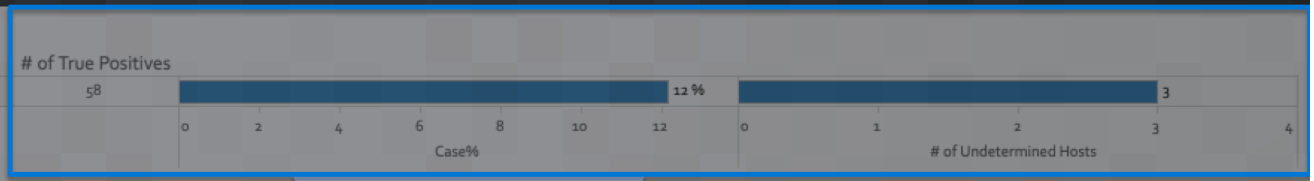


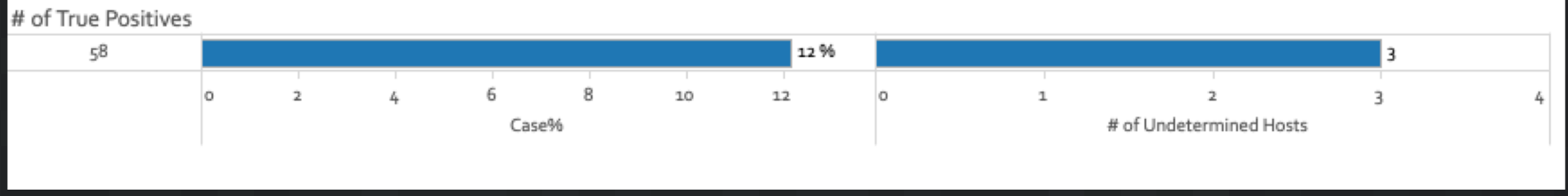
Title	# of Runs	Total # of Events	Avg. Run Time
Unauthorized Hacking Tools	478	695	32 mins

From Data to Detection

Result Details

Play Id	Title	# of Runs	Total # of Events	Avg. Run Time	# of True Positives
600037	Unauthorized Hacking Tools	478	695	32 mins	58





ANALYST PLAYBOOK OVERVIEW

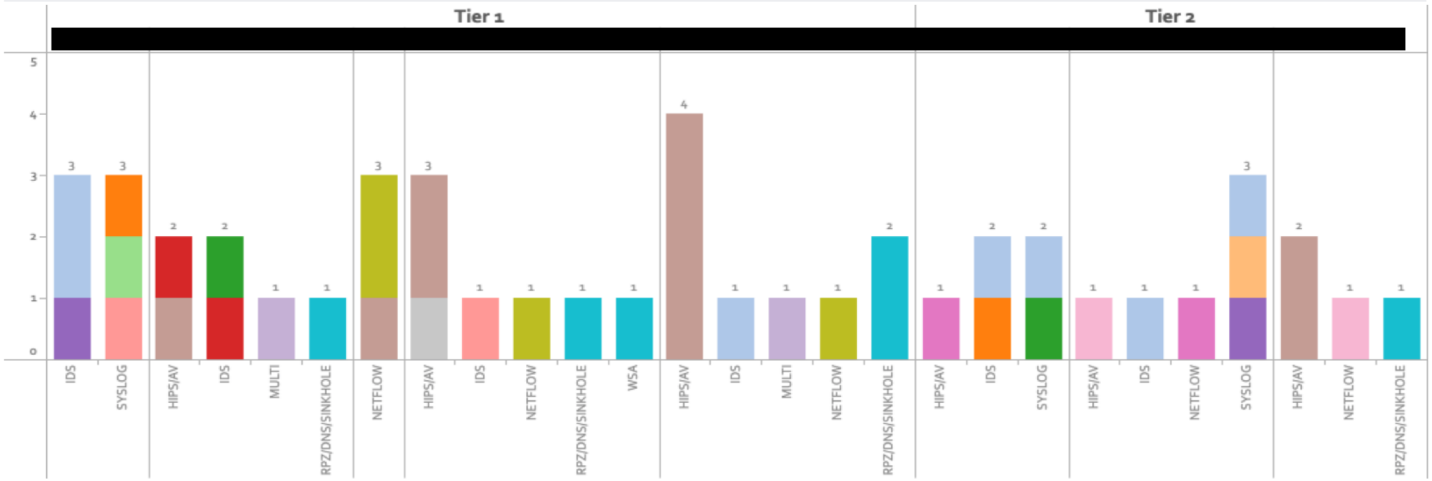
INITIAL DATE: Last 3 months

AGENT: (Multiple values)

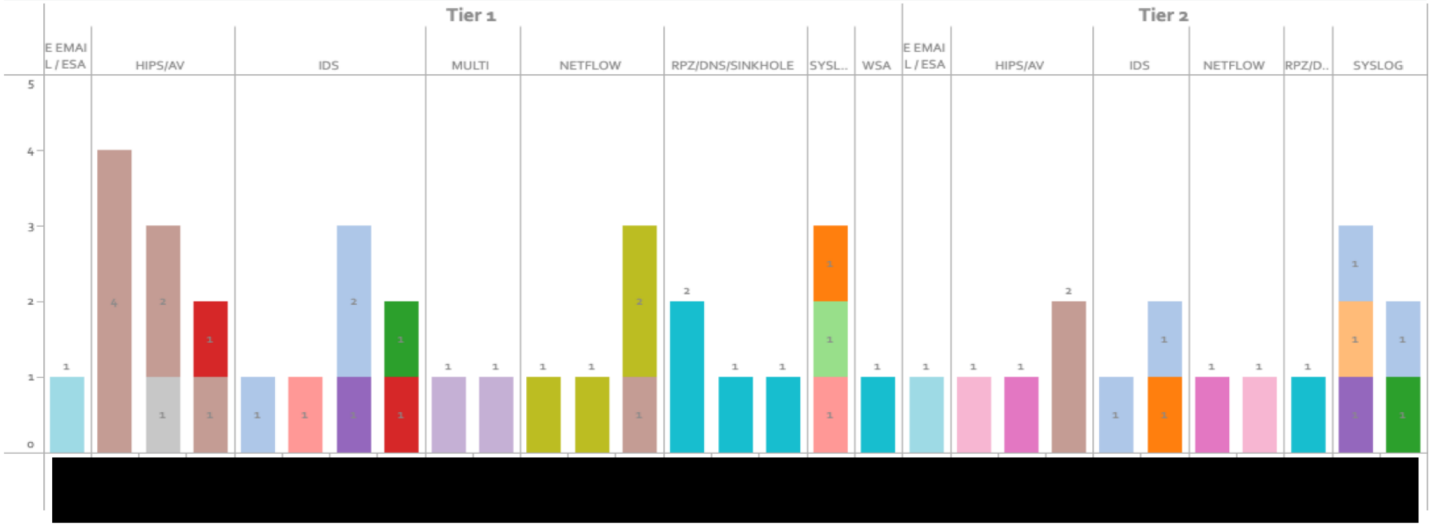
PLAYBOOK INCIDENTS BY MONTH

		Jul-2019	Aug-2019	Sep-2019
HIPS/AV	600030		●	●
	600051	●		
	600116		●	
	600133	●	●	●
	610002	●	●	●
	610007	●		●
	610008			●
	610012			●
	610017		●	
IDS	110004	●		●
	110044	●	●	●
	110051			●
	110127			●
	110128		●	
	110129			●
NETFLOW	200005	●		●
	200025			●
	200047		●	
	200048		●	
	200313		●	
RPZ/DNS/SINKHOLE	700024	●	●	●
SYSLOG	800040	●		●
	830038			●
	860005		●	
	860006	●		
	860011	●		
	870003			●
	870008			●
WSA	300110		●	

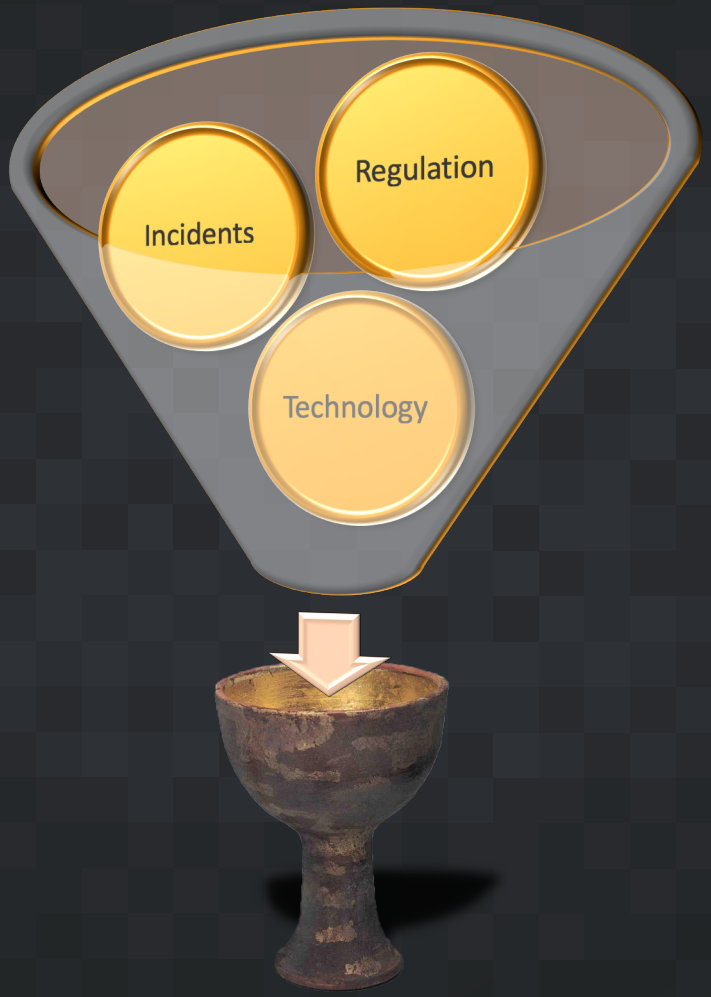
PLAYBOOK INCIDENTS OPENED BY AGENT



AGENT INCIDENTS WORKED BY PLAYBOOK



Data Drivers



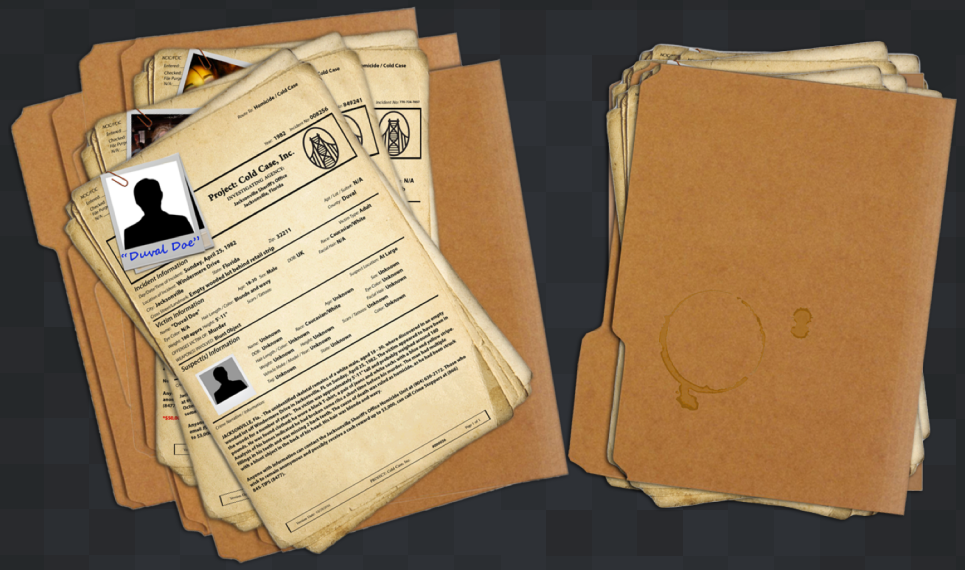
Case Study 1

Unique data source cracks the case of the malicious insider

The Alert

Aware employee sees something and says something

The Case



Credential abuse + private documents viewed without authorization

The Investigation

Investigators, exhausting available data,
establish a motive but lack a smoking gun

The Breakthrough

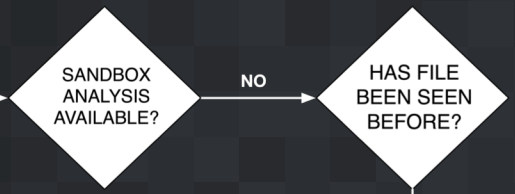
A new data source captures forensic endpoint artifacts

Waste not Want not

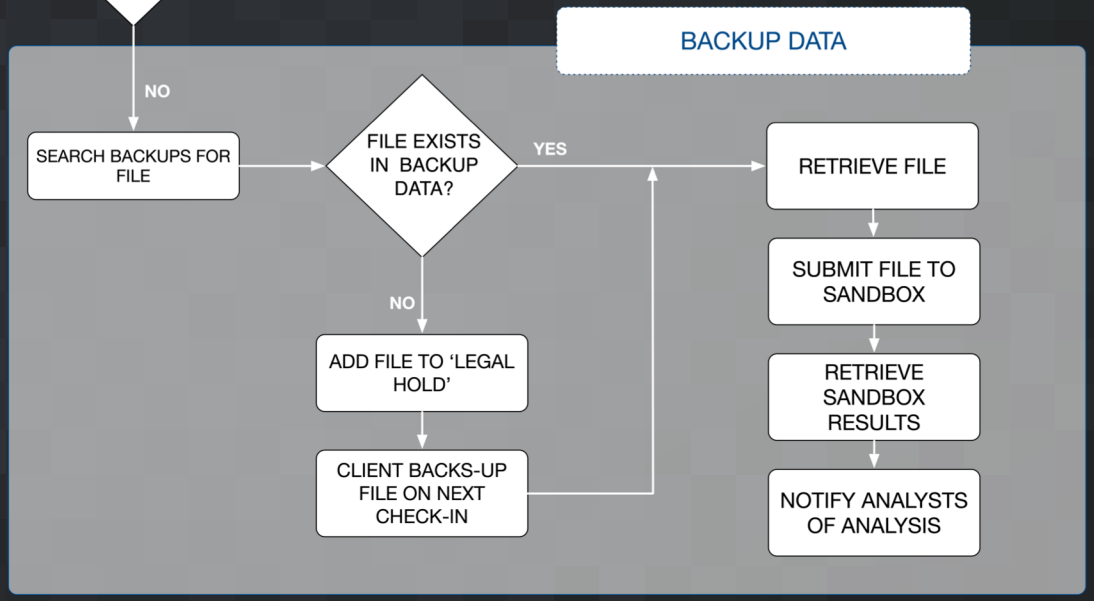
860005-INV-AUTORUNS-MALWARE: Detection of emerging Hashes which ImagePath is not signed

860006-INV-AUTORUNS-MALWARE: Detection of suspicious Microsoft and Google program which ImagePath is not signed

860004-INV-AUTORUNS-MALWARE: Detection of suspicious Windows component launched from unusual location



AUTOMATED FILE ACQUISITION AND ANALYSIS

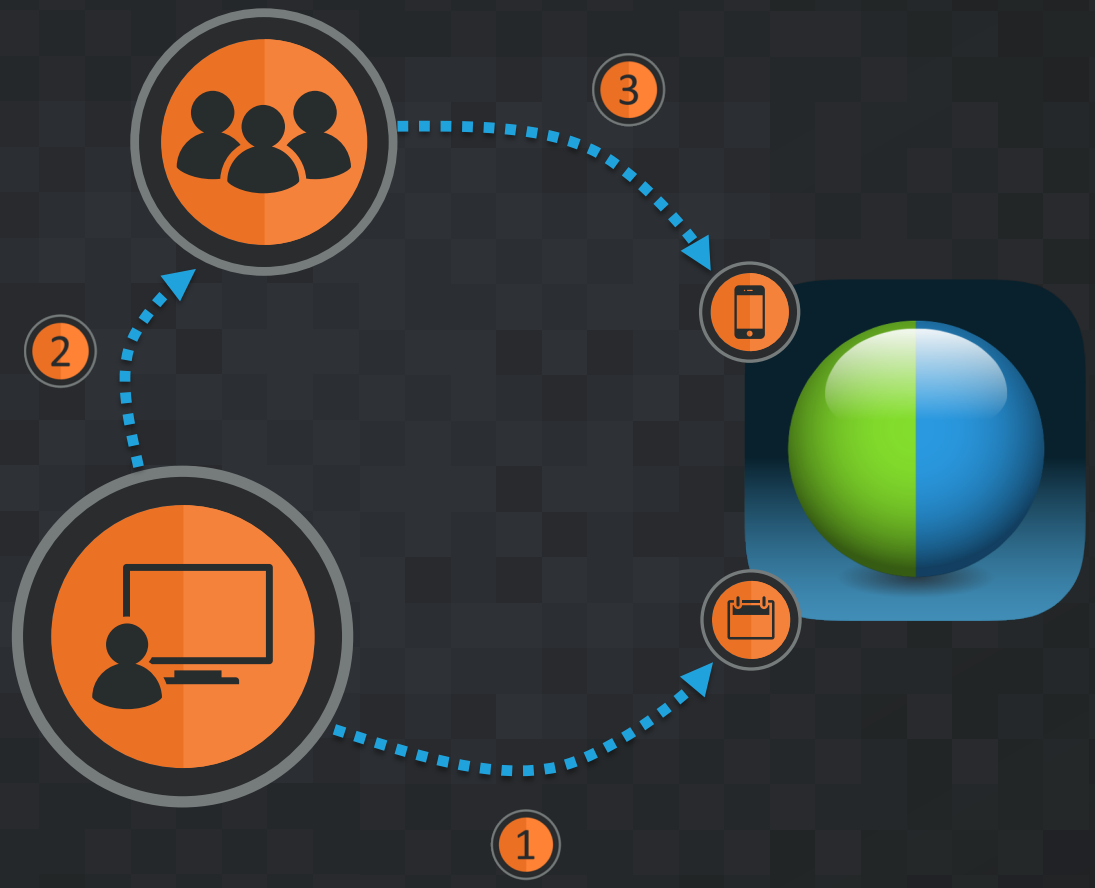


Case Study 2

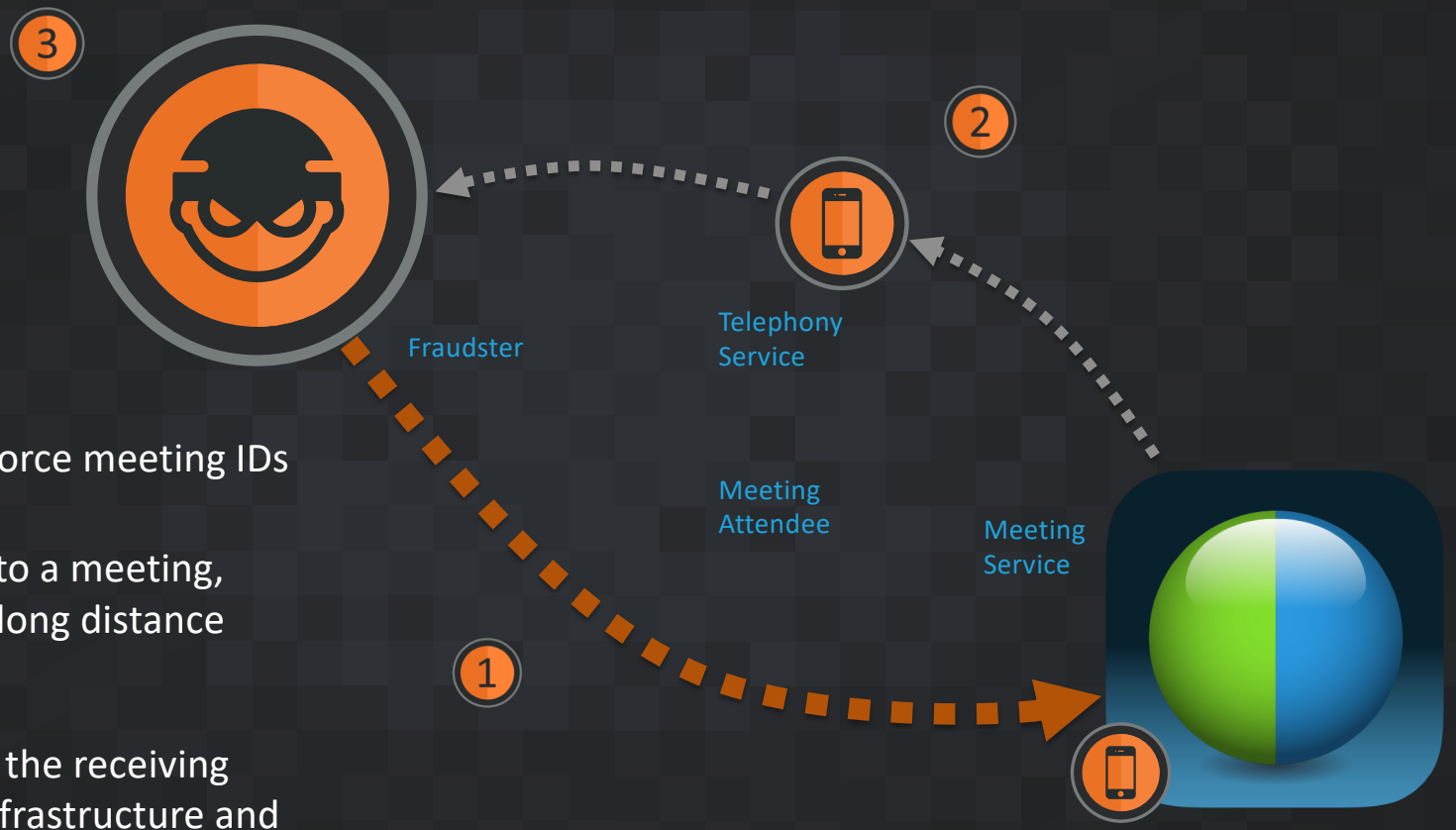
Application data identifies hosted service fraud

How It's Supposed To Work

1. Web conference host schedules a meeting
2. Host distributes unique meeting ID to attendees
3. Attendees connect into meeting with meeting ID on phones and computers



How it Worked



1. Attackers brute force meeting IDs
2. Once connected to a meeting, attackers 'invite' long distance attendees to join
3. Attackers control the receiving toll-generating infrastructure and profit from long distance calls

Incident -> Data -> Detection

```
index=webex _index_earliest="03/07/2019:12:00:00" _index_latest="03/08/2019:00:00:00" earliest="0" latest="1999999999" (sourcetype=access_log OR sourcetype=error_log) "j.php?MTID=" http_status=200
| rex "MTID=%*(?<MT_ID>\w*)"
| stats earliest(_time) AS FirstEvent, latest(_time) AS LastEvent, dc(MT_ID) as MTID_count, values(siteurl) as client,values(MT_ID) as MTID by m_ip
| convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime(FirstEvent), ctime(LastEvent)
| rename m_ip as src_ip
| eval MTID=if(mvcount(MTID) > 10, mvappend(mvindex(MTID,0,10), "[...]"), MTID)
| where MTID_count > 150
| sort -MTID_count
```

✓ 54,418 events (9/24/18 10:49:35.000 AM to 5/18/33 3:33:19.000 AM) No Event Sampling ▾ Job ▾

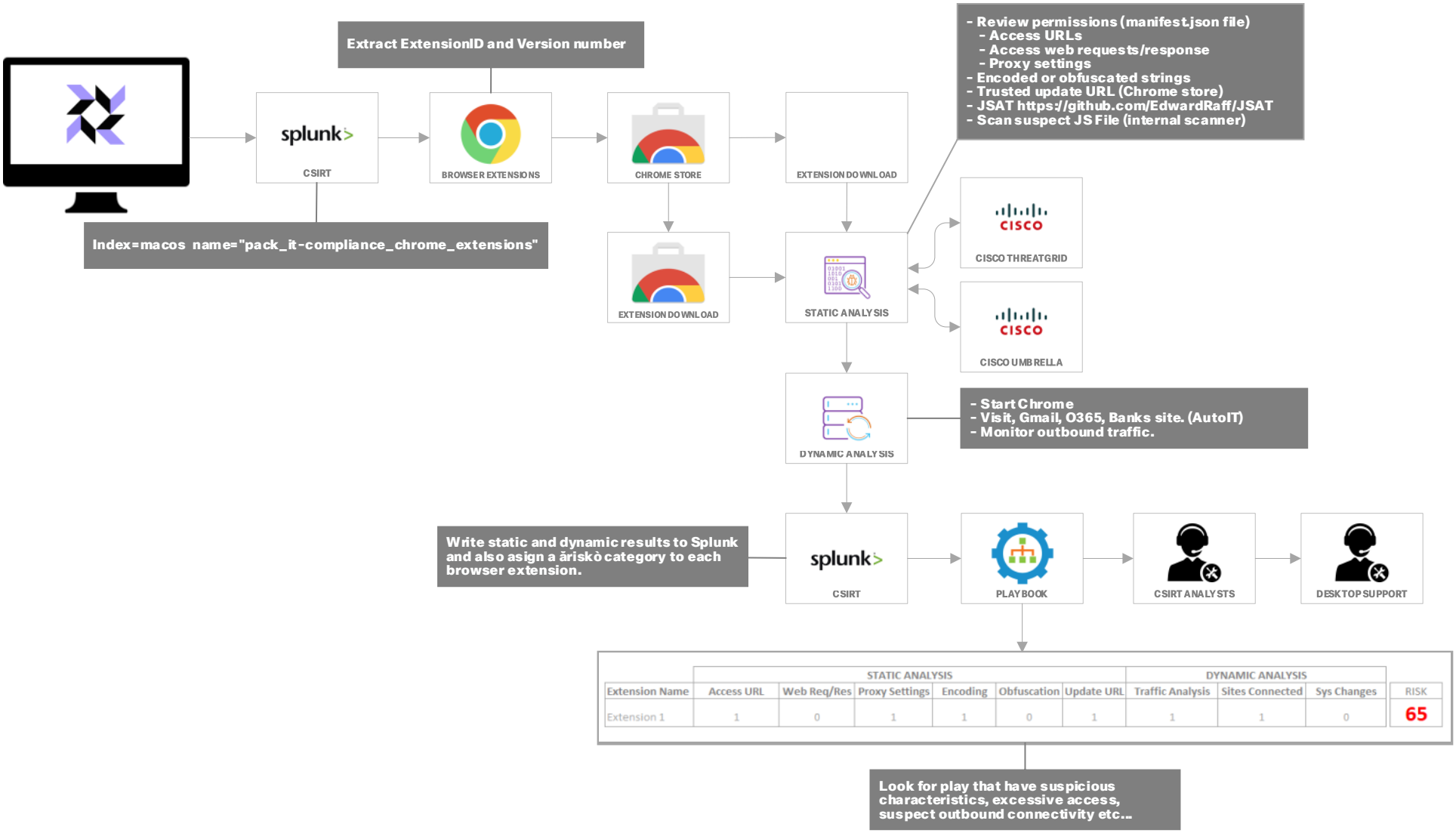
Events (54,418) Patterns **Statistics (1)** Visualization

10 Per Page ▾ Format Preview ▾

	src_ip	FirstEvent	LastEvent	MTID_count	client	MTID
1	[redacted]	03/07/2019 12:55:21 GMT	03/07/2019 22:31:03 GMT	151	[redacted]	m03bf850aa466796be847a1ad72002a77 m03d06319b6892d999832d4ddc98999c1 m0451472e89952808e72aa057c7b11842 m072edd550f626c2562f21c41b74125b7 m07637571f80ac663b3ada9d9928209d4 m0a468c550c7a6489695b41c33201e637 m0c32999973f7f4d4a3ad22152aaa716c m0eeb4af5d6585850c9f177661c78b1f6 m0fe5422e5b0acc4b06fab46cb23140ff m144c7a3dc3c3173de60b6f4e55e6f8e6 m160b4854382255ad51e6658651a7789a [...]

Case Study 3

Make your own data


Extract ExtensionID and Version number
splunk>
CSIRT
BROWSER EXTENSIONS
CHROME STORE
EXTENSION DOWNLOAD
- Review permissions (manifest.json file)
- Access URLs
- Access web requests/response
- Proxy settings
- Encoded or obfuscated strings
- Trusted update URL (Chrome store)
- JSAT https://github.com/EdwardRaff/JSAT
- Scan suspect JS File (internal scanner)
Index=macos name="pack_it-compliance_chrome_extensions"
EXTENSION DOWNLOAD
STATIC ANALYSIS
CISCO
CISCO THREATGRID
CISCO
CISCO UMBRELLA
DYNAMIC ANALYSIS
- Start Chrome
- Visit, Gmail, O365, Banks site. (AutoIT)
- Monitor outbound traffic.
Write static and dynamic results to Splunk and also asign a ăriskò category to each browser extension.
splunk>
CSIRT
PLAYBOOK
CSIRT ANALYSTS
DESKTOP SUPPORT
STATIC ANALYSIS
DYNAMIC ANALYSIS
Extension Name
Access URL
Web Req/Res
Proxy Settings
Encoding
Obfuscation
Update URL
Traffic Analysis
Sites Connected
Sys Changes
RISK
Extension 1
1
0
1
1
0
1
1
1
0
65
Look for play that have suspicious characteristics, excessive access, suspect outbound connectivity etc...

Case Study 4

Trends in computing require adapting capabilities

Technology Trends

Cloud adoption

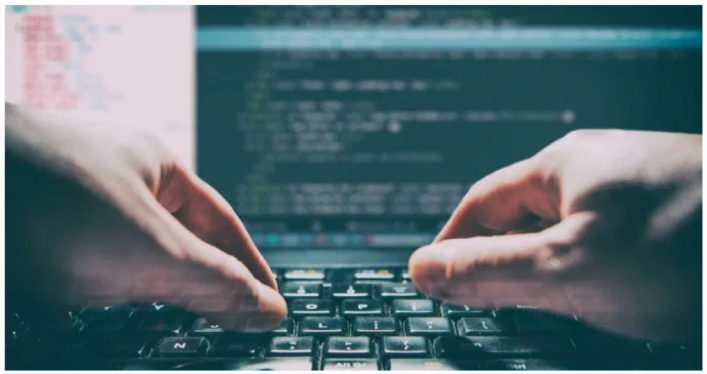
Borderless

Containers

Thousands of API and cryptographic keys leaking on GitHub every day

25 MAR 2019 10

Data loss, Privacy, Security threats



Previous: Update now! WordPress hackers target Easy ... Next: Medtronic cardiac implants can be hacked, FDA is...

by Danny Bradbury

Researchers have found that one of the most popular source code repositories in the world is still housing thousands of publicly accessible encryption keys.

Over 100,000 code repositories on source code management site GitHub contain secret access keys that can give attackers privileged access to those repositories (repos) or to online service providers' services.

Researchers at North Carolina State University (NCSU) scanned almost 13% of GitHub's public repositories over nearly six months. In a paper revealing the findings, they said:

> *We find that not only is secret leakage pervasive – affecting over 100,000 repositories – but that thousands of new, unique secrets are leaked every day.*

The credentials that developers routinely publish on their GitHub repos fall into several categories. These include SSH keys, which are digital certificates that automatically unlock online resources. Another is application programming interface (API) keys (also known as tokens). These are digital keys that enable developers to access online services ranging from Twitter to Google Search directly from their programs. The researchers found a mixture of these keys for services including Google,

A shared responsibility model where nobody is responsible…

https://nakedsecurity.sophos.com/2019/03/25/thousands-of-coders-are-leaving-their-crown-jewels-exposed-on-github/

Technology Trends

Cloud adoption

- Cloud Native
- OSquery

Borderless

- MDM
- IDM
- EDR

Containers

- FluentD
- Datadog

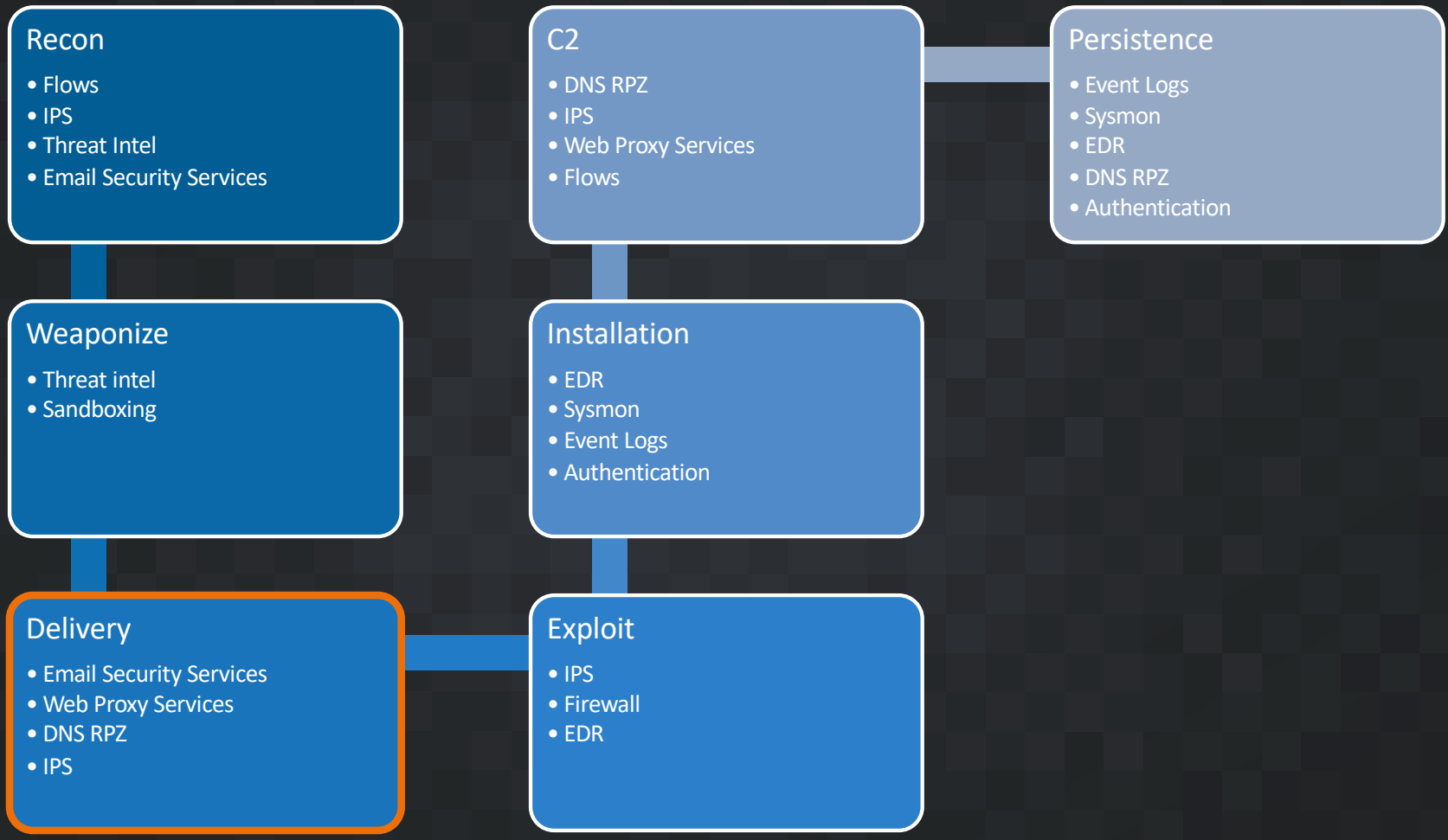
AWS Tenant Monitoring Plan

Type	Color	Meaning
Informational		This type of play provides numbers/statistics and other kind of information
Best Practice Violation		This type of play detects when a best practice is not followed
IR/Analysis Required		This type of play might require further analysis/tuning if investigative in nature or straight IR if high fidelity
Undefined		Either does not belong to any of the above or is still WIP

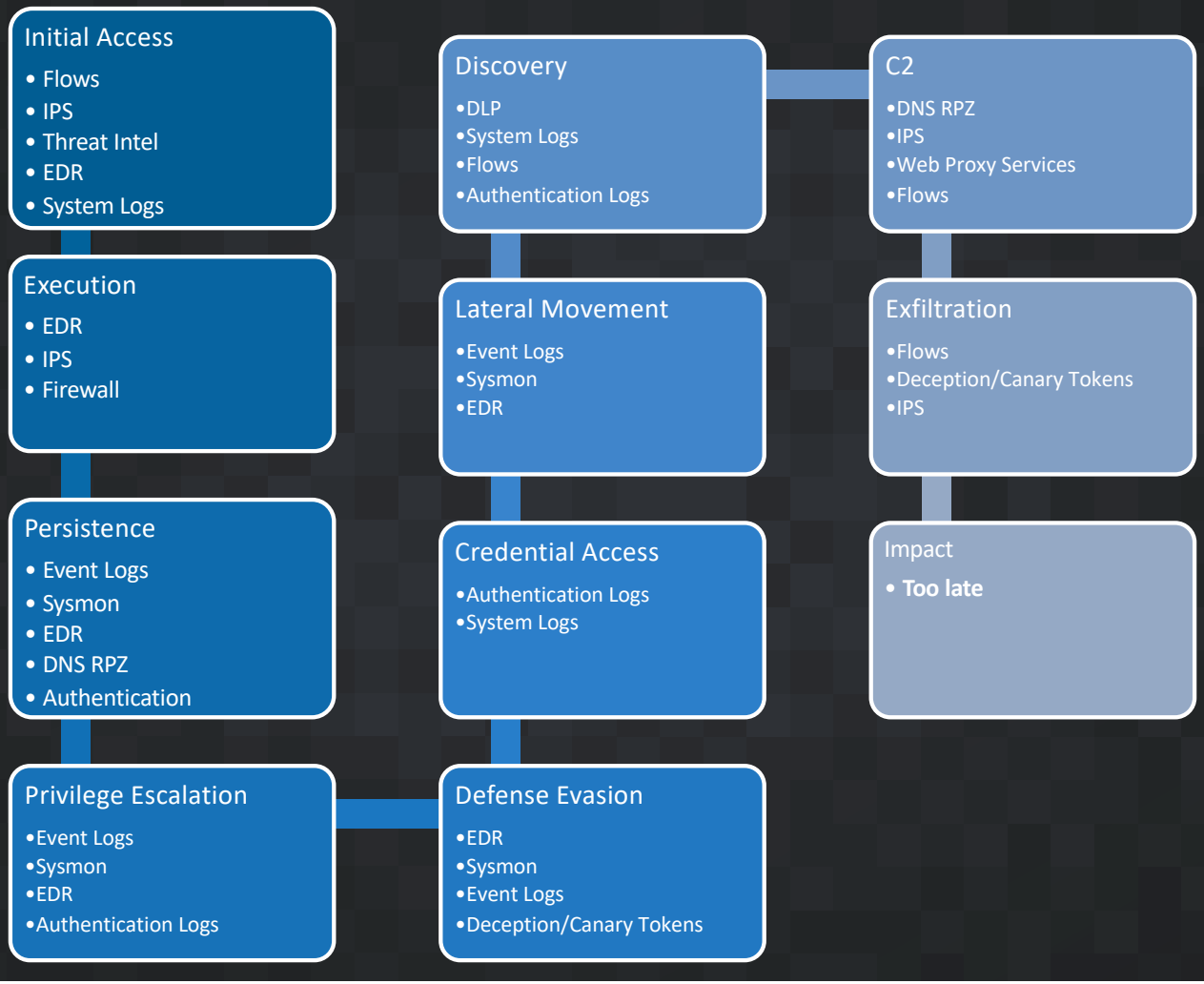
Threat	Detection Method/Objective	Data Source	Example Plays	Type of Play
Account abuse Unauthorized access Improper usage	AWS Root Signin	AWS CloudTrail	810000-HF-AWS-CloudTrail: Root Sign In	
	AWS IAM Accounts without MFA	AWS CloudTrail	810001-HF-AWS-CloudTrail: Users Without MFA	
	AWS Network Events	AWS CloudTrail	810033-INV-AWS-CloudTrail: Network Events	
	AWS Disabled / Deleted MFA	AWS CloudTrail	810007-HF-AWS-CloudTrail: MFA Disabled / Deleted	
	AWS Specific Infrastructure Events	AWS CloudTrail	810010-HF-AWS-CloudTrail: AWS Specific Infrastructure Events	
	AWS Console Login Events	AWS CloudTrail	810030-INV-AWS-CloudTrail: Login Events	
	AWS Secondary Key Creation for IAM Users	AWS CloudTrail	In Progress	
	AWS EC2 Instance Launched by Role	AWS CloudTrail	810006-HF-AWS-CloudTrail: EC2 Instance Launched by Role	
	AWS Unapproved AMI Launch	AWS CloudTrail	In Progress	
	AWS Encryption of CloudTrail Logs	AWS CloudTrail	In Progress	
	AWS Typosquatting events for IAM or EC2	AWS CloudTrail	In Progress	

Tying it all together

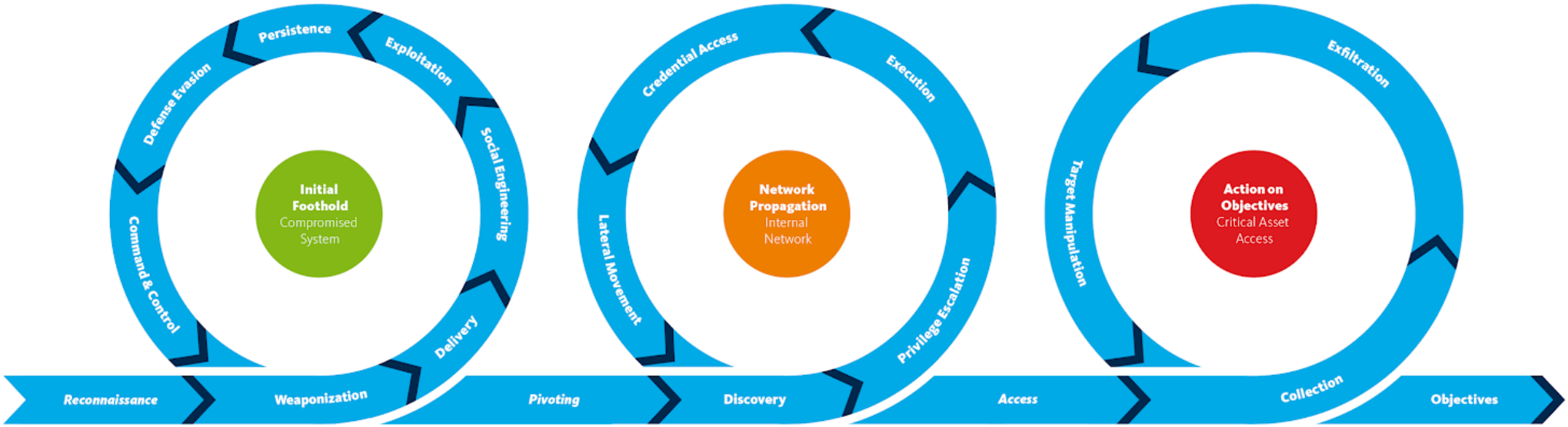
Kill Chain


Recon
• Flows
• IPS
• Threat Intel
• Email Security Services
C2
• DNS RPZ
• IPS
• Web Proxy Services
• Flows
Persistence
• Event Logs
• Sysmon
• EDR
• DNS RPZ
• Authentication
Weaponize
• Threat intel
• Sandboxing
Installation
• EDR
• Sysmon
• Event Logs
• Authentication
Delivery
• Email Security Services
• Web Proxy Services
• DNS RPZ
• IPS
Exploit
• IPS
• Firewall
• EDR

ATT&CK


Initial Access
• Flows
• IPS
• Threat Intel
• EDR
• System Logs
Execution
• EDR
• IPS
• Firewall
Persistence
• Event Logs
• Sysmon
• EDR
• DNS RPZ
• Authentication
Privilege Escalation
•Event Logs
•Sysmon
•EDR
•Authentication Logs
Discovery
•DLP
•System Logs
•Flows
•Authentication Logs
Lateral Movement
•Event Logs
•Sysmon
•EDR
Credential Access
•Authentication Logs
•System Logs
Defense Evasion
•EDR
•Sysmon
•Event Logs
•Deception/Canary Tokens
C2
•DNS RPZ
•IPS
•Web Proxy Services
•Flows
Exfiltration
•Flows
•Deception/Canary Tokens
•IPS
Impact
• Too late

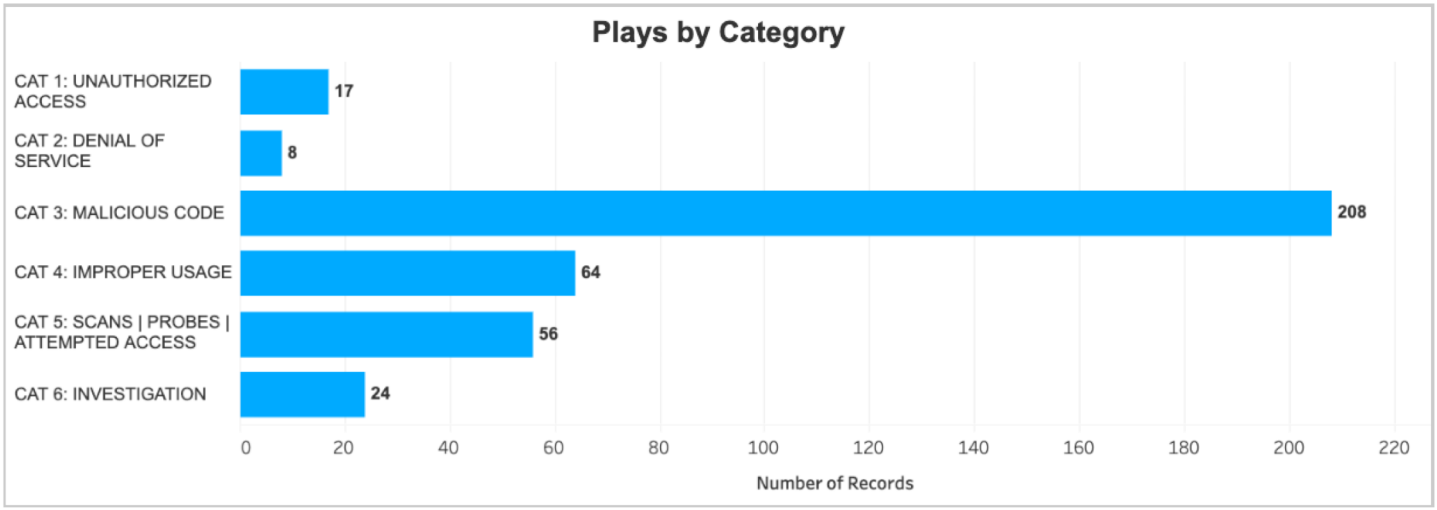
“The observation that attack phases can be bypassed affects defensive strategies fundamentally, as an attacker may also bypass the security controls that apply to that phase in doing so. Instead of focusing on thwarting attacks at the earliest point in time, ***layered defense strategies that focus on phases*** that are vital for the attack path or that occur with a higher frequency are thus expected to be more successful.”



https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

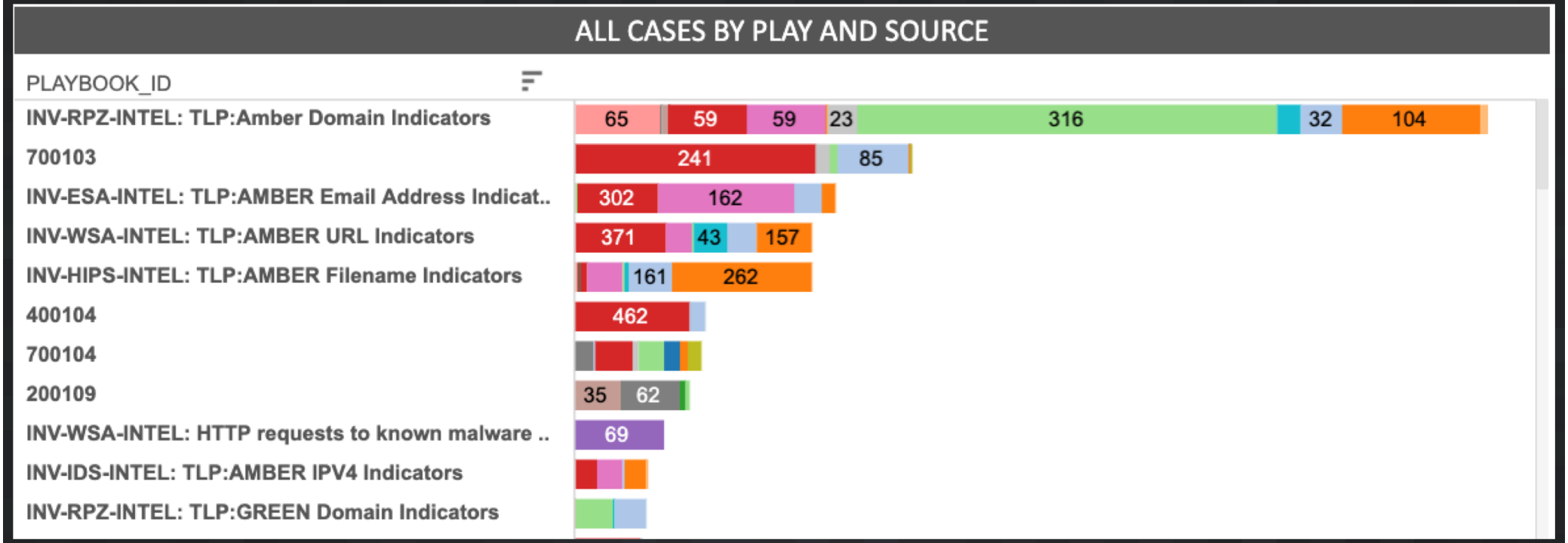
Playbook Coverage of Tactics

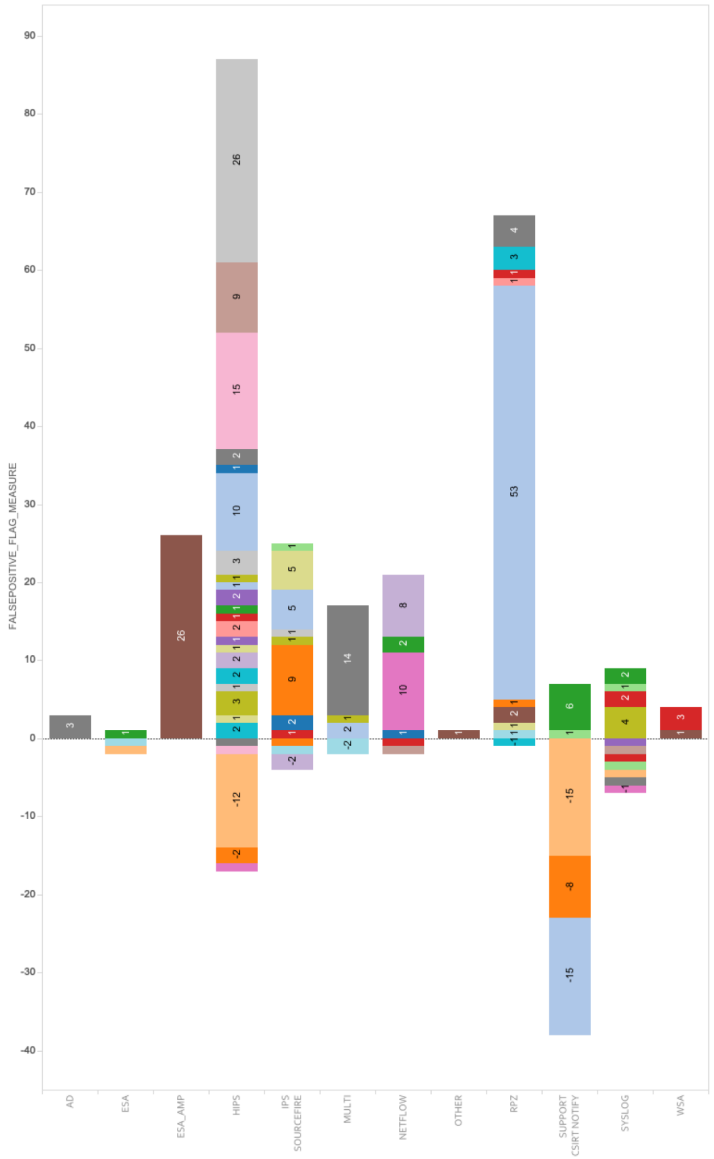
select a block to filter dashboard by tactic

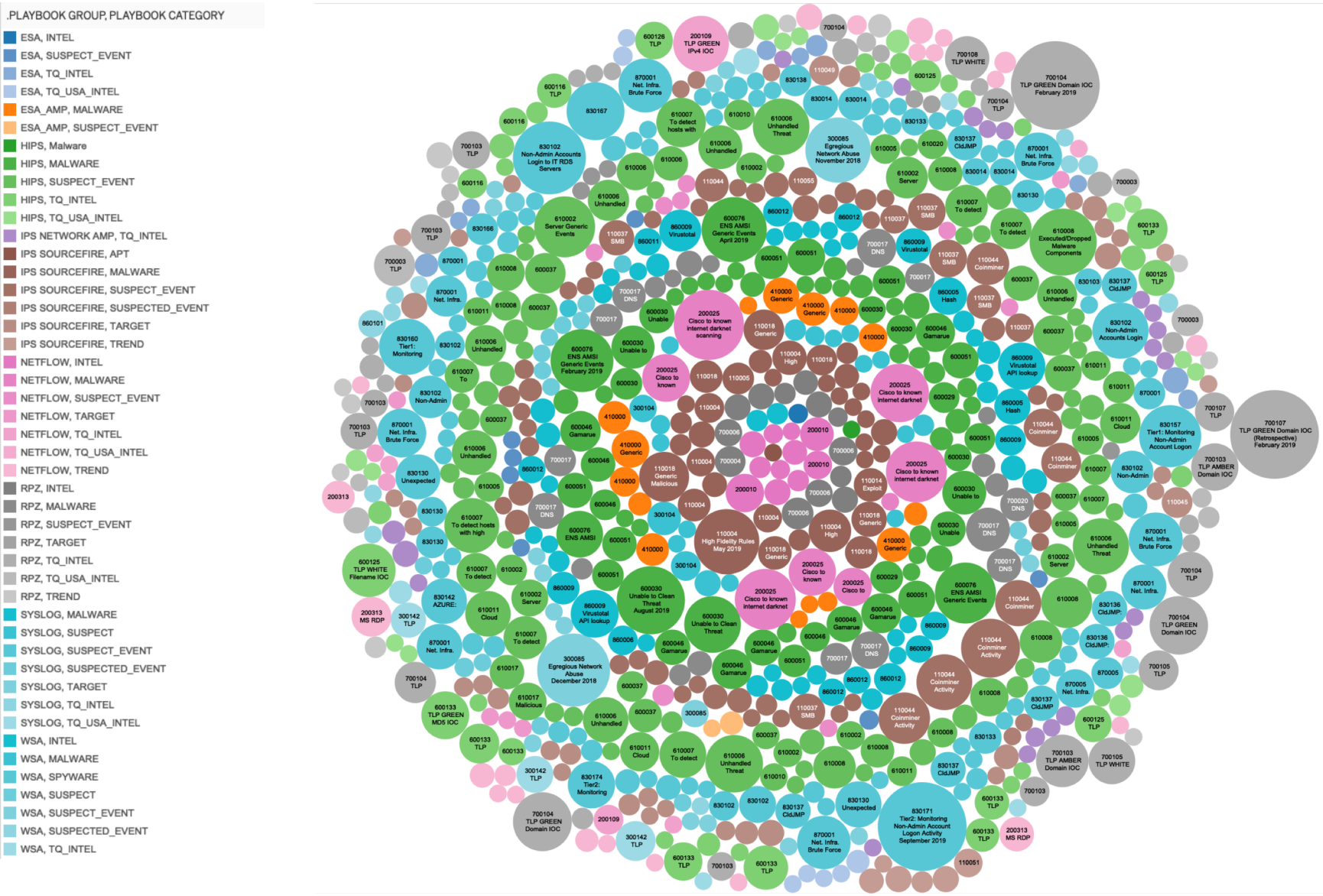


Coloring With Data

Enhance!


ALL CASES BY PLAY AND SOURCE
PLAYBOOK_ID
INV-RPZ-INTEL: TLP:Amber Domain Indicators
65
59
59
23
316
32
104
700103
241
85
INV-ESA-INTEL: TLP:AMBER Email Address Indicat..
302
162
INV-WSA-INTEL: TLP:AMBER URL Indicators
371
43
157
INV-HIPS-INTEL: TLP:AMBER Filename Indicators
161
262
400104
462
700104
200109
35
62
INV-WSA-INTEL: HTTP requests to known malware ..
69
INV-IDS-INTEL: TLP:AMBER IPV4 Indicators
INV-RPZ-INTEL: TLP:GREEN Domain Indicators


FALSEPOSITIVE_FLAG_MEASURE
90
80
70
60
50
40
30
20
10
0
-10
-20
-30
-40
AD
ESA
ESA_AMP
HIPS
IPS SOURCEFIRE
MULTI
NETFLOW
OTHER
RPZ
SUPPORT CSIRT NOTIFY
SYSLOG
WSA


.PLAYBOOK GROUP, PLAYBOOK CATEGORY
ESA, INTEL
ESA, SUSPECT_EVENT
ESA, TQ_INTEL
ESA, TQ_USA_INTEL
ESA_AMP, MALWARE
ESA_AMP, SUSPECT_EVENT
HIPS, Malware
HIPS, MALWARE
HIPS, SUSPECT_EVENT
HIPS, TQ_INTEL
HIPS, TQ_USA_INTEL
IPS NETWORK AMP, TQ_INTEL
IPS SOURCEFIRE, APT
IPS SOURCEFIRE, MALWARE
IPS SOURCEFIRE, SUSPECT_EVENT
IPS SOURCEFIRE, SUSPECTED_EVENT
IPS SOURCEFIRE, TARGET
IPS SOURCEFIRE, TREND
NETFLOW, INTEL
NETFLOW, MALWARE
NETFLOW, SUSPECT_EVENT
NETFLOW, TARGET
NETFLOW, TQ_INTEL
NETFLOW, TQ_USA_INTEL
NETFLOW, TREND
RPZ, INTEL
RPZ, MALWARE
RPZ, SUSPECT_EVENT
RPZ, TARGET
RPZ, TQ_INTEL
RPZ, TQ_USA_INTEL
RPZ, TREND
SYSLOG, MALWARE
SYSLOG, SUSPECT
SYSLOG, SUSPECT_EVENT
SYSLOG, SUSPECTED_EVENT
SYSLOG, TARGET
SYSLOG, TQ_INTEL
SYSLOG, TQ_USA_INTEL
WSA, INTEL
WSA, MALWARE
WSA, SPYWARE
WSA, SUSPECT
WSA, SUSPECT_EVENT
WSA, SUSPECTED_EVENT
WSA, TQ_INTEL

Questions?