Security Forum 2019

Security Operations
(위협으로부터 당신을 지켜드릴 케르베로스)

2019. 07. 04

황원섭 부장 (bob.hwang@microfocus.com)
ArcSight Pre-Sales Consultant / Micro Focus Korea

Confidential Information Disclaimer.

Software product roadmaps indicate Micro Focus’ directional intention at a point in time in an evolving environment. This roadmap is subject to change and is therefore not a commitment or representation by Micro Focus to develop, modify, market or deliver a software product, code or functionality, or to meet any specific timetable.

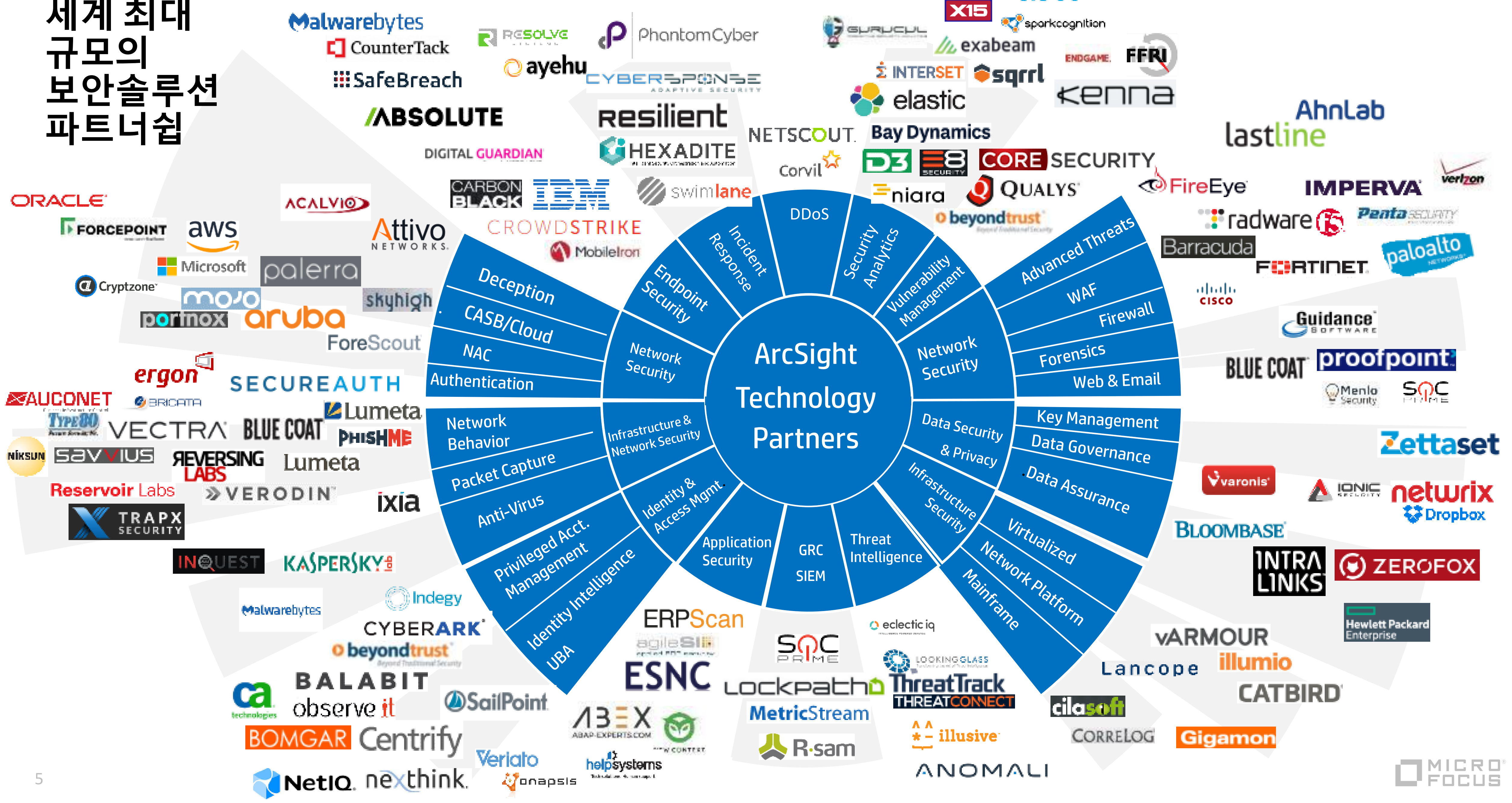
This document contains confidential information of Micro Focus and/or its affiliates. You may not disclose information in this document to others, or use it other than for your evaluation of a business relationship with Micro Focus. Micro Focus, its affiliates, and any participating company make no representations or warranties with respect to the contents of this document, and disclaim any express or implied warranties, including those of merchantability or fitness for any particular purpose.

Why Cerberus(케르베로스)?

NetIQ
(IAM)
ArcSight
(SIEM)
Fortify
(AppSec)

ArcSight는 하루아침에 만들어지지 않았다!

세계 최대 규모의 보안솔루션 파트너쉽



실시간? 상관분석? 그거 우리도 가능합니다?

Advanced Real-time Correlation

vs

Disk-Based/Search-Based Correlation

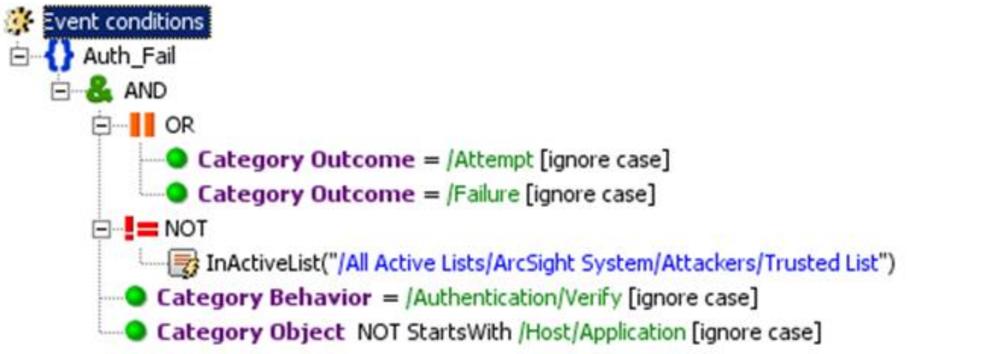
실시간? 상관분석? 그거 우리도 가능합니다?

검색엔진 Approach - Correlation *__Search__* – Brute Force Login

- Sample correlation search:

| `datamodel("Authentication","Authentication")` | stats values(Authentication.tag) as tag,count(eval('Authentication.action'=="failure")) as failure,count(eval('Authentication.action'=="success")) as success by Authentication.src | `drop_dm_object_name("Authentication")` | search success>0 | xswhere failure from failures_by_src_count_1h in authentication is above medium | `settags("access")`

ArcSight Approach – In Memory *__Real Time__* Correlation



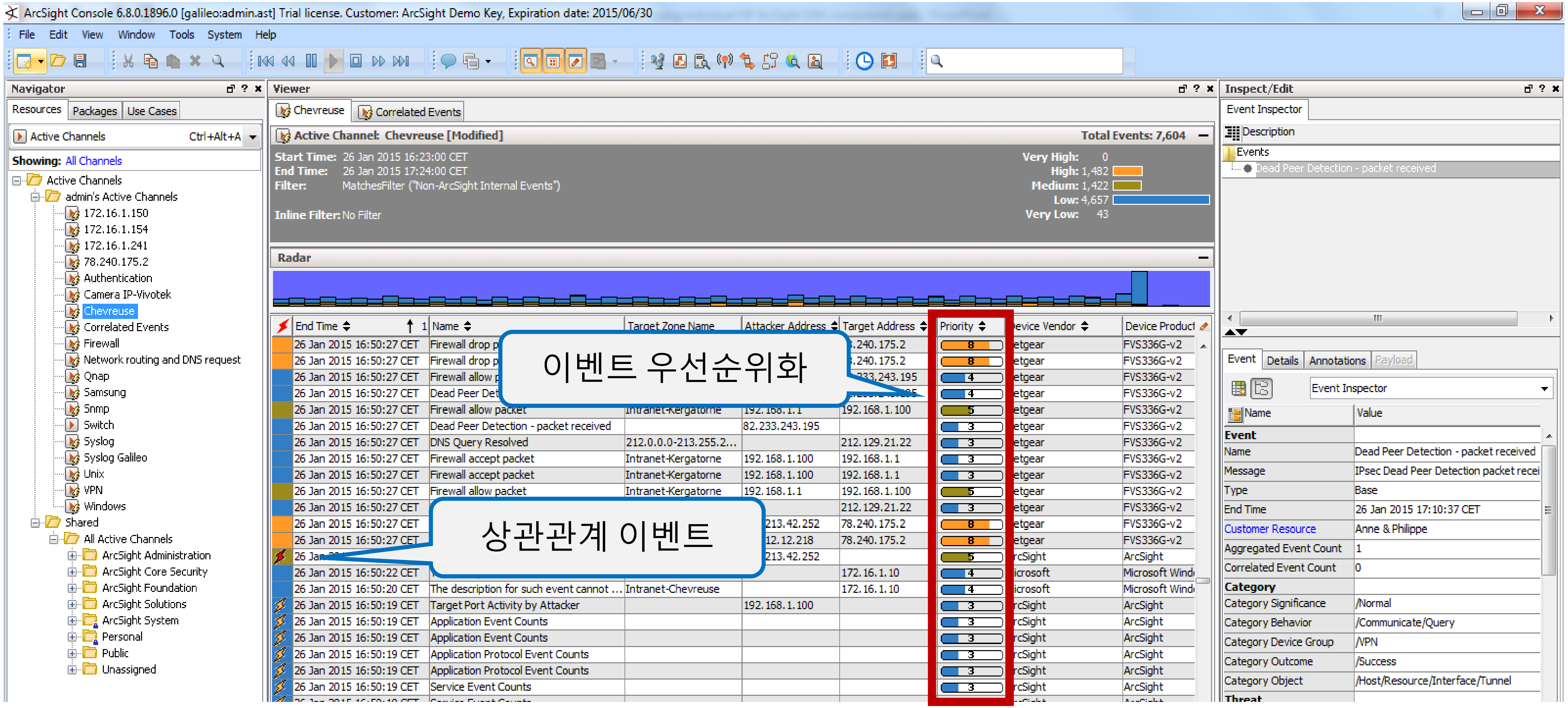
```
Event conditions
  Auth_Fail
    AND
      OR
        Category Outcome = /Attempt [ignore case]
        Category Outcome = /Failure [ignore case]
      NOT
        InActiveList("/All Active Lists/ArcSight System/Attackers/Trusted List")
      Category Behavior = /Authentication/Verify [ignore case]
      Category Object NOT StartsWith /Host/Application [ignore case]
```

/*This rule detects brute force login attempts. It looks for occurrences of login attempts or failures from sources that are not listed on a trusted active list.

It fires after 5 occurrences in 2 minutes. On first threshold, the attacker address is added to the /Suspicious active list. */

ArcSight ESM 콘솔 – 사용자(모니터링/분석가)중심의 직관적인 GUI

사용자가 쉽게 이벤트를 분석할 수 있는 직관적인 단일 GUI 방식



ArcSight Console 6.8.0.1896.0 [galileo:admin.ast] Trial license. Customer: ArcSight Demo Key, Expiration date: 2015/06/30

Showing: All Channels

- Active Channels
  - admin's Active Channels
    - 172.16.1.150
    - 172.16.1.154
    - 172.16.1.241
    - 78.240.175.2
    - Authentication
    - Camera IP-Vivotek
    - Chevreuse
    - Correlated Events
    - Firewall
    - Network routing and DNS request
    - Qnap
    - Samsung
    - Snmp
    - Switch
    - Syslog
    - Syslog Galileo
    - Unix
    - VPN
    - Windows
  - Shared
    - All Active Channels
      - ArcSight Administration
      - ArcSight Core Security
      - ArcSight Foundation
      - ArcSight Solutions
      - ArcSight System
      - Personal
      - Public
      - Unassigned

Active Channel: Chevreuse [Modified] Total Events: 7,604

Start Time: 26 Jan 2015 16:23:00 CET
End Time: 26 Jan 2015 17:24:00 CET
Filter: MatchesFilter ("Non-ArcSight Internal Events")

Inline Filter: No Filter

Very High: 0
High: 1,482
Medium: 1,422
Low: 4,657
Very Low: 43

End Time	Name	Target Zone Name	Attacker Address	Target Address	Priority	evice Vendor	Device Product
26 Jan 2015 16:50:27 CET	Firewall drop p			.240.175.2	8	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall drop p			.240.175.2	8	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall allow p			233.243.195	4	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Dead Peer Det				4	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall allow packet	Intranet-Kergatorne	192.168.1.1	192.168.1.100	5	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Dead Peer Detection - packet received		82.233.243.195		3	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	DNS Query Resolved	212.0.0.0-213.255.2...		212.129.21.22	3	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall accept packet	Intranet-Kergatorne	192.168.1.100	192.168.1.1	3	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall accept packet	Intranet-Kergatorne	192.168.1.100	192.168.1.1	3	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall allow packet	Intranet-Kergatorne	192.168.1.1	192.168.1.100	5	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET				212.129.21.22	3	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET			213.42.252	78.240.175.2	8	etgear	FVS336G-v2
26 Jan 2015 16:50:27 CET			12.12.218	78.240.175.2	8	etgear	FVS336G-v2
26 Jan			213.42.252		5	rcSight	ArcSight
26 Jan 2015 16:50:22 CET				172.16.1.10	4	icrosoft	Microsoft Wind
26 Jan 2015 16:50:20 CET	The description for such event cannot ...	Intranet-Chevreuse		172.16.1.10	4	icrosoft	Microsoft Wind
26 Jan 2015 16:50:19 CET	Target Port Activity by Attacker		192.168.1.100		3	rcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Event Counts				3	rcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Event Counts				3	rcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Protocol Event Counts				3	rcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Protocol Event Counts				3	rcSight	ArcSight
26 Jan 2015 16:50:19 CET	Service Event Counts				3	rcSight	ArcSight

이벤트 우선순위화

상관관계 이벤트

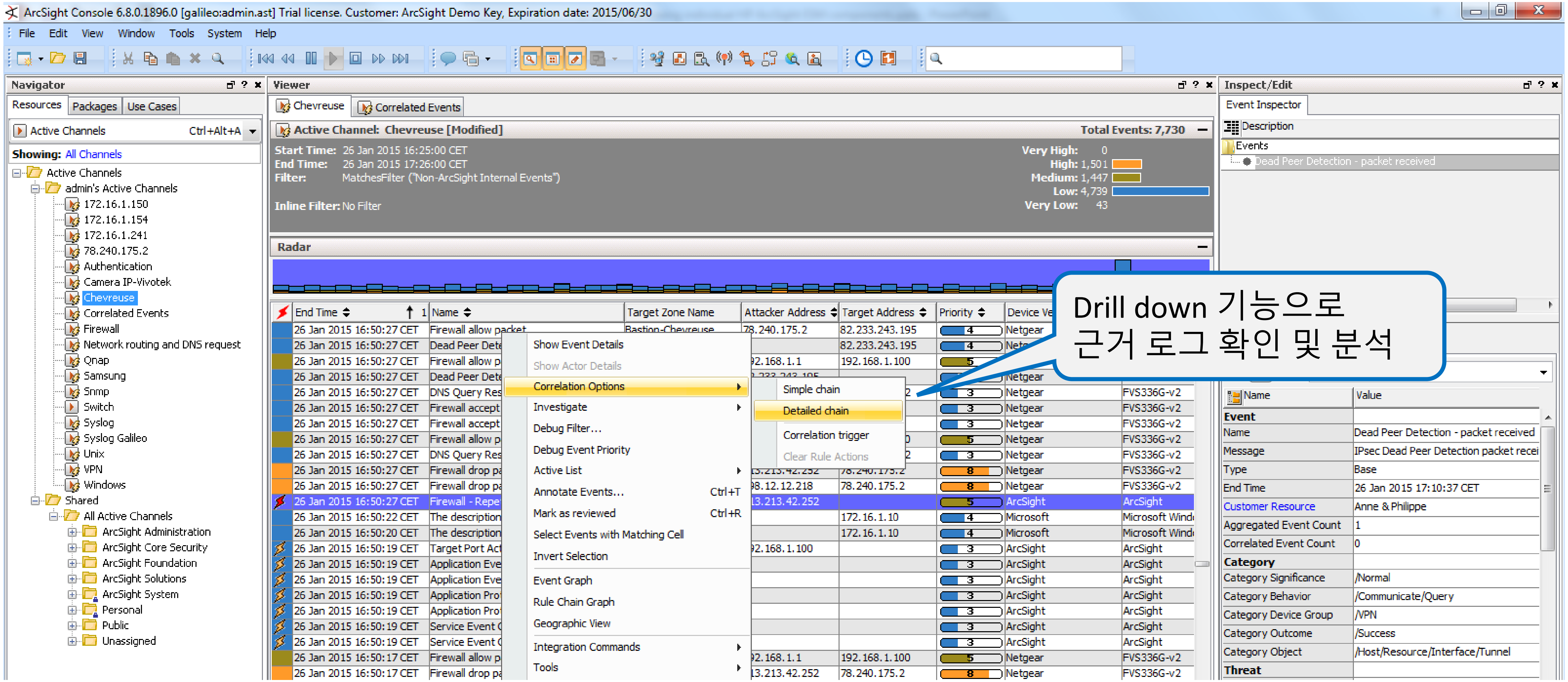
Description

- Events
  - Dead Peer Detection - packet received

Name	Value
Event	
Name	Dead Peer Detection - packet received
Message	IPsec Dead Peer Detection packet recei
Type	Base
End Time	26 Jan 2015 17:10:37 CET
Customer Resource	Anne & Philippe
Aggregated Event Count	1
Correlated Event Count	0
Category	
Category Significance	/Normal
Category Behavior	/Communicate/Query
Category Device Group	/VPN
Category Outcome	/Success
Category Object	/Host/Resource/Interface/Tunnel
Threat	

ArcSight ESM 콘솔 – 사용자(모니터링/분석가)중심의 직관적인 GUI

사용자가 쉽게 이벤트를 분석할 수 있는 직관적인 단일 GUI 방식



ArcSight Console 6.8.0.1896.0 [galileo:admin.ast] Trial license. Customer: ArcSight Demo Key, Expiration date: 2015/06/30

Showing: All Channels

- Active Channels
  - admin's Active Channels
    - 172.16.1.150
    - 172.16.1.154
    - 172.16.1.241
    - 78.240.175.2
    - Authentication
    - Camera IP-Vivotek
    - Chevreuse
    - Correlated Events
    - Firewall
    - Network routing and DNS request
    - Qnap
    - Samsung
    - Snmp
    - Switch
    - Syslog
    - Syslog Galileo
    - Unix
    - VPN
    - Windows
  - Shared
    - All Active Channels
      - ArcSight Administration
      - ArcSight Core Security
      - ArcSight Foundation
      - ArcSight Solutions
      - ArcSight System
      - Personal
      - Public
      - Unassigned

Active Channel: Chevreuse [Modified] **Total Events: 7,730**

Start Time: 26 Jan 2015 16:25:00 CET
End Time: 26 Jan 2015 17:26:00 CET
Filter: MatchesFilter ("Non-ArcSight Internal Events")

Inline Filter: No Filter

Very High: 0
High: 1,501
Medium: 1,447
Low: 4,739
Very Low: 43

End Time	Name	Target Zone Name	Attacker Address	Target Address	Priority	Device Ve	
26 Jan 2015 16:50:27 CET	Firewall allow packet	Bastion-Chevreuse	78.240.175.2	82.233.243.195	4	Netgear	
26 Jan 2015 16:50:27 CET	Dead Peer Dete			82.233.243.195	4	Netg	
26 Jan 2015 16:50:27 CET	Firewall allow p		92.168.1.1	192.168.1.100	5		
26 Jan 2015 16:50:27 CET	Dead Peer Dete		2.233.243.195			Netgear	
26 Jan 2015 16:50:27 CET	DNS Query Res			2	3	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall accept				3	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall accept				3	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall allow p			0	5	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	DNS Query Res			2	3	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall drop pa		13.213.42.252	78.240.175.2	8	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall drop pa		98.12.12.218	78.240.175.2	8	Netgear	FVS336G-v2
26 Jan 2015 16:50:27 CET	Firewall - Repe		13.213.42.252		5	ArcSight	ArcSight
26 Jan 2015 16:50:22 CET	The description			172.16.1.10	4	Microsoft	Microsoft Wind
26 Jan 2015 16:50:20 CET	The description			172.16.1.10	4	Microsoft	Microsoft Wind
26 Jan 2015 16:50:19 CET	Target Port Act		92.168.1.100		3	ArcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Eve				3	ArcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Eve				3	ArcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Prot				3	ArcSight	ArcSight
26 Jan 2015 16:50:19 CET	Application Prot				3	ArcSight	ArcSight
26 Jan 2015 16:50:19 CET	Service Event (				3	ArcSight	ArcSight
26 Jan 2015 16:50:19 CET	Service Event (				3	ArcSight	ArcSight
26 Jan 2015 16:50:17 CET	Firewall allow p		92.168.1.1	192.168.1.100	5	Netgear	FVS336G-v2
26 Jan 2015 16:50:17 CET	Firewall drop pa		13.213.42.252	78.240.175.2	8	Netgear	FVS336G-v2

Description

- Events
  - Dead Peer Detection - packet received

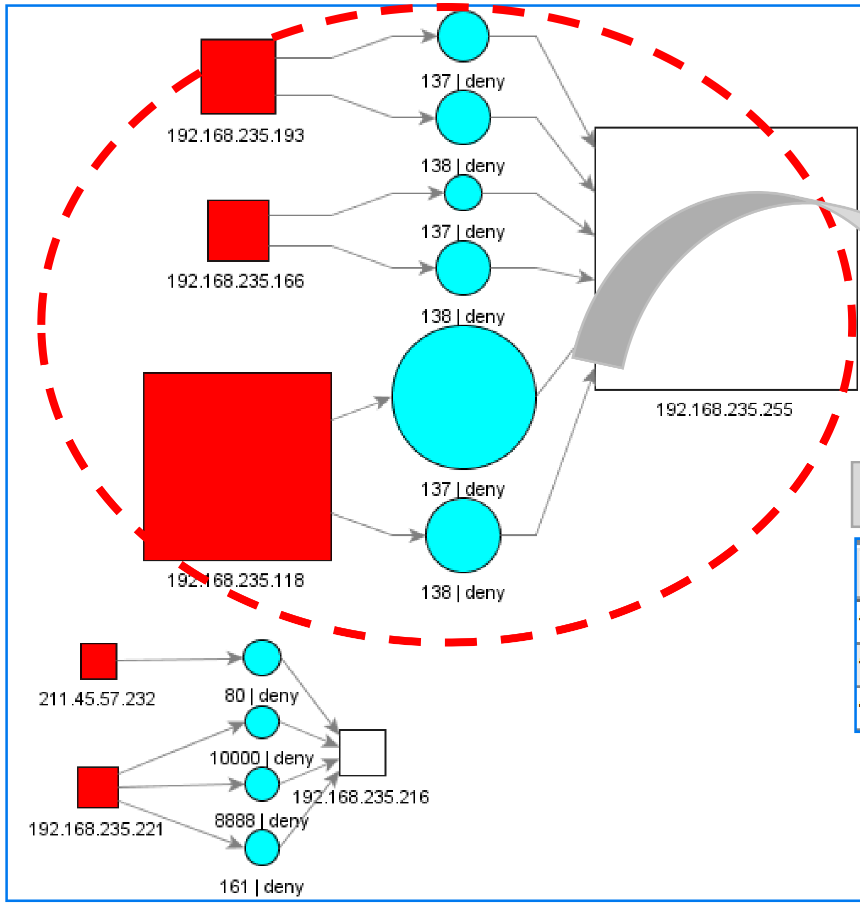
Name	Value
Event	
Name	Dead Peer Detection - packet received
Message	IPsec Dead Peer Detection packet recei
Type	Base
End Time	26 Jan 2015 17:10:37 CET
Customer Resource	Anne & Philippe
Aggregated Event Count	1
Correlated Event Count	0
Category	
Category Significance	/Normal
Category Behavior	/Communicate/Query
Category Device Group	/VPN
Category Outcome	/Success
Category Object	/Host/Resource/Interface/Tunnel
Threat	

Drill down 기능으로
근거 로그 확인 및 분석

ArcSight ESM 콘솔 – 단일 GUI(콘솔)에서 시각화(마우스우클릭)

방화벽 로그의 이벤트 그래프는 허용 트래픽 유형을 빠르고 직관적으로 파악 가능

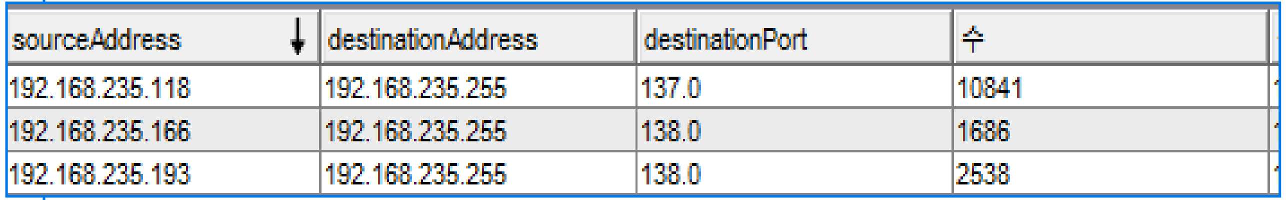
방화벽에서 Deny된 로그 분석



활용 사례

- 중요 서버에서 과도한 Broadcast 시도 탐지
- 트래픽을 모니터링하여 서비스 abusing 행위 적발

특정 소스주소에서 몇번의 접속 시도가 있었는지 현황 파악



sourceAddress ↓	destinationAddress	destinationPort	수
192.168.235.118	192.168.235.255	137.0	10841
192.168.235.166	192.168.235.255	138.0	1686
192.168.235.193	192.168.235.255	138.0	2538

Significant Market Trends

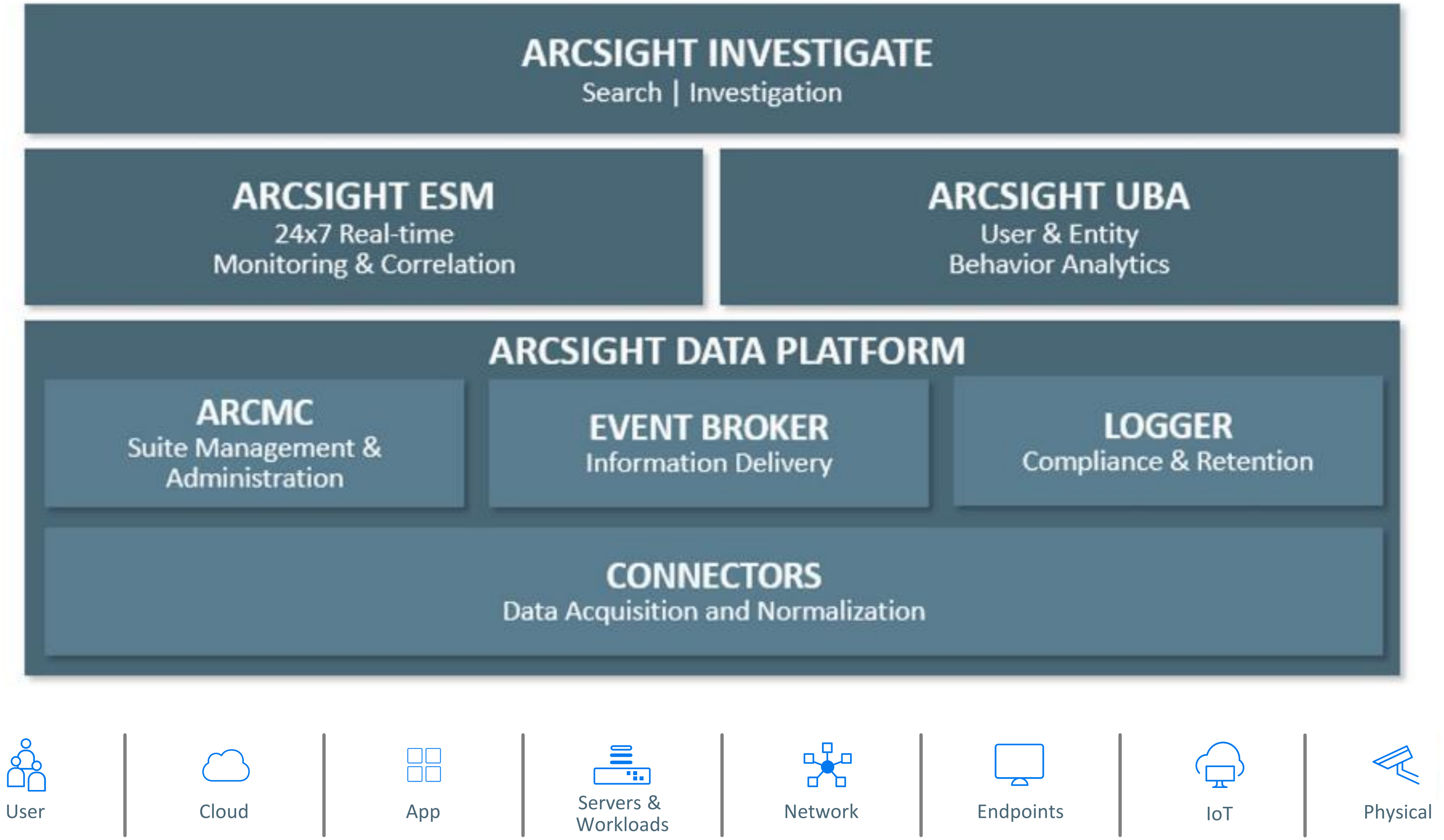
- **Simplicity** – Install in minutes, configure in hours, value in days

- **User experience** – As few clicks as possible; immersive; intuitive; proactive knowledge
- **Analytic Insight** – Reduce burden of content development, identifying unknown threats more quickly

- **Hybrid Cloud** – Full deployment and monitoring into critical cloud environments and monitoring of key cloud applications

- **SaaS** – Expected that SIEM vendors offer SaaS options in addition to on-prem / hybrid options

The Current ArcSight Architecture



ARCSIGHT INVESTIGATE
Search | Investigation

ARCSIGHT ESM
24x7 Real-time
Monitoring & Correlation

ARCSIGHT UBA
User & Entity
Behavior Analytics

ARCSIGHT DATA PLATFORM

ARCMC
Suite Management &
Administration

EVENT BROKER
Information Delivery

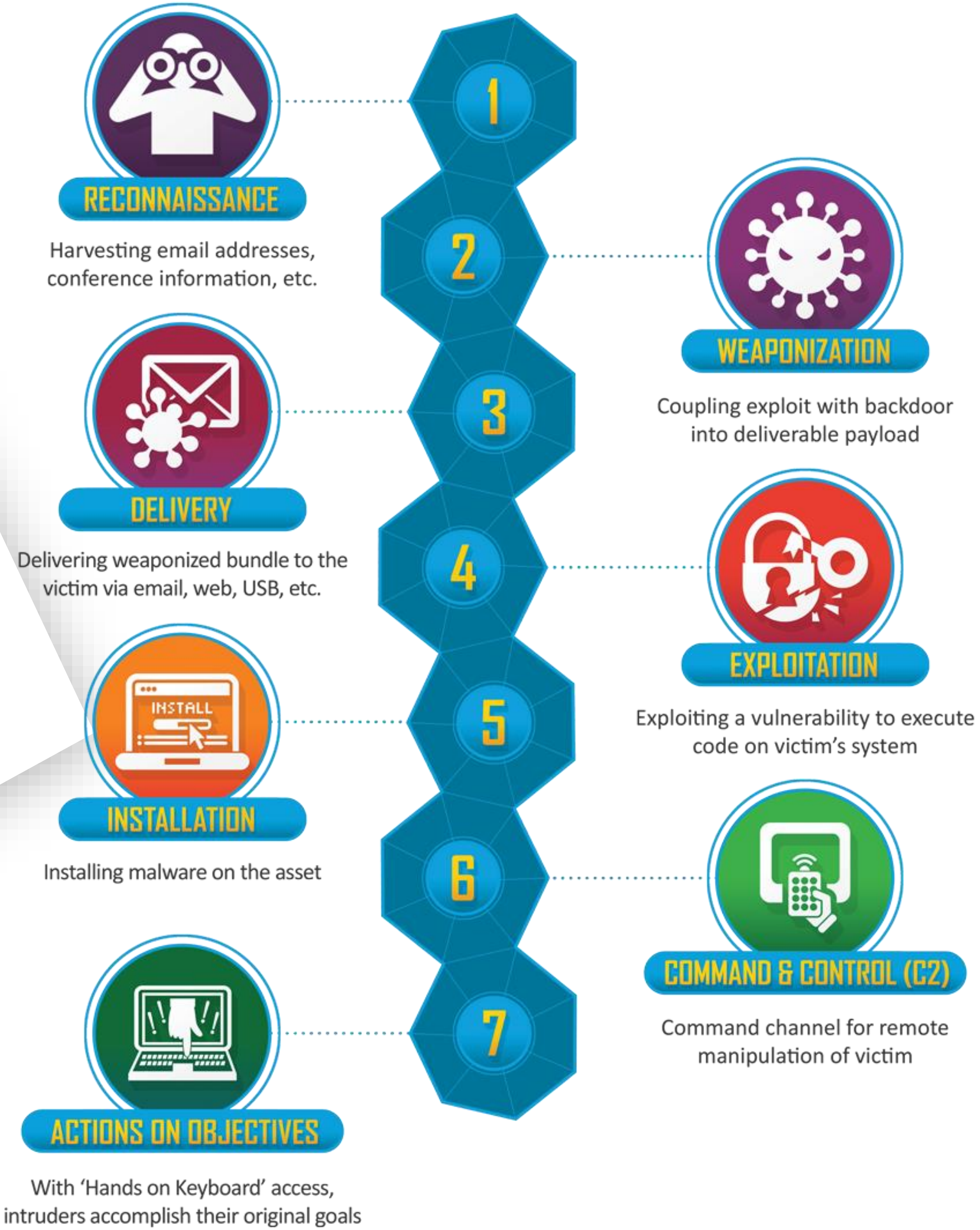
LOGGER
Compliance & Retention

CONNECTORS
Data Acquisition and Normalization

User | Cloud | App | Servers & Workloads | Network | Endpoints | IoT | Physical

Cyber Kill Chain

Good, but MITRE ATT&CK is a more advanced framework to describe latest coordinated attacks.

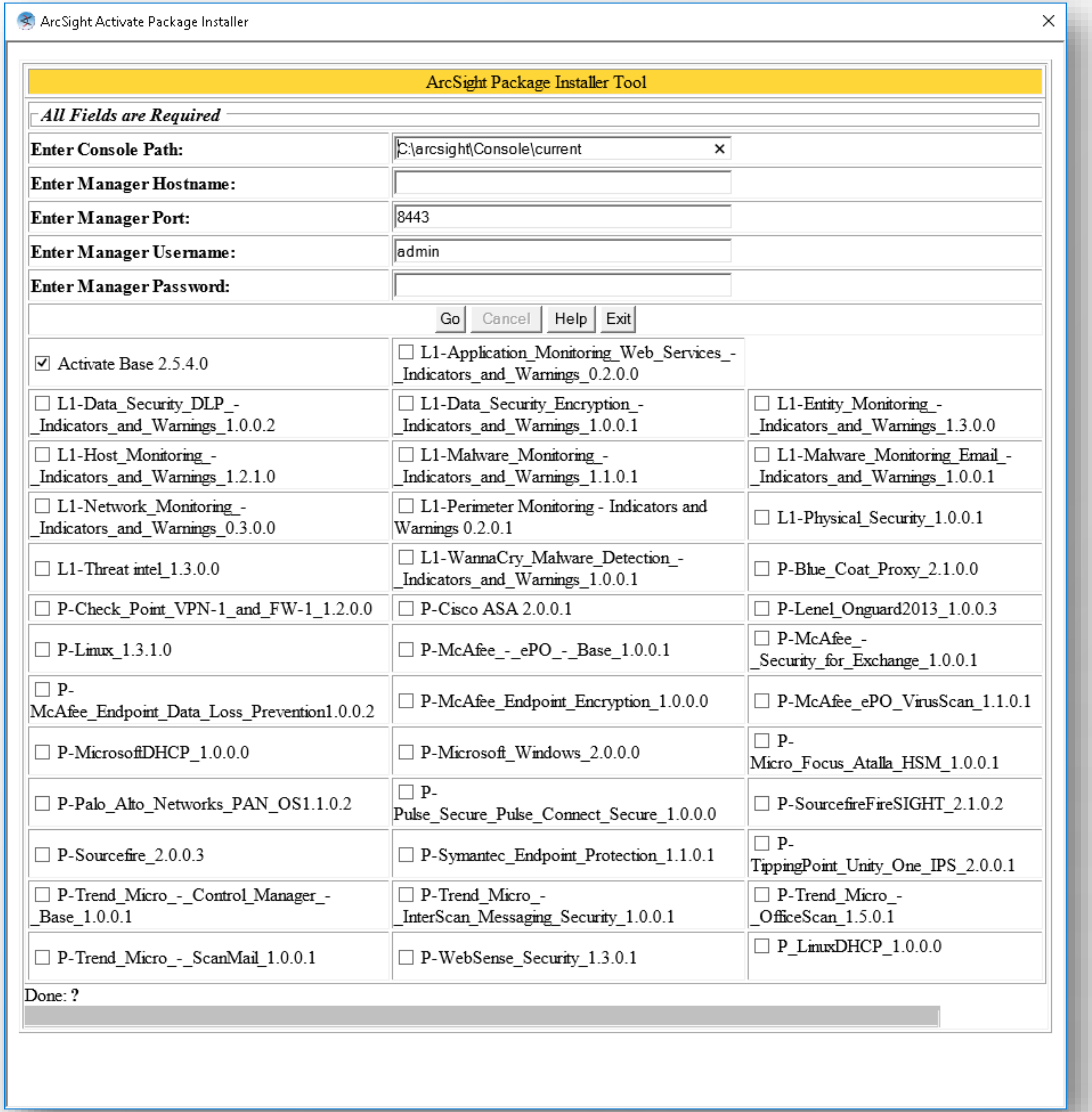


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

MICRO FOCUS

Activate Framework

- Good Idea, but…
- Innovators left long time ago
- Ad hoc and not a concerted effort (Wiki is hit and miss)
- Not easy to deploy: Package Installer Tool invented for this purpose)
- Customer feedback is ‘Negative’
- Content is niche & not customer-driven (not real-world)
- Notoriously outdated
- No versioning
- Not obvious where to start
- L1 packages have lots of *noise*



ArcSight Activate Package Installer

ArcSight Package Installer Tool

All Fields are Required

Enter Console Path:	C:\arcsight\Console\current
Enter Manager Hostname:	
Enter Manager Port:	8443
Enter Manager Username:	admin
Enter Manager Password:	

☑ Activate Base 2.5.4.0	☐ L1-Application_Monitoring_Web_Services_-_Indicators_and_Warnings_0.2.0.0	
☐ L1-Data_Security_DLP_-_Indicators_and_Warnings_1.0.0.2	☐ L1-Data_Security_Encryption_-_Indicators_and_Warnings_1.0.0.1	☐ L1-Entity_Monitoring_-_Indicators_and_Warnings_1.3.0.0
☐ L1-Host_Monitoring_-_Indicators_and_Warnings_1.2.1.0	☐ L1-Malware_Monitoring_-_Indicators_and_Warnings_1.1.0.1	☐ L1-Malware_Monitoring_Email_-_Indicators_and_Warnings_1.0.0.1
☐ L1-Network_Monitoring_-_Indicators_and_Warnings_0.3.0.0	☐ L1-Perimeter Monitoring - Indicators and Warnings 0.2.0.1	☐ L1-Physical_Security_1.0.0.1
☐ L1-Threat intel_1.3.0.0	☐ L1-WannaCry_Malware_Detection_-_Indicators_and_Warnings_1.0.0.1	☐ P-Blue_Coat_Proxy_2.1.0.0
☐ P-Check_Point_VPN-1_and_FW-1_1.2.0.0	☐ P-Cisco ASA 2.0.0.1	☐ P-Lenel_Onguard2013_1.0.0.3
☐ P-Linux_1.3.1.0	☐ P-McAfee_-_ePO_-_Base_1.0.0.1	☐ P-McAfee_-_Security_for_Exchange_1.0.0.1
☐ P-McAfee_Endpoint_Data_Loss_Prevention1.0.0.2	☐ P-McAfee_Endpoint_Encryption_1.0.0.0	☐ P-McAfee_ePO_VirusScan_1.1.0.1
☐ P-MicrosoftDHCP_1.0.0.0	☐ P-Microsoft_Windows_2.0.0.0	☐ P-Micro_Focus_Atalla_HSM_1.0.0.1
☐ P-Palo_Alto_Networks_PAN_OS1.1.0.2	☐ P-Pulse_Secure_Pulse_Connect_Secure_1.0.0.0	☐ P-SourcefireFireSIGHT_2.1.0.2
☐ P-Sourcefire_2.0.0.3	☐ P-Symantec_Endpoint_Protection_1.1.0.1	☐ P-TippingPoint_Unity_One_IPS_2.0.0.1
☐ P-Trend_Micro_-_Control_Manager_-_Base_1.0.0.1	☐ P-Trend_Micro_-_InterScan_Messaging_Security_1.0.0.1	☐ P-Trend_Micro_-_OfficeScan_1.5.0.1
☐ P-Trend_Micro_-_ScanMail_1.0.0.1	☐ P-WebSense_Security_1.3.0.1	☐ P_LinuxDHCP_1.0.0.0

Done: ?

MITRE ATT&CK MATRIX

Adversary

Tactics

Techniques

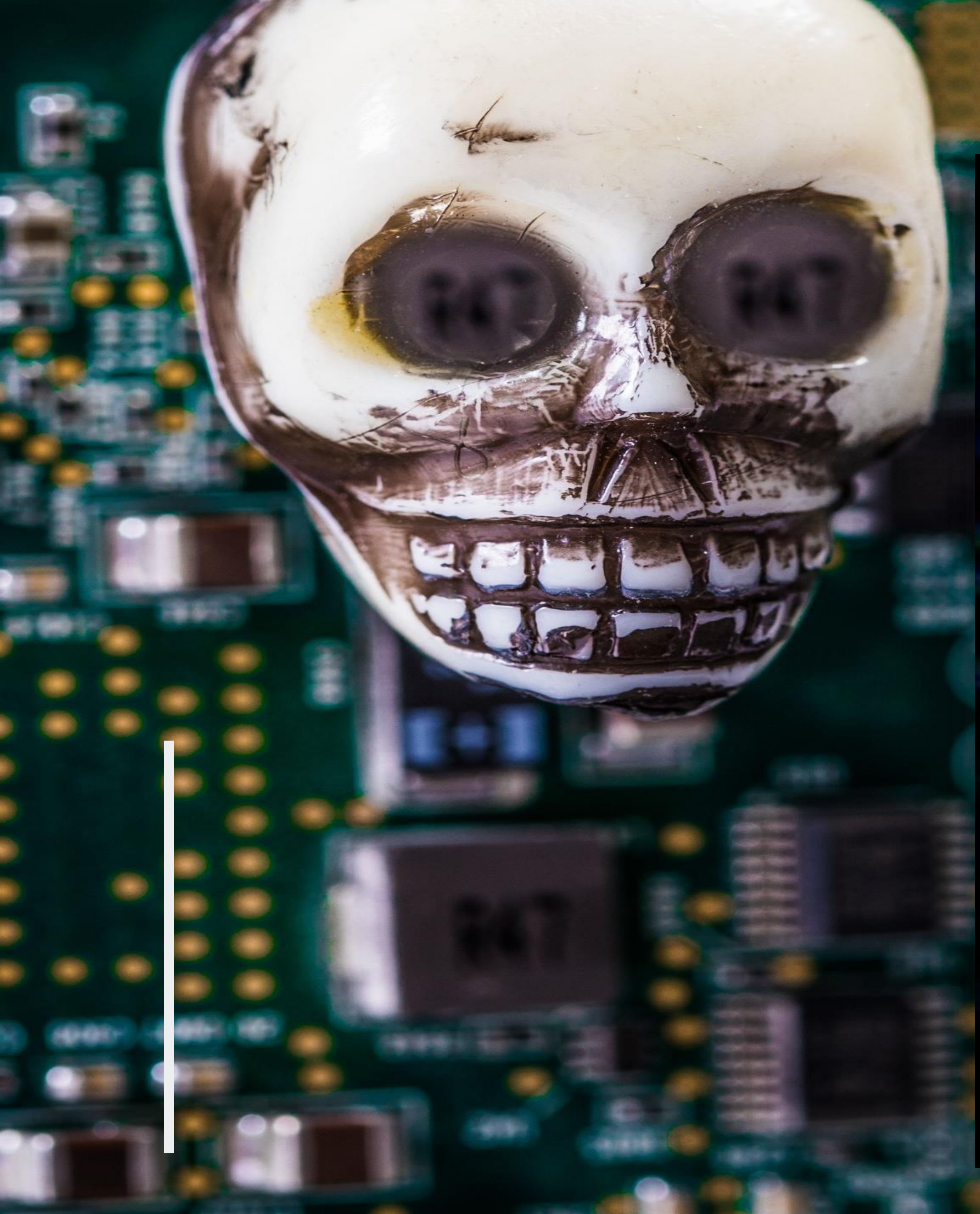
&

Common

Knowledge

ATT&CK™

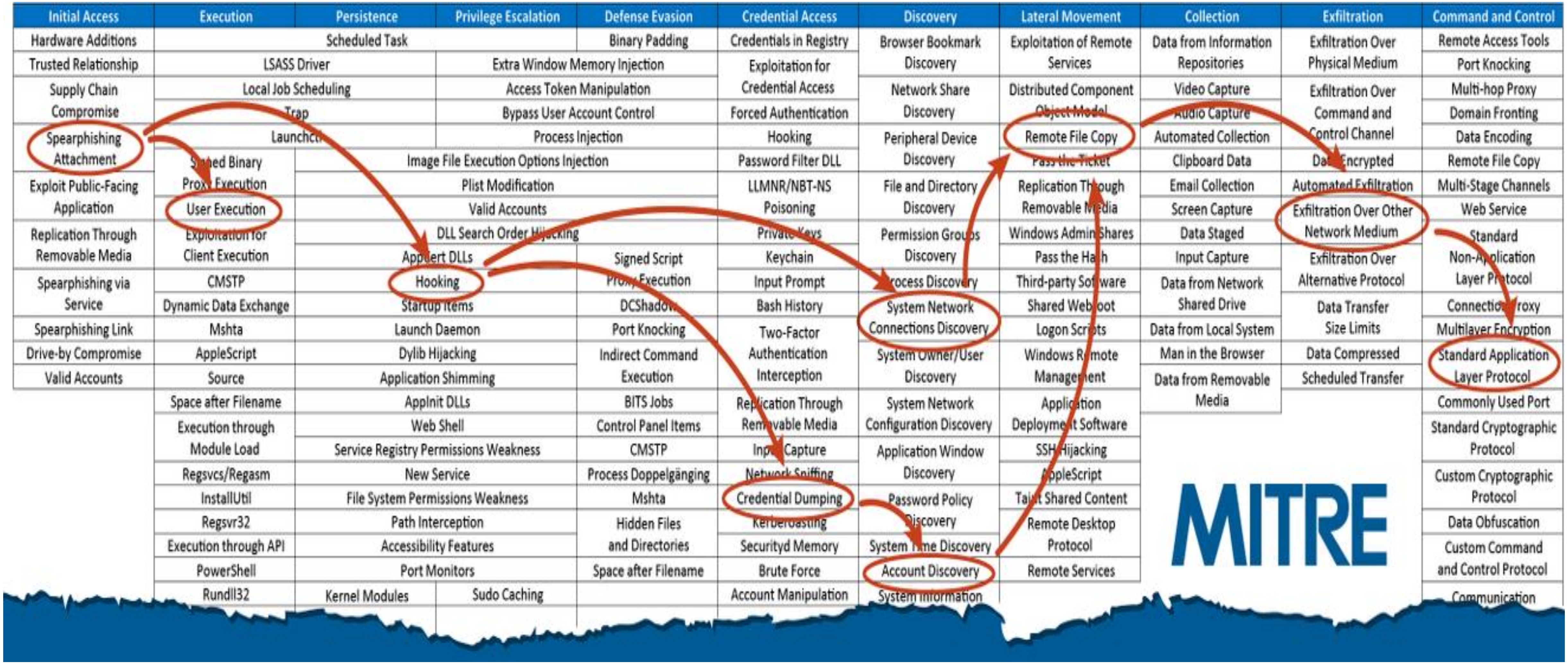
https://attack.mitre.org/



Current Attack Trends

- APT with built-in AI
- Less Command & Control
- No direct attack on servers
- Footprint @ endpoints
- Powershell on endpoints
- DNS for CnC & exfiltration

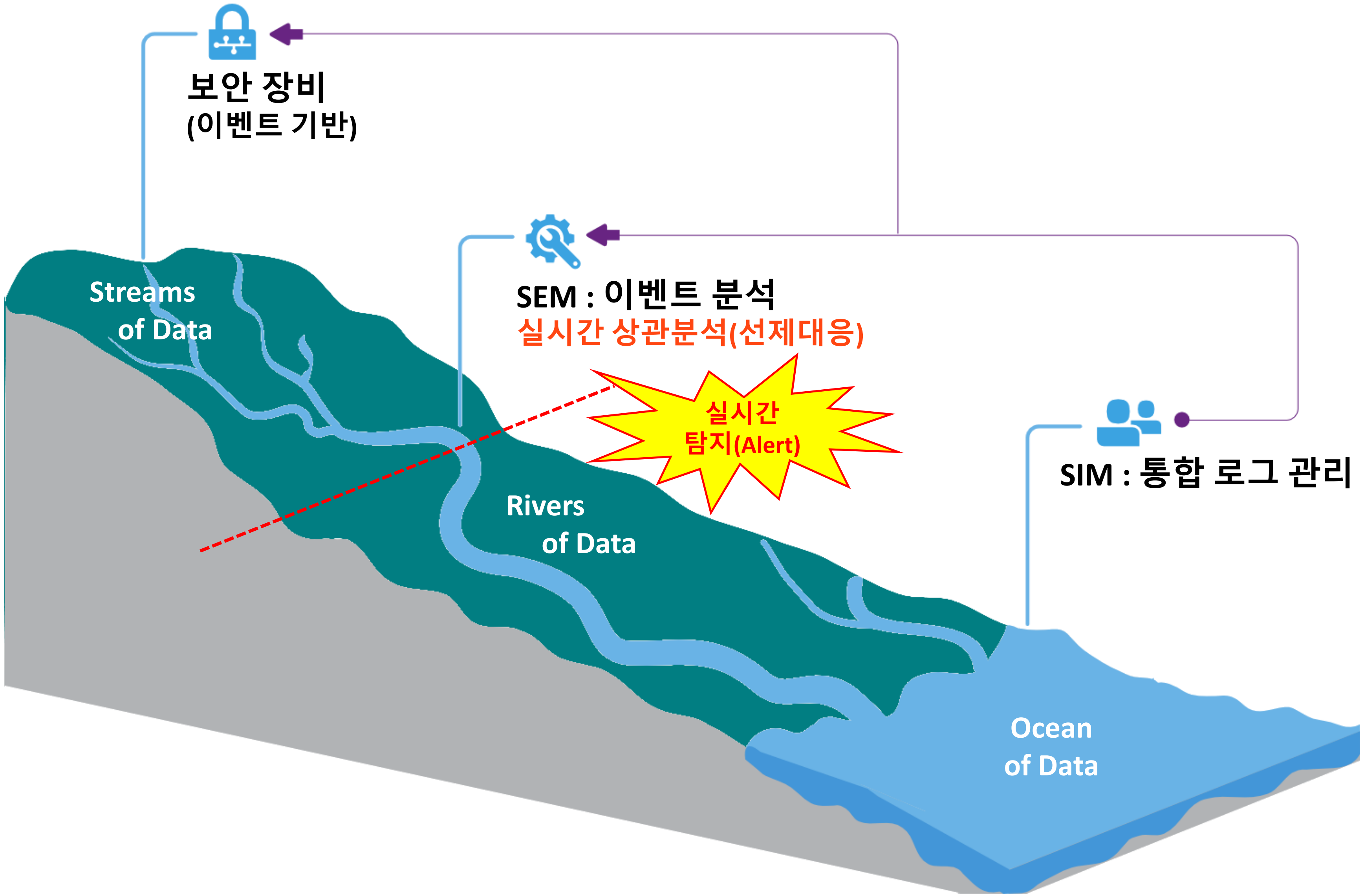
MITRE ATT&CK – Blueprint for Attack Tactic & Techniques



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions	Scheduled Task			Binary Padding	Credentials in Registry	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Exfiltration Over Physical Medium	Remote Access Tools
Trusted Relationship	LSASS Driver		Extra Window Memory Injection		Exploitation for Credential Access					Port Knocking
Supply Chain Compromise	Local Job Scheduling		Access Token Manipulation			Network Share Discovery	Distributed Component Object Model	Video Capture	Exfiltration Over Command and Control Channel	Multi-hop Proxy
	Trap		Bypass User Account Control		Forced Authentication			Audio Capture		Domain Fronting
Spearphishing Attachment	Launchctl		Process Injection		Hooking	Peripheral Device Discovery	Remote File Copy	Automated Collection		Data Encoding
	Signed Binary Proxy Execution	Image File Execution Options Injection			Password Filter DLL		Pass the Ticket	Clipboard Data	Data Encrypted	Remote File Copy
Exploit Public-Facing Application		Plist Modification			LLMNR/NBT-NS Poisoning	File and Directory Discovery	Replication Through Removable Media	Email Collection	Automated Exfiltration	Multi-Stage Channels
	User Execution	Valid Accounts						Screen Capture	Exfiltration Over Other Network Medium	Web Service
Replication Through Removable Media	Exploitation for Client Execution	DLL Search Order Hijacking			Private Keys	Permission Groups Discovery	Windows Admin Shares	Data Staged		Standard Non-Application Layer Protocol
		AppCert DLLs		Signed Script Proxy Execution	Keychain		Pass the Hash	Input Capture	Exfiltration Over Alternative Protocol	
Spearphishing via Service	CMSTP	Hooking			Input Prompt	Process Discovery	Third-party Software	Data from Network Shared Drive		
	Dynamic Data Exchange	Startup Items		DCShadow	Bash History	System Network Connections Discovery	Shared Webroot		Data Transfer Size Limits	Connection Proxy
Spearphishing Link	Mshta	Launch Daemon		Port Knocking	Two-Factor Authentication Interception		Logon Scripts	Data from Local System		Multilayer Encryption
Drive-by Compromise	AppleScript	Dylib Hijacking		Indirect Command Execution		System Owner/User Discovery	Windows Remote Management	Man in the Browser	Data Compressed	Standard Application Layer Protocol
Valid Accounts	Source	Application Shimming						Data from Removable Media	Scheduled Transfer	
	Space after Filename	AppInit DLLs		BITS Jobs	Replication Through Removable Media	System Network Configuration Discovery	Application Deployment Software			Commonly Used Port
	Execution through Module Load	Web Shell		Control Panel Items						Standard Cryptographic Protocol
		Service Registry Permissions Weakness		CMSTP	Input Capture	Application Window Discovery	SSH Hijacking			
	Regsvcs/Regasm	New Service		Process Doppelgänging	Network Sniffing		AppleScript			Custom Cryptographic Protocol
	InstallUtil	File System Permissions Weakness		Mshta	Credential Dumping	Password Policy Discovery	Taint Shared Content			
	Regsvr32	Path Interception		Hidden Files and Directories	Kerberoasting		Remote Desktop Protocol			Data Obfuscation
	Execution through API	Accessibility Features			Securityd Memory	System Time Discovery				Custom Command and Control Protocol
	PowerShell	Port Monitors		Space after Filename	Brute Force	Account Discovery	Remote Services			
	Rundll32	Kernel Modules	Sudo Caching		Account Manipulation	System Information				Communication

SIEM Security information and event management = SIM 통합로그관리 + SEM 이벤트 분석

제대로 활용할 수 있는 SIEM은, 실시간 보안 위협에 대한 가시성 및 대응 근거를 제공해야!!



보안 장비
(이벤트 기반)

SEM : 이벤트 분석
실시간 상관분석(선제대응)

실시간
탐지(Alert)

SIM : 통합 로그 관리

국내외 SIEM 제품

ArcSight (ESM)

~~IBM QRadar (NBAD)~~

ArcSight (Logger, Investigate)

splunk>

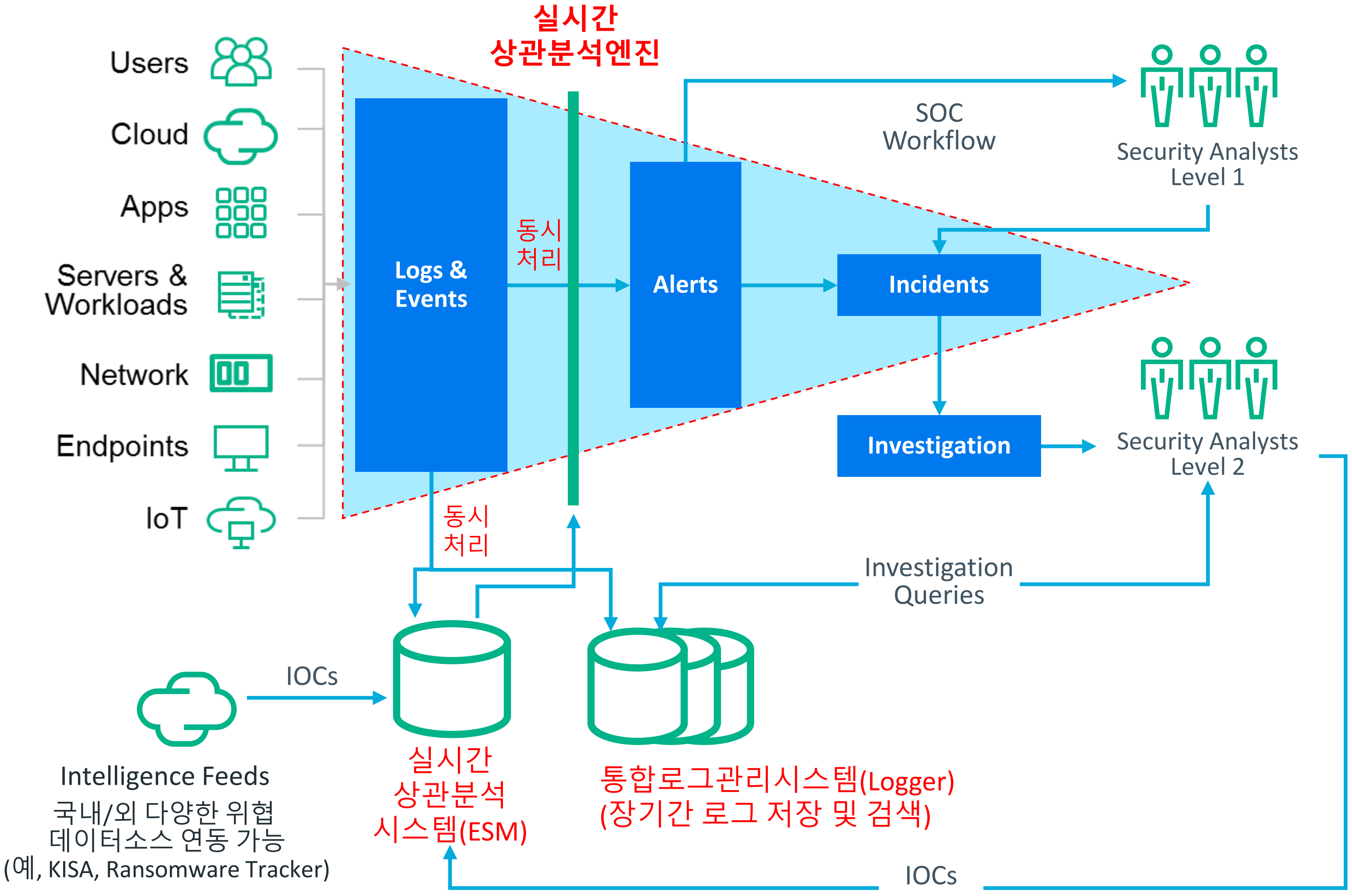
SecuLayer

elastic

LOGPRESSO

SIEM은 '실시간 상관분석' 및 '빅데이터기반 지능형 분석' 모두 필요

'실시간 상관분석 엔진'과 '통합로그시스템'을 분리 구성하여, 기술적으로 합리적 아키텍쳐 구현



실시간
상관분석엔진
Users
Cloud
Apps
Servers & Workloads
Network
Endpoints
IoT
Logs & Events
동시 처리
Alerts
Incidents
Investigation
SOC Workflow
Security Analysts Level 1
Security Analysts Level 2
동시 처리
Investigation Queries
IOCs
Intelligence Feeds
국내/외 다양한 위협 데이터소스 연동 가능
(예, KISA, Ransomware Tracker)
실시간 상관분석 시스템(ESM)
통합로그관리시스템(Logger)
(장기간 로그 저장 및 검색)
IOCs

실시간 위협(공격) 탐지

- 증가하는 보안이벤트의 실시간 탐지
- 침해지표에 대한 실시간 상관분석
- 내/외부 공격 시나리오 기반 탐지
- 오탐(false positives) 수 감소

로그 분석 및 조사

- 환경 및 시간대 전반에 걸친 사용자 정의 쿼리 기능 제공
- 의심 데이터 분석 및 대응
- 정/오탐 여부 검증

※ IOC(Indicators of Compromise) : 침해지표 (예, 지리적인 불규칙성, 이상한 IP주소, 이상한 활동, 갑작스런 트래픽 급증 등)

The Ultimate Goal

Timely, Actionable Security Insights

- Need for Visibility
- Need to Detect
- Need to Respond

Thank you.

#MicroFocusSecurityForum2019