

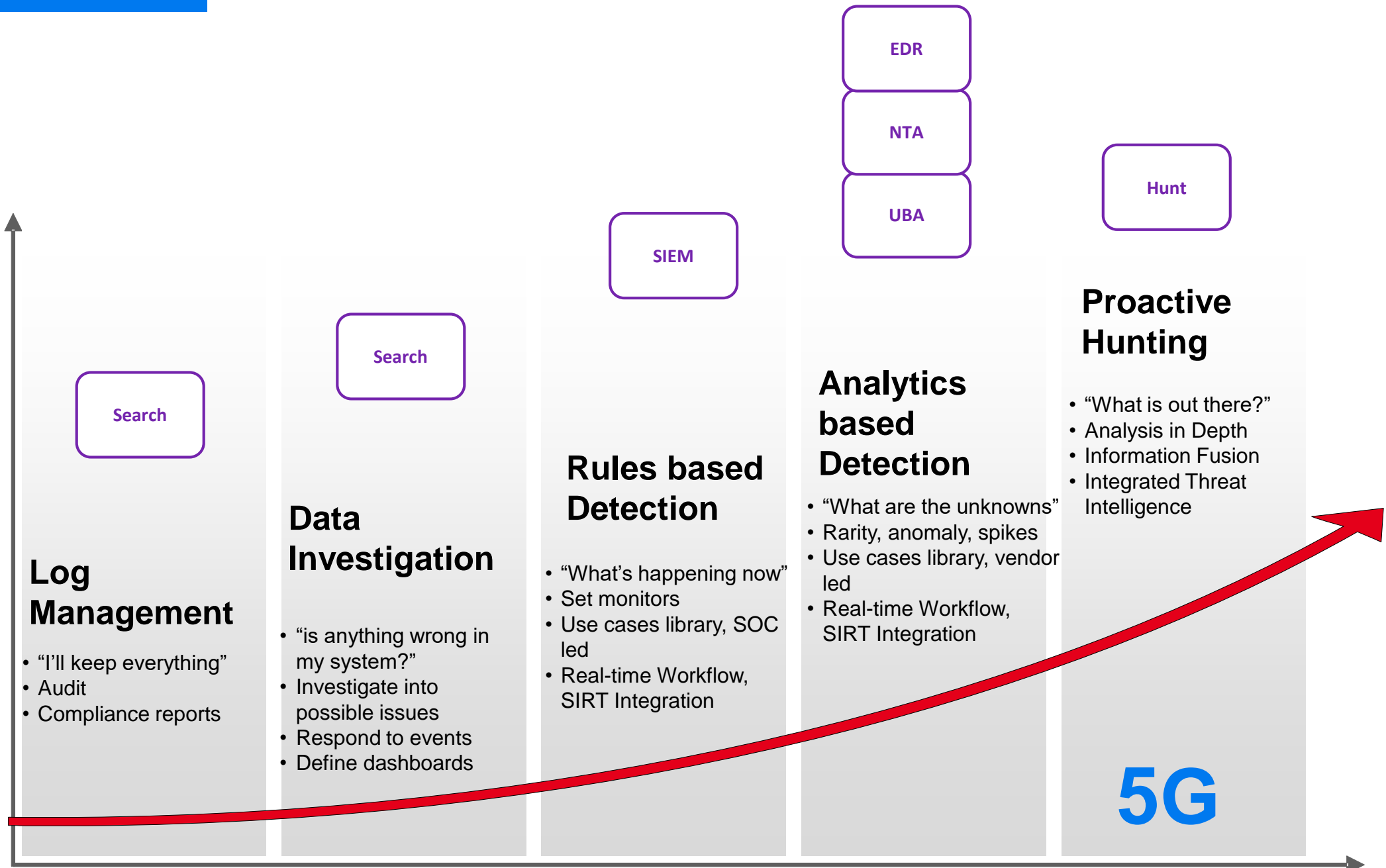


Experience Tour Poland 2019

Arcsight & Interset acquisition (UEBA)

Cfir Homeri
Security Presales - East Central Europe & Israel
Cfir.homeri@microfocus.com





Log Management

- "I'll keep everything"
- Audit
- Compliance reports

Data Investigation

- "is anything wrong in my system?"
- Investigate into possible issues
- Respond to events
- Define dashboards

Rules based Detection

- "What's happening now"
- Set monitors
- Use cases library, SOC led
- Real-time Workflow, SIRT Integration

Analytics based Detection

- "What are the unknowns"
- Rarity, anomaly, spikes
- Use cases library, vendor led
- Real-time Workflow, SIRT Integration

Proactive Hunting

- "What is out there?"
- Analysis in Depth
- Information Fusion
- Integrated Threat Intelligence

5G

VISION

To deliver the market's first layered security analytics platform, and reestablish ArcSight as the standard by which all others will again be measured

MISSION-

Our Mission:

Deliver an **open** and **integrated** security analytics platform that **simplifies** delivery of **layered analytics**

Outcome:

Reduce **exposure** by empowering **intelligent** detection, investigation, and response for **enabling** the self-defending enterprise

WEB CONSOLE

Accessible Monitoring & Platform Management

CONTENT

Unified | Actionable | Insight

ARCSIGHT LOGGER

Compliance | Search | Retention

ARCSIGHT ENTERPRISE SECURITY MANAGER

24x7 Real-time Monitoring & Correlation

ARCSIGHT INVESTIGATE

Hunt | Investigation

UEBA

User Entity Behavior Analytics

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER

Suite Management & Administration

TRANSFORMATION HUB

Information delivery

SMART/FLEX CONNECTORS

Data Collection, Enrichment, and Normalization



User



Cloud



App



Servers &
Workloads



Network



Endpoints



IoT



Physical

WEB CONSOLE

Accessible Monitoring & Platform Management

CONTENT

Unified | Actionable | Insight

ARCSIGHT LOGGER

Compliance | Search | Retention

ARCSIGHT ENTERPRISE SECURITY MANAGER

24x7 Real-time Monitoring & Correlation

ARCSIGHT INVESTIGATE

Hunt | Investigation

UEBA

User Entity Behavior Analytics

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER

Suite Management & Administration

TRANSFORMATION HUB

Information delivery

SMART/FLEX CONNECTORS

Data Collection, Enrichment, and Normalization



User



Cloud



App



Servers &
Workloads



Network



Endpoints



IoT

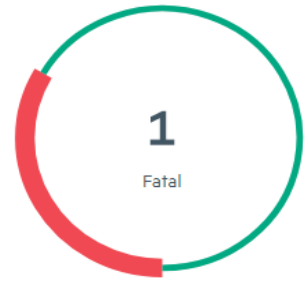


Physical

Total Number of Nodes

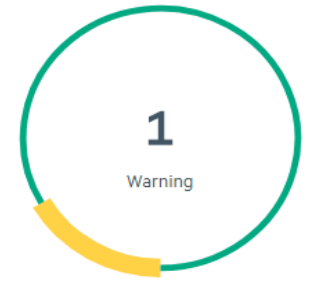
5009 Devices 3 ArcMC/CHA 6 Connectors 6 Collectors 2 Loggers 3 Nodes (1 Event Broker)

ArcMC/CHA



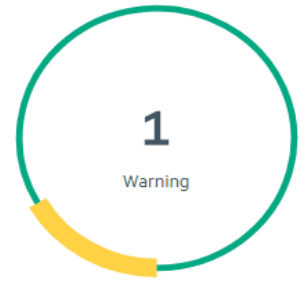
Fatal	Count(1)
ArcMC Down	1
Healthy	Count(2)
Healthy Nodes	2

Connectors



Warning	Count(1)
08_10_2017_Full GC	1
Healthy	Count(5)
Healthy Nodes	5

Collectors



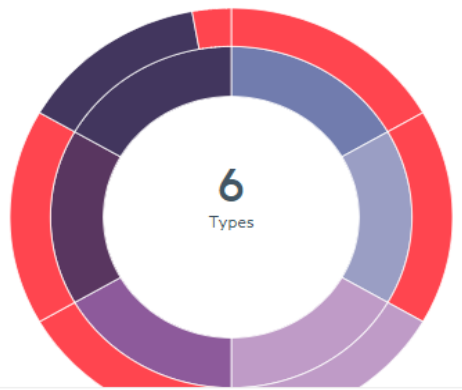
Warning	Count(1)
08_10_2017_Full GC	1
Healthy	Count(5)
Healthy Nodes	5

Loggers



Warning	Count(1)
08_10_2017_Receiver Down	1
Healthy	Count(1)
Healthy Nodes	1

Devices by Device Product



Device Product	Total Devices	Inactive Devices
Fortigate	4999	4999
Microsoft Windows	1	1
Unknown	1	0
Connector Appliance	1	1
System or Application Event	1	1
ArcSight	6	1
Total	5009	5003

WEB CONSOLE

Accessible Monitoring & Platform Management

CONTENT

Unified | Actionable | Insight

ARCSIGHT LOGGER

Compliance | Search | Retention

ARCSIGHT ENTERPRISE SECURITY MANAGER

24x7 Real-time Monitoring & Correlation

ARCSIGHT INVESTIGATE

Hunt | Investigation

UEBA

User Entity Behavior Analytics

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER

Suite Management & Administration

TRANSFORMATION HUB

Information delivery

SMART/FLEX CONNECTORS

Data Collection, Enrichment, and Normalization



User



Cloud



App



Servers &
Workloads



Network



Endpoints

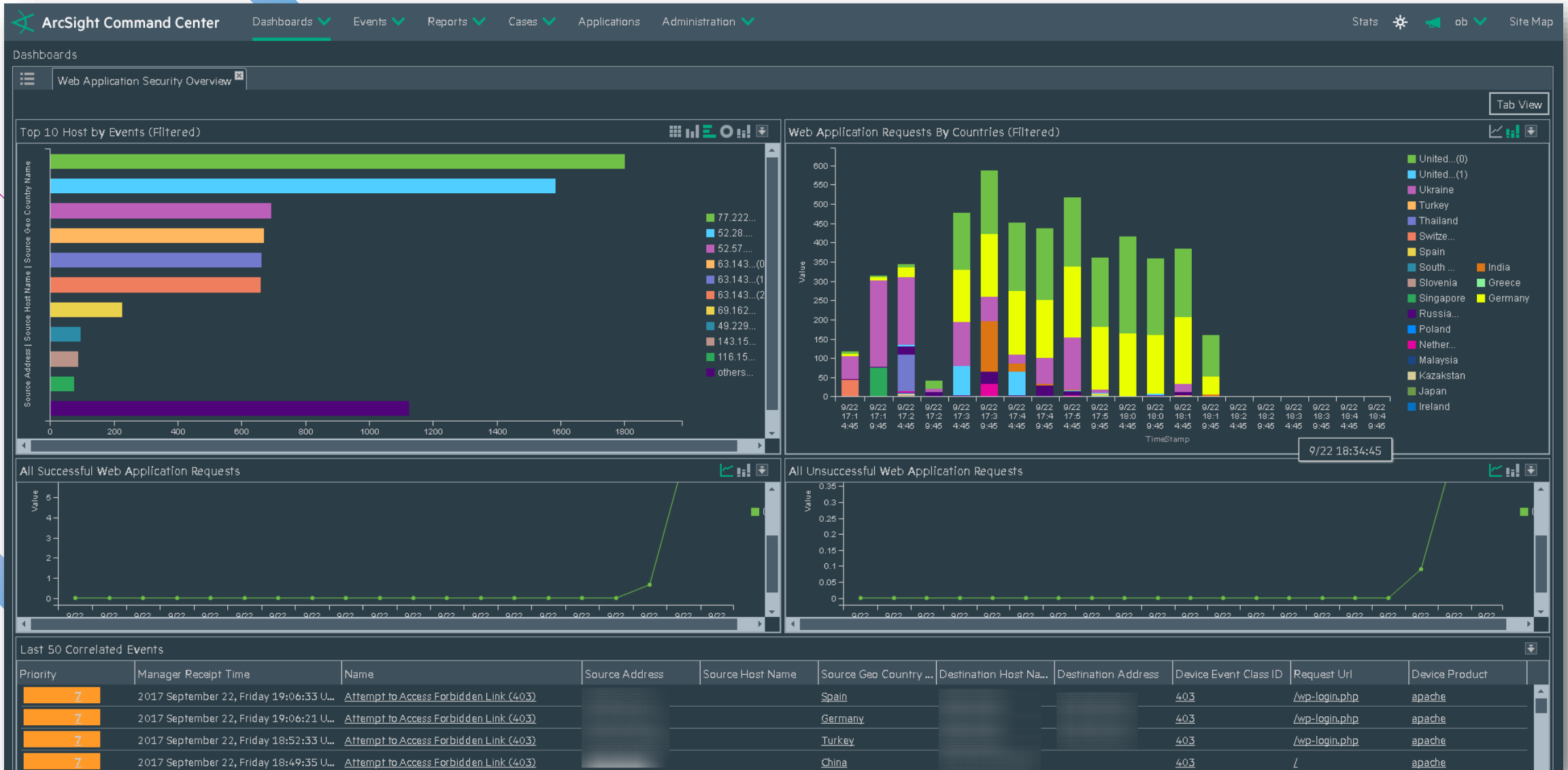


IoT



Physical

ArcSight ESM Command Center - Visualizations



WEB CONSOLE

Accessible Monitoring & Platform Management

CONTENT

Unified | Actionable | Insight

ARCSIGHT LOGGER

Compliance | Search | Retention

ARCSIGHT ENTERPRISE SECURITY MANAGER

24x7 Real-time Monitoring & Correlation

ARCSIGHT INVESTIGATE

Hunt | Investigation

UEBA

User Entity Behavior Analytics

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER

Suite Management & Administration

TRANSFORMATION HUB

Information delivery

SMART/FLEX CONNECTORS

Data Collection, Enrichment, and Normalization



User



Cloud



App



Servers &
Workloads



Network



Endpoints



IoT



Physical

All Fields Custom time range Start SNow - 1h Dynamic End SNow Dynamic

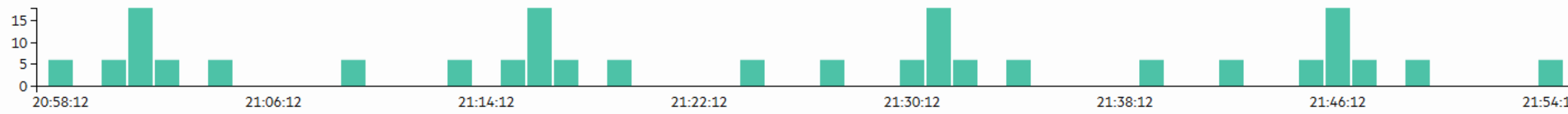
dgchung AND sourceHostName CONTAINS "finance_DB1"

Go! Advanced

Active Searches

192 events (Scanned: 377,407 events, 00:00.821)

1 bar = 1 minute



- Selected Fields (4)
deviceEventClassId 6
deviceProduct 1
deviceVendor 1
name 6

Table with columns: ent Device [UDP Receiver], Logger, deviceVendor, deviceProduct, deviceVersion, deviceEventClassId, name, agentAddress, agentHostName, agentType, agentZone. Contains 10 rows of event data.

Show RAW Enable Multi-select of field values.

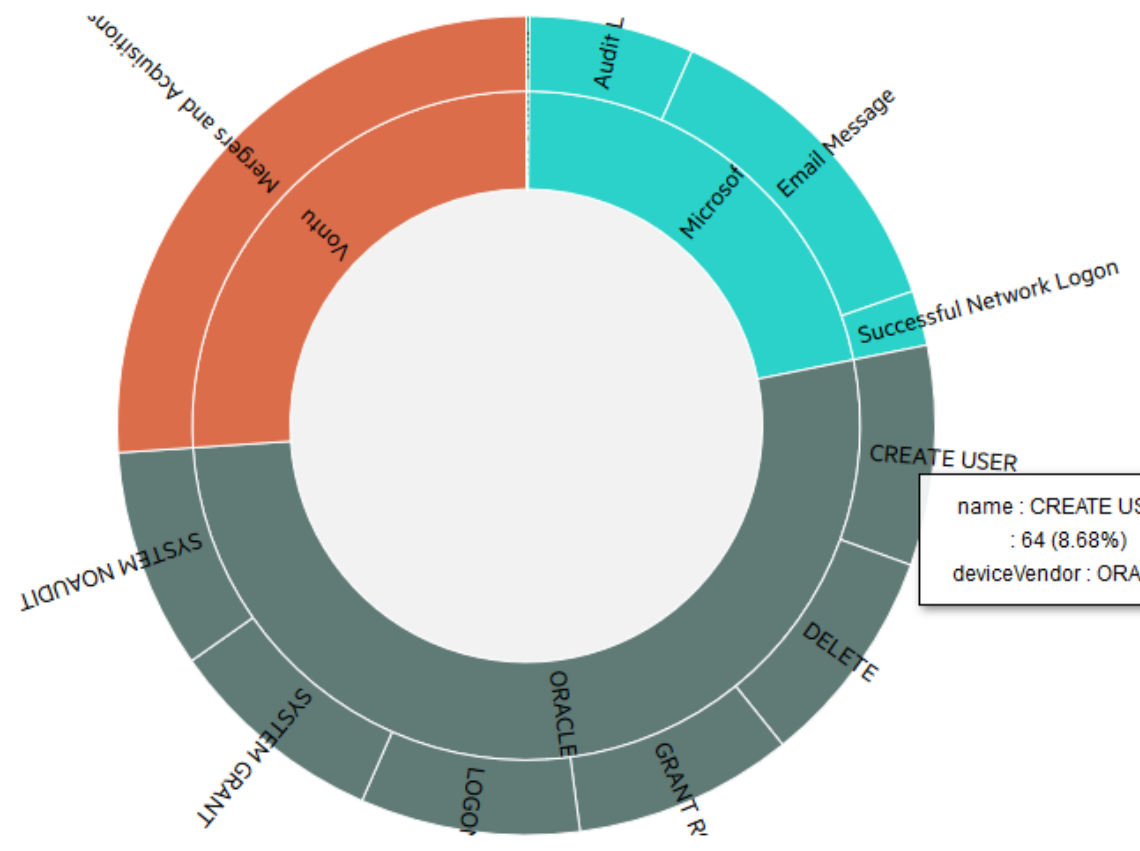
- Explorer
- Schedule Reports
- Design
 - Dashboards
 - New Report
 - Queries
 - Parameters
 - Parameter Value Groups
 - Template Styles
- Classic
 - Dashboards
 - New Report
- Administration
 - Deploy Report Bundler
 - Report Configuration
 - Report Category Filters
 - Report Categories
 - Job Execution Status
 - iPackager

Recent Reports dgchung x

dgchung

Adhoc Filters Edit Mode

dgchung's Data



name : CREATE USER
 : 64 (8.68%)
 deviceVendor : ORACLE

Grid Chart + Data Source: dgchung

WEB CONSOLE

Accessible Monitoring & Platform Management

CONTENT

Unified | Actionable | Insight

ARCSIGHT LOGGER

Compliance | Search | Retention

ARCSIGHT ENTERPRISE SECURITY MANAGER

24x7 Real-time Monitoring & Correlation

ARCSIGHT INVESTIGATE

Hunt | Investigation

UEBA

User Entity Behavior Analytics

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER

Suite Management & Administration

TRANSFORMATION HUB

Information delivery

SMART/FLEX CONNECTORS

Data Collection, Enrichment, and Normalization



User



Cloud



App



Servers &
Workloads



Network



Endpoints



IoT



Physical

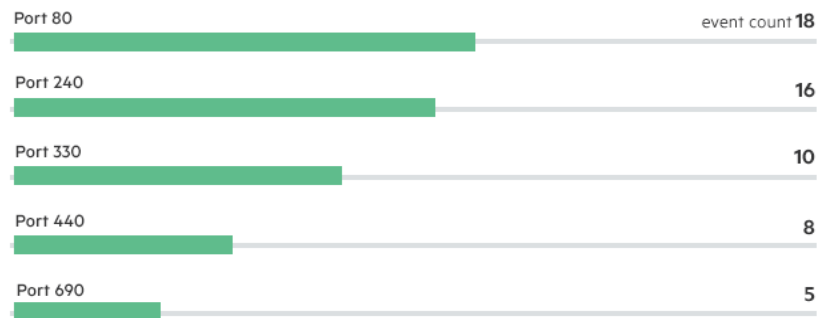
- DASHBOARD >
- SEARCH >
- INSIGHTS** >
- DNS Analytics
- Outliers
- IP Profiler**
- CONFIGURATION >
- ADMIN >

Hostname = 1.1.112.1

Last 24 hours PROFILE

Top 5 outgoing ports from the host (1.1.112.1)

Information about the number of ports displayed VS total ports



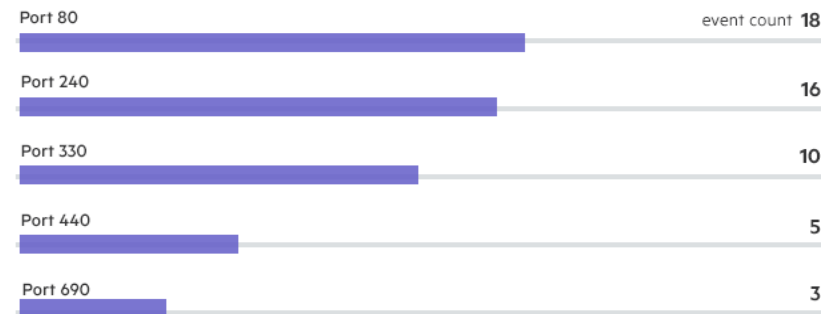
57 Event Count

60 Distinct Ports

15 Bytes Out

Top 5 Incoming ports to the host (1.1.112.1)

Information about the number of ports displayed VS total ports

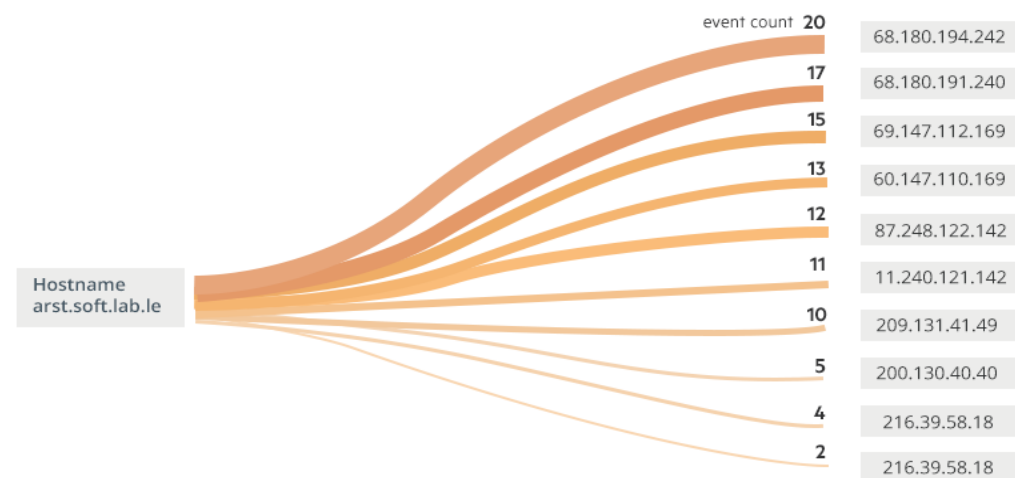


157 Event Count

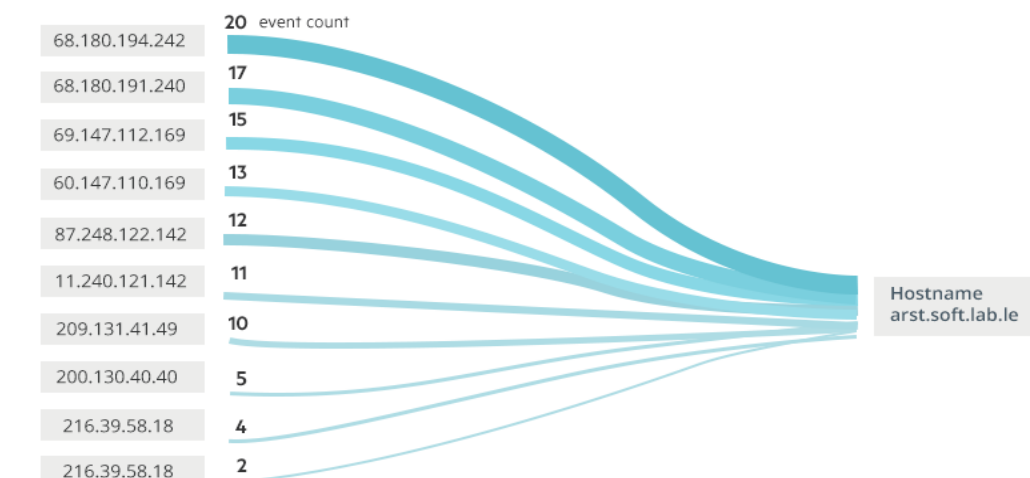
60 Distinct Ports

89 Bytes In

Top 10 Communication Paths from the host (arst.soft.lab.le)



Top Communication Paths to the host (arst.soft.lab.le)



WEB CONSOLE

Accessible Monitoring & Platform Management

CONTENT

Unified | Actionable | Insight

ARCSIGHT LOGGER

Compliance | Search | Retention

ARCSIGHT ENTERPRISE SECURITY MANAGER

24x7 Real-time Monitoring & Correlation

ARCSIGHT INVESTIGATE

Hunt | Investigation

UEBA

User Entity Behavior Analytics

SECURITY OPEN DATA PLATFORM

MANAGEMENT CENTER

Suite Management & Administration

TRANSFORMATION HUB

Information delivery

SMART/FLEX CONNECTORS

Data Collection, Enrichment, and Normalization



User



Cloud



App



Servers &
Workloads



Network



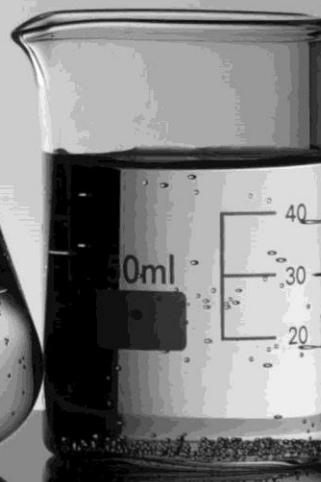
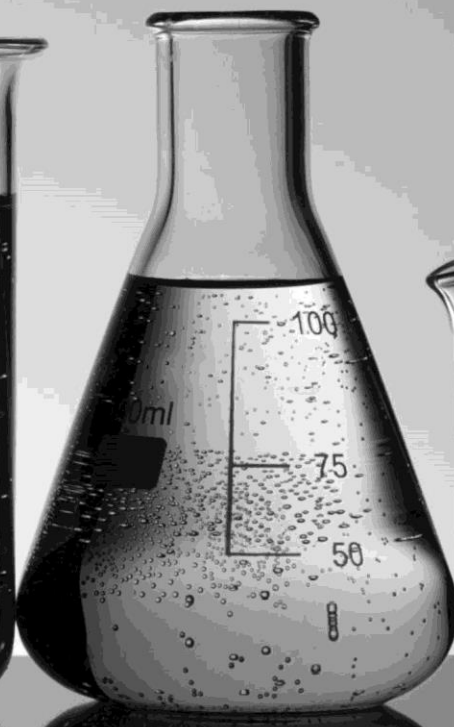
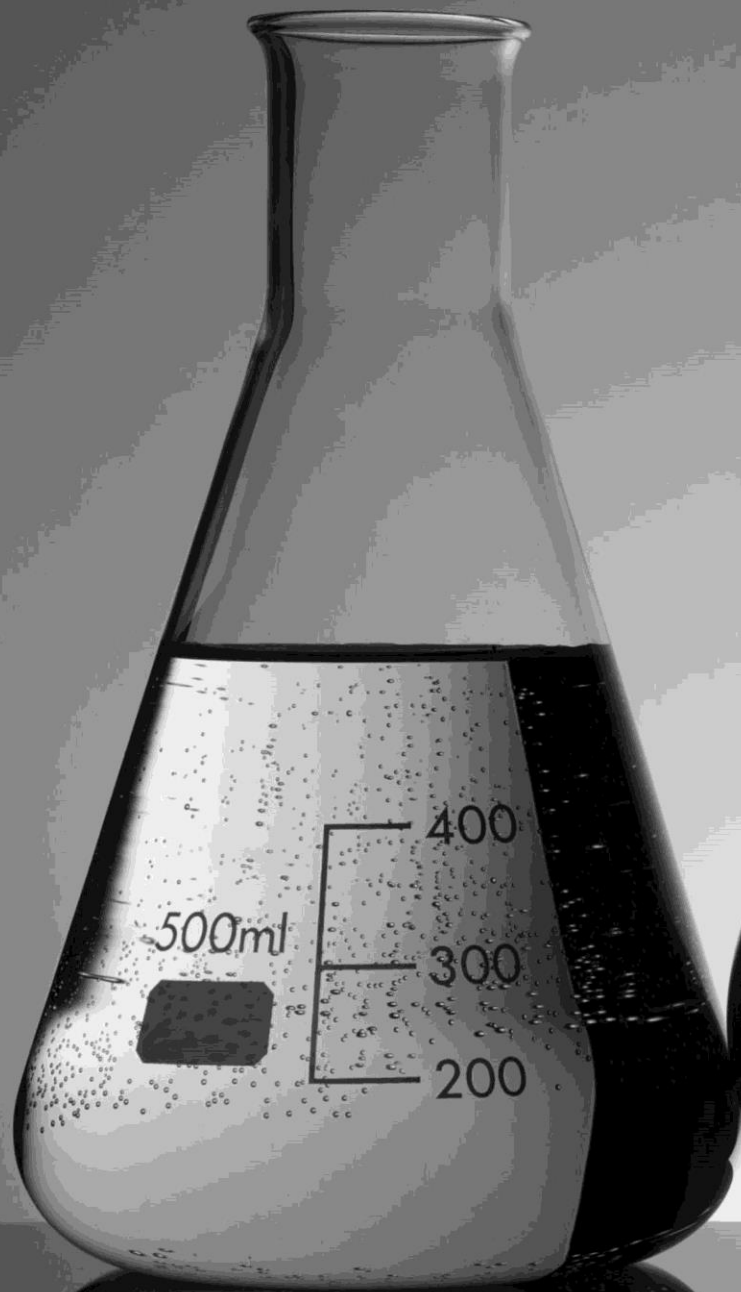
Endpoints



IoT



Physical



Requires Clarity Of Focus

1

Simple

2

Intelligent



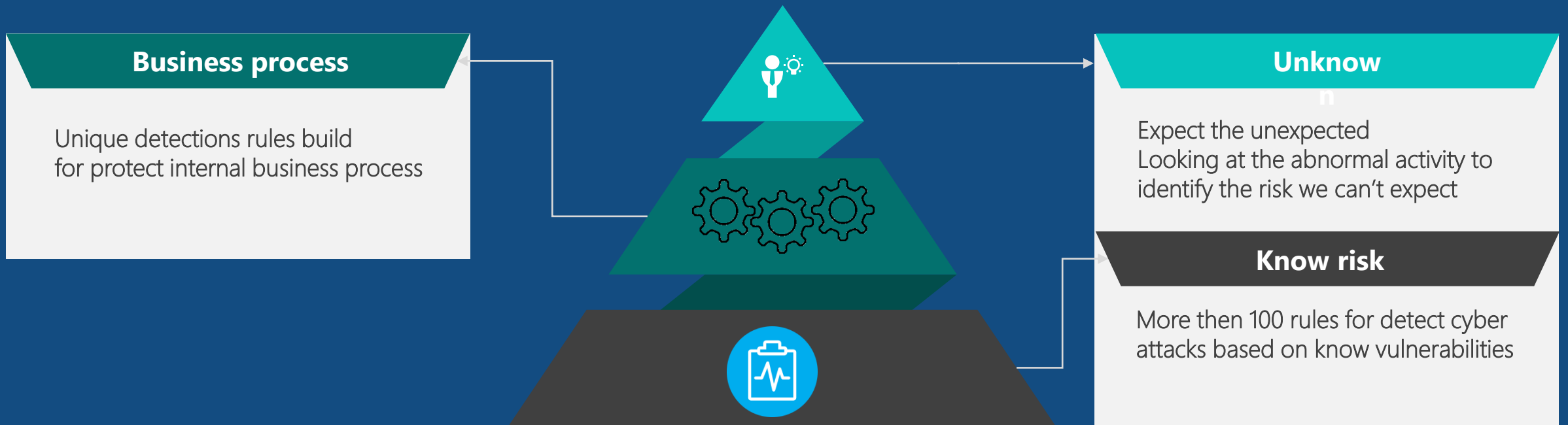
3

Open

4

Converged

Detection layers



Show all Techniques
 Real-time
Download

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Command-Line Interface	Image File Execution Options Injection	Extra Window Memory Injection	File Deletion	Hooking	Remote System Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Connection Proxy	Data Compressed	Data Encrypted for Impact
Spearphishing Link	PowerShell	Hooking	Image File Execution Options Injection	Disabling Security Tools	Credential Dumping	Network Service Scanning	Remote File Copy	Data Staged	Remote File Copy	Exfiltration Over Physical Medium	
Trusted Relationship	Scheduled Task	DLL Search Order Hijacking	Process Injection	Extra Window Memory Injection	Account Manipulation	System Network Configuration Discovery	Remote Services	Clipboard Data	Communication Through Removable Media	Exfiltration Over Other Network Medium	
Valid Accounts	Scripting	Scheduled Task	SID-History Injection	Image File Execution Options Injection	Brute Force	System Network Connections Discovery	Exploitation of Remote Services	Screen Capture	Web Service	Exfiltration Over Alternative Protocol	
Spearphishing Attachment	User Execution	Valid Accounts	Hooking	Process Injection	Network Sniffing	Account Discovery		Email Collection	Commonly Used Port	Exfiltration Over Command and Control Channel	
Spearphishing via Service	Service Execution	Account Manipulation	DLL Search Order Hijacking	Deobfuscate/Decode Files or Information		Network Sniffing			Uncommonly Used Port		
	Exploitation for Client Execution	Create Account	Scheduled Task	DLL Search Order Hijacking							
	Local Job Scheduling	New Service	Valid Accounts	DLL Side-Loading							
		Modify Existing Service	New Service	Process Hollowing							
		Kernel Modules and Extensions	Exploitation for Privilege Escalation	Scripting							
		Local Job Scheduling		Valid Accounts							
				Web Service							
				Code Signing							

DEMO

MITRE ATT&CK Landing Page

How we get there

Reduce deployment time

Reduce knowledge burden

Align deployment options between on-premise, hybrid, and SaaS

Improve UI and overall user experience

MICRO FOCUS

Settings

Show all Techniques: Disabled

Coverage: Machine Learning

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	Control Panel Items	Credential Dumping	Network Service Scanning	Replication Through Removable Media	Email Collection	Remote File Copy	Automated Exfiltration	
Exploit Public-Facing Application	CMSTP	Hooking	Hooking	CMSTP	Hooking	Permission Groups Discovery	Remote File Copy	Audio Capture	Multiband Communication	Data Encrypted	
Drive-by Compromise	Execution through Module Load	Create Account	Bypass User Account Control	Bypass User Account Control	Forced Authentication	Password Policy Discovery	Remote Services	Automated Collection	Custom Cryptographic Protocol	Data Transfer Size Limits	
Valid Accounts	Execution through API	Accessibility Features	Accessibility Features	DLL Search Order Hijacking	Credentials in Files	Security Software Discovery	Pass the Ticket	Video Capture	Data Encoding	Exfiltration Over Physical Medium	
Spearphishing Attachment	InstallUHL	DLL Search Order Hijacking	DLL Search Order Hijacking	InstallUHL	Input Capture	File and Directory Discovery	Remote Desktop Protocol	Data from Information Repositories	Multi-Stage Channels	Exfiltration Over Alternative Protocol	
Trusted Relationship	Command-Line Interface	AppCert DLLs	AppCert DLLs	Valid Accounts	Kerberoasting	Network Share Discovery	Exploitation of Remote Services	Data from Network Shared Drive	Multilayer Encryption	Exfiltration Over Command and Control Channel	
	LSASS Driver	Authentication Package	Valid Accounts	Access Token Manipulation	Exploitation for Credential Access	Account Discovery	Distributed Component Object Model	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	
	Dynamic Data Exchange	Valid Accounts	Access Token Manipulation	Image File Execution Options Injection	Credentials in Registry	Remote System Discovery	Logon Scripts	Data from Local System	Commonly Used Port	Scheduled Transfer	
	Exploitation for Client Execution	Image File Execution Options Injection	Image File Execution Options Injection	BITS Jobs	Brute Force	Application Window Discovery	SSH Hijacking	Data Staged	Fallback Channels	Data Compressed	
	Graphical User Interface	AppInit DLLs	AppInit DLLs	DLL Side-Loading		Query Registry	Pass the Hash	Man in the Browser	Custom Command and Control Protocol		
		Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking		Peripheral Device Discovery		Input Capture	Connection Proxy		
		BITS Jobs	File System Permissions Weakness	Binary Padding							
		LSASS Driver									
		Component Object Model Hijacking									
		Logon Scripts									
		File System Permissions Weakness									

MITRE ATT&CK Packages

- Available as part of Default Content in ESM 7.2
- Will also be made available as a separate downloadable package @ Marketplace – targeted for October 2019



Dashboards | MITRE ATT&CK Overview

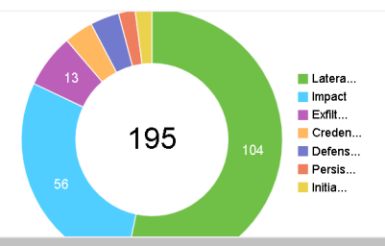
Tab View

Last MITRE ATT&CK Events

MITRE ID	Incident Time	Name	Agent Severity	Attacker Address	Target Address	Target Host Name	Target Zone Name	Target Port	Target User Name	Priority
T1048	2019 September 9, Monday 00:13:...	Egress DNS Communications Passe...	Medium	10.0.112.110	1.9.165.83		1.0.0.0-1.255.255.255 (APNIC)	53		5
T1089	2019 September 9, Monday 00:12:...	Audit Cleared Leg	High		10.0.112.110	finance1	RFC1918: 10.0.0.0-10.255.255.255		JOSHC	7
T1498	2019 September 9, Monday 00:12:...	DoS Activity Detected by IDS	Medium	10.0.112.251	10.0.112.119		RFC1918: 10.0.0.0-10.255.255.255			6
T1210	2019 September 9, Monday 00:10:...	Exploit Attempt Detected by IDS	Very-High	10.0.112.115	10.0.112.6		RFC1918: 10.0.0.0-10.255.255.255			10
T1210	2019 September 9, Monday 00:09:...	Exploit Attempt Detected by IDS	Very-High	10.0.112.115	10.0.113.84		RFC1918: 10.0.0.0-10.255.255.255			10
T1210	2019 September 9, Monday 00:09:...	Exploit Attempt Detected by IDS	Very-High	10.0.112.115	10.0.112.101		RFC1918: 10.0.0.0-10.255.255.255			10

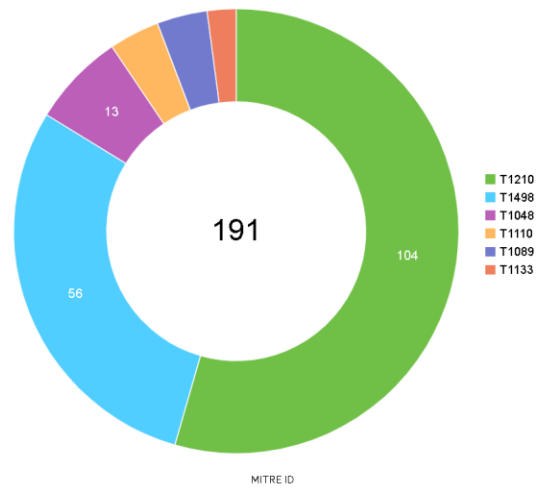
Data time range: 09/08 22:06:44 - 09/09 00:46:33 Data last refreshed: 09/09 00:46:33

MITRE by Tactic



Data last refreshed: 09/09 00:46:33

MITRE by ID



Data last refreshed: 09/09 00:46:33

MITRE ATT&CK Overview Dashboard

Command Center

[Dashboards](#) |
 [Events](#) |
 [Reports](#) |
 [Cases](#) |
 [Administration](#)

MITRE ATT&CK Overview

Last MITRE ATT&CK Events

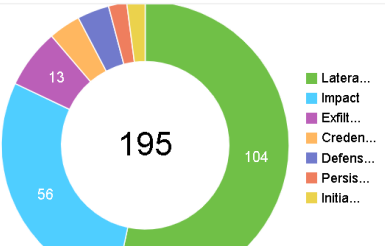
MITRE ID	Incident Time	Name	Agent Severity	Attacker Address	Target Address	Target Host Name	Target Zone Name
T1048	2019 September 9, Monday 00:13:...	Egress DNS Communications Passe...	Medium	10.0.112.110	1.9.165.83		1.0.0.0-1.255.255.255 (APNIC)
T1089	2019 September 9, Monday 00:12:...	Audit Cleared Log	High		10.0.112.110	finance1	RFC1918: 10.0.0.0-10.255.255.255
T1498	2019 September 9, Monday 00:12:...	DoS Activity Detected by IDS	Medium	10.0.112.251	10.0.112.119		RFC1918: 10.0.0.0-10.255.255.255
T1210	2019 September 9, Monday 00:10:...	Exploit Attempt Detected by IDS	Very-High	10.0.112.115	10.0.112.6		RFC1918: 10.0.0.0-10.255.255.255
T1210	2019 September 9, Monday 00:09:...	Exploit Attempt Detected by IDS	Very-High	10.0.112.115	10.0.113.84		RFC1918: 10.0.0.0-10.255.255.255
T1210	2019 September 9, Monday 00:09:...	Exploit Attempt Detected by IDS	Very-High	10.0.112.115	10.0.112.101		RFC1918: 10.0.0.0-10.255.255.255

Data time range: 09/08 22:06:44 - 09/09 00:46:33 Data last refreshed: 09/09 00:46:33

MITRE by Tactic

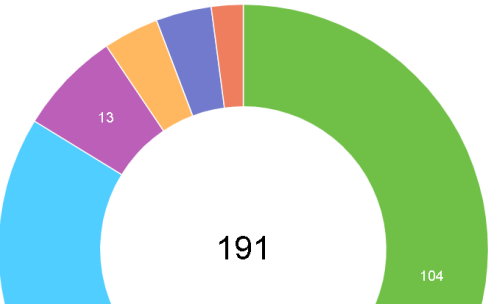
MITRE ATT&CK Matrix Overview Dashboard

MITRE ATT&CK-tagged correlated alerts/events and specific dashboards per MITRE Tactic and MITRE Technique ID are provided OOTB and as a downloadable MITRE ATT&CK Content Pack.

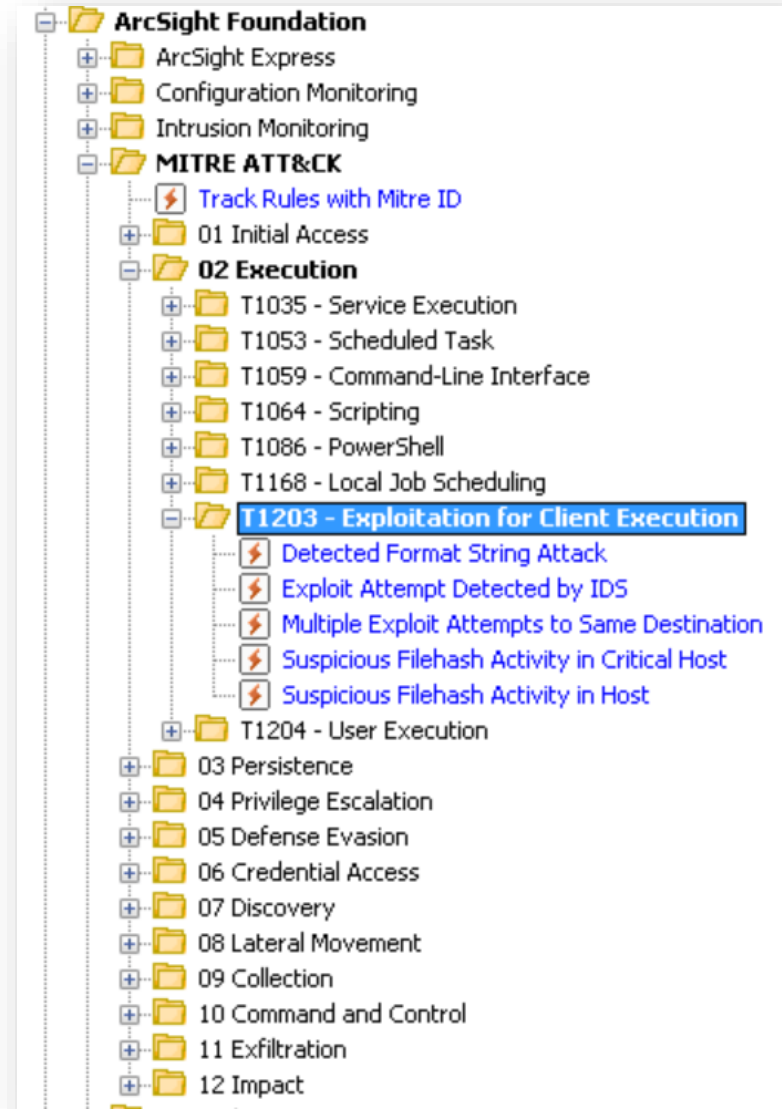


Data last refreshed: 09/09 00:46:33

MITRE by ID



MITRE ATT&CK Framework – Content Pack



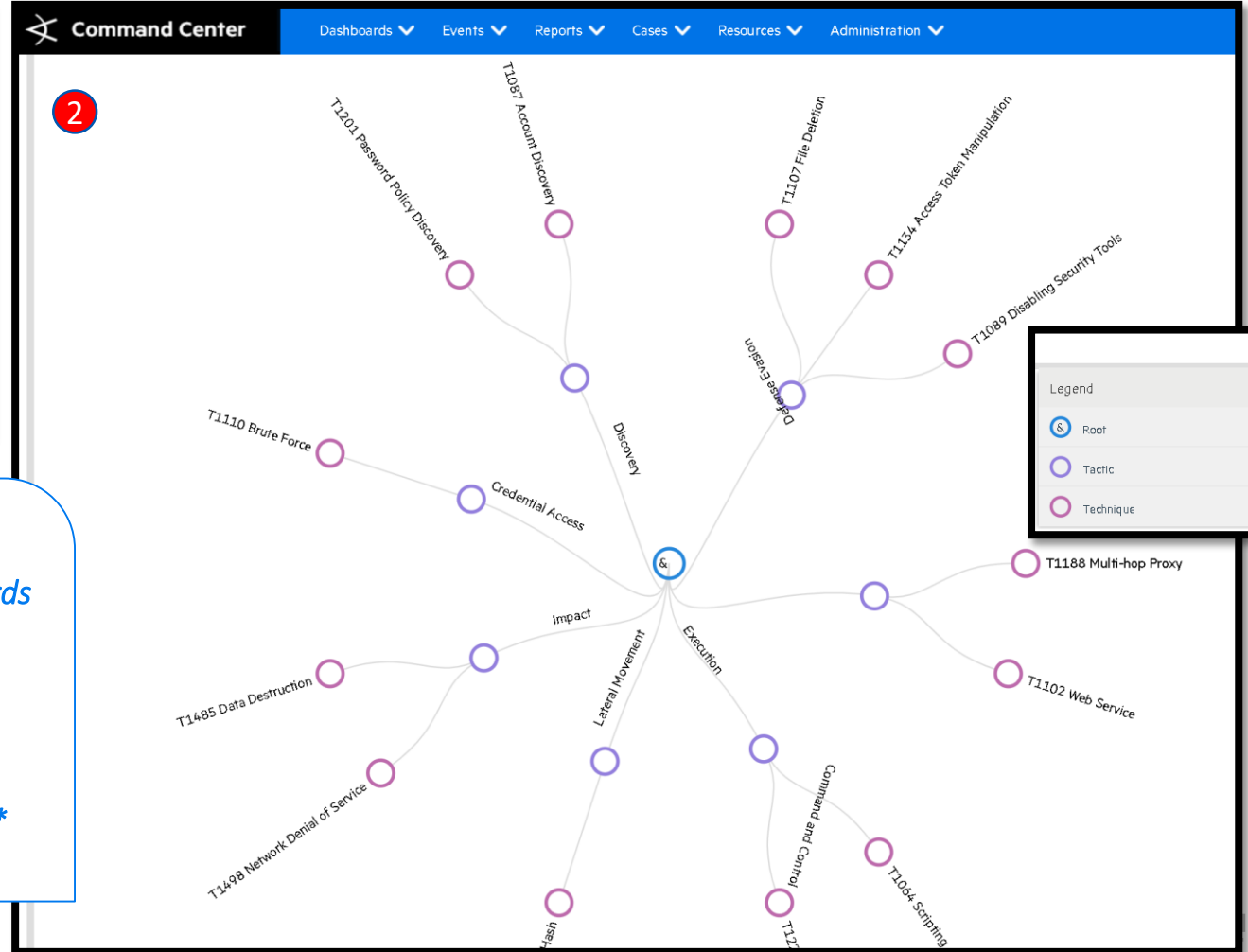
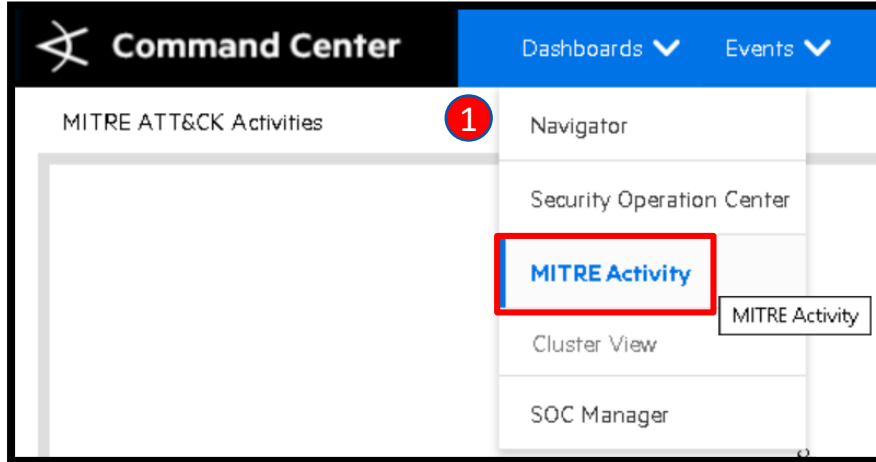


MITRE ATT&CK Visualizations

ESM 7.2 [targeted for November 2019]

MITRE ATT&CK Activity Dashboard

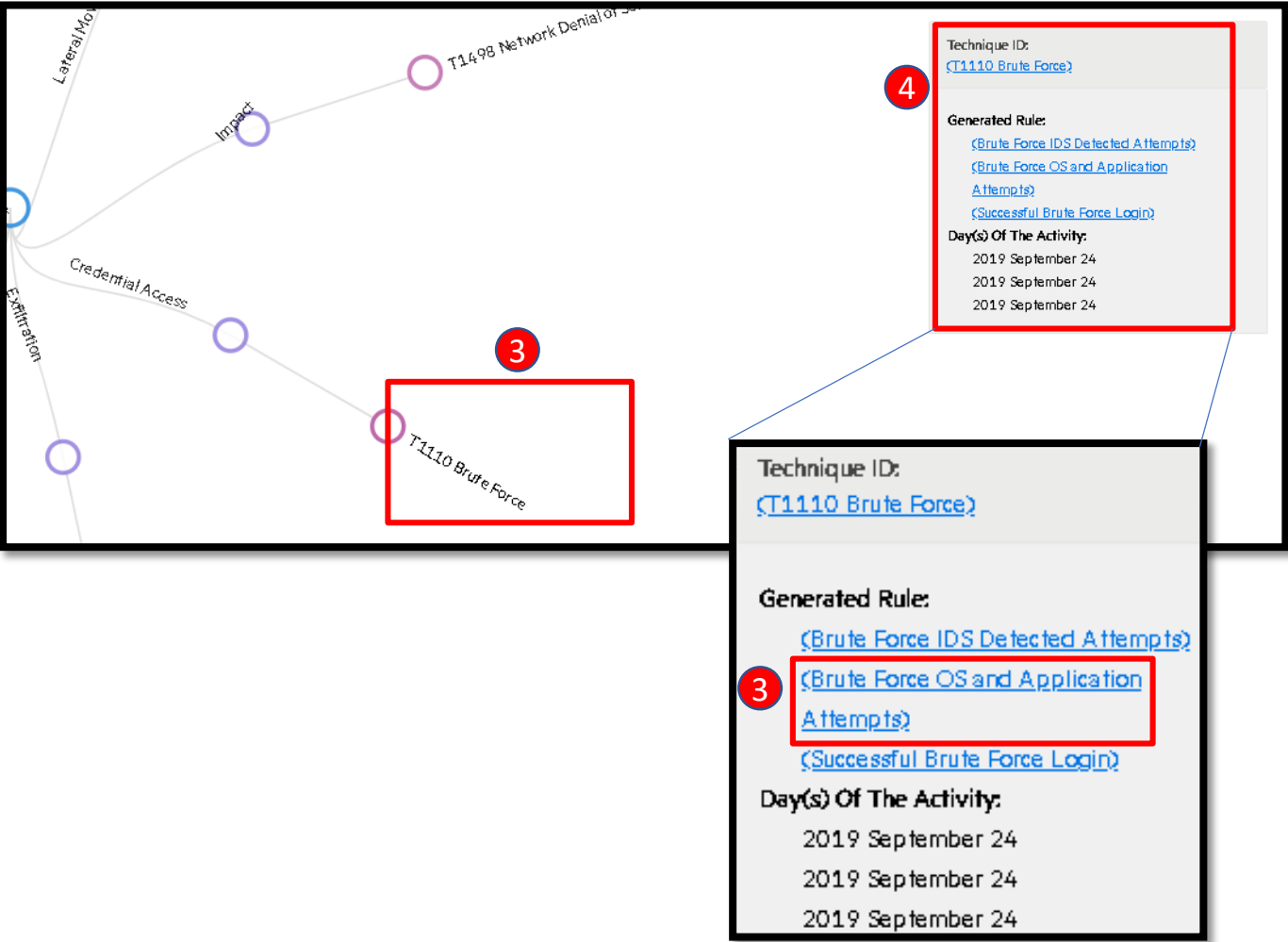
A special visualization, showing a tree-view structure: MITRE ATT&CK tactics in the middle + techniques as the branches.



MITRE ATT&CK Activity Dashboard with Drilldown

- 1) User selects "MITRE Activity" from the main dashboards
- 2) Within the tree visualization, user selects a specific technique.
- 3) All real-time correlation rules related to that alert are shown on the right, along with more MITRE-related information.
- 4) When clicked, a special channel opens up with **ONLY** those events related to the selected technique.

MITRE ATT&CK Activity Dashboard



MITRE ATT&CK Activity Dashboard Drilldown Steps

- 1) User selects "MITRE Technique" from the main dashboard. E.g. "Brute Force"
- 2) All real-time correlation *rules* related to that alert are shown on the right, along with more MITRE-related information.
- 3) When clicked on a specific 'rule' (e.g. "Brute Force OS and Application Attempts"), a special channel opens up with *ONLY* those events related to that rule.

MITRE ATT&CK Activity Dashboard

Command Center

Dashboards ▾ Events ▾ Reports ▾ Cases ▾ Resources ▾ Administration ▾

Active Channel - MITRE Activity_1569401539304

MITRE Activity_1569401496931 MITRE Activity_1569401539304

Save As... Start Time = 2019 September 23, Monday 10:52:20 UTC+2 End Time = 2019 September 25, Wednesday 10:52:20 UTC+2

Visualize Events

Event List

View Details Add to Case Annotate Mark As Reviewed Add to Active List

End Time ▾	Name	Attacker Address	Target Address	mitreID	mitreName	tacticName	Priority
2019 September 24, Tuesday 13:50:29 UTC+2	Brute Force OS and Application Attempts	10.0.113.27	172.16.1.10	'T1110'	'Brute Force'	'Credential Access'	5
2019 September 24, Tuesday 13:48:39 UTC+2	Brute Force OS and Application Attempts	10.0.110.34	10.0.112.200	'T1110'	'Brute Force'	'Credential Access'	6
2019 September 24, Tuesday 13:48:18 UTC+2	Brute Force OS and Application Attempts	10.0.111.5	10.0.111.6	'T1110'	'Brute Force'	'Credential Access'	7
2019 September 24, Tuesday 13:48:16 UTC+2	Brute Force OS and Application Attempts	10.0.111.23	10.0.111.5	'T1110'	'Brute Force'	'Credential Access'	7

MITRE ATT&CK Activity Dashboard with Drilldown

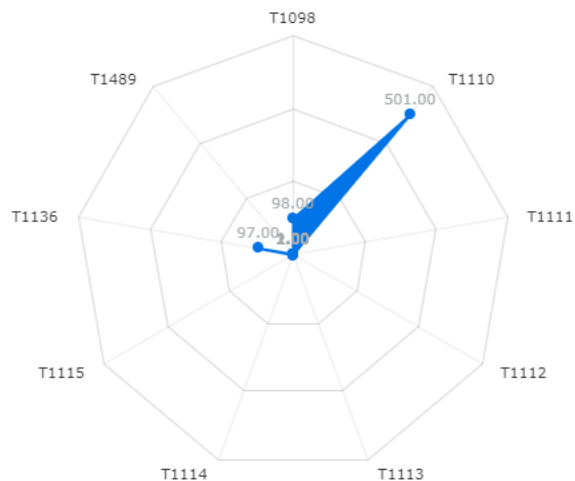
- 1) The special active channel opens up **ONLY** those special events related to the rule, associated with the chosen MITRE Technique: "Brute Force"
- 2) All other MITRE ATT&CK artifacts are displayed in the channel.

- Explorer
- Report Status
- Schedule Reports
- Design >
- Classic >
- Administration >

MITRE Attacks Events Overview

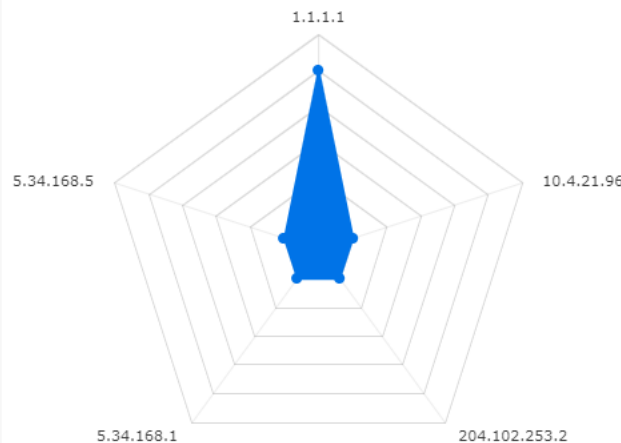
MITRE IDs

MITRE ID's



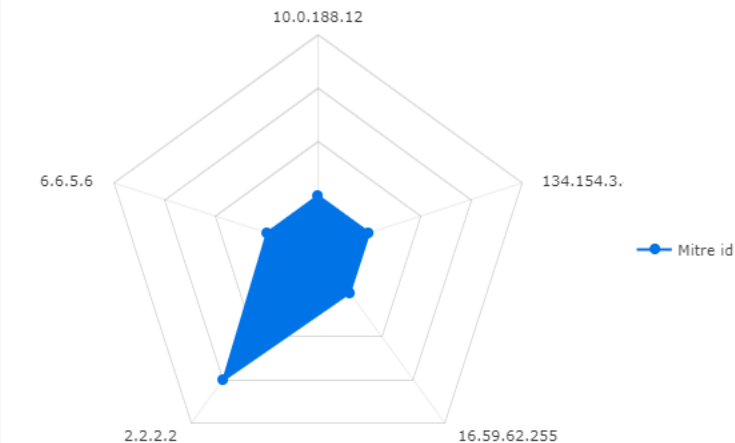
Source Addresses with Unique MITRE IDs

Source Addresses with Unique MITRE ID's



Destination Addresses with Unique MITRE IDs

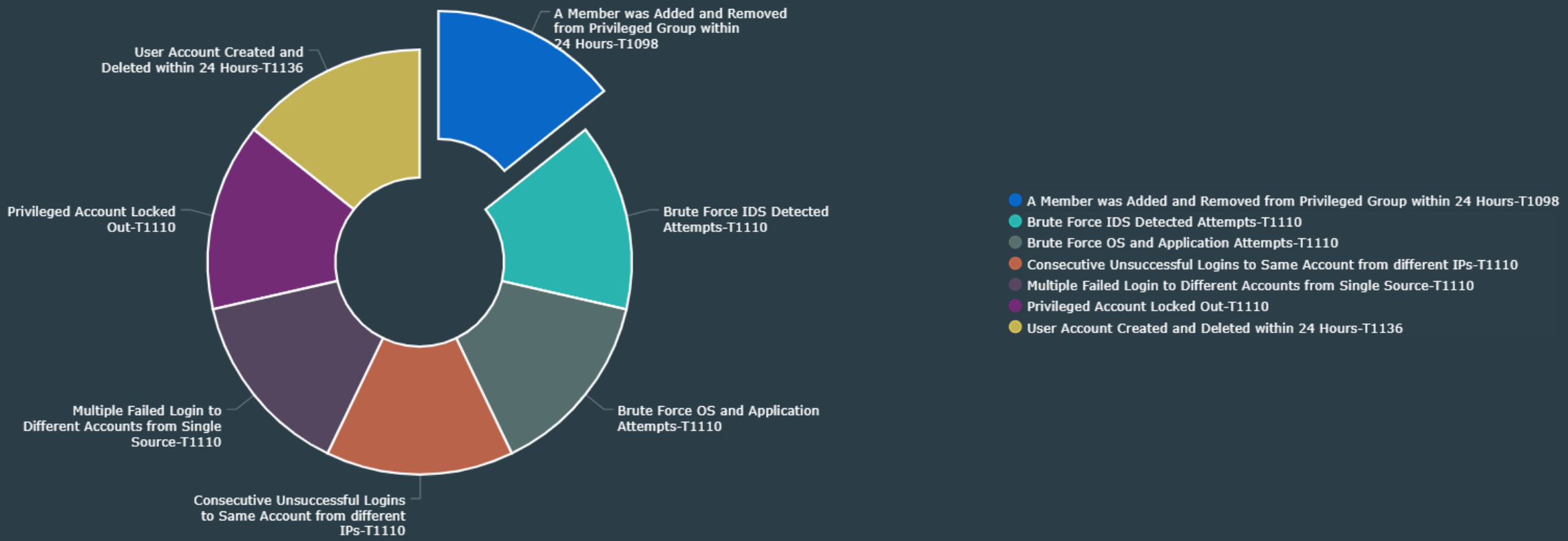
Destination Addresses with Unique MITRE ID's



(*) DISCLAIMER:
 This MITRE ATT&CK Events Overview report from ArcSight Logger is targeted for November 2019.

MITRE Attacks Events Overview

Top Reported Rules with MITRE IDs

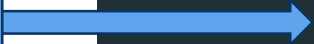


Mitre id |

- Explorer
- Report Status
- Schedule Reports
- Design >
- Classic >
- Administration >

Name	Object Type	Report Type	Report Format
Explorer			
Search Here			
Report			
(Root)			
Cloud			
Default Reports			
Device Monitoring			
Foundation			
Configuration Monitoring			
Intrusion Monitoring			
MITRE Monitoring			
MITRE Attacks Events - Drill Down by Destination Address	REPORT	AD HOC	SMART
MITRE Attacks Events - Drill Down by Destination User	REPORT	AD HOC	SMART
MITRE Attacks Events - Drill Down by Event Name	REPORT	AD HOC	SMART
MITRE Attacks Events - Drill Down by Hour	REPORT	AD HOC	SMART
MITRE Attacks Events - Drill Down by Source Address	REPORT	AD HOC	SMART
MITRE Attacks Events - Drill Down by Source User	REPORT	AD HOC	SMART
MITRE Attacks Events Overview	REPORT	AD HOC	SMART
NetFlow Monitoring			
Network Monitoring			
Vulnerabilities			
Logger Administration			
OWASP			
SANS Top 5			

New Out of the Box MITRE Reports



(*) DISCLAIMER:
This MITRE ATT&CK Events Overview report from ArcSight Logger is targeted for November 2019.

MISP CRCL: Malware Information Sharing Platform



circl.lu
Computer Incident
Response Center
LUXEMBOURG



**CIRCL
MISP**
Threat Sharing

- 01.** Threat sharing platform – API integration
- 02.** Free, Open Source & MITRE ATT&CK Compatible
- 03.** 6,000+ organisations worldwide are using MISP

MISP CIRCL is a best-of-breed Public TI feed.

5 x ESM Active Lists

Always up-to-date through MISP CRCL Model Import Connector.

Name: Suspicious Email List
Start Time : 15 Jun 2019 12:30:41 UTC
End Time : 13 Sep 2019 12:30:41 UTC
Last Update: 13 Sep 2019 12:30:41 UTC
Filter: No Filter

Suspicious Email List @ ArcSight ESM

email	indicatorType	lastDetectTime	description	extrainfo	actors	reference	threatLevel	mitreAttack
JOSTEIN.SOLHEIM@LOFOTK...	suspicious	3/21 5:53:50	Unknown Malspam Run (2019-03-20) Mastercard Authorization			Payload delivery	Low	
NENIA.CANOV@PHARMAPLU...	suspicious	3/20 6:11:46	Unknown Malspam Run (2019-03-20) Mastercard Authorization			Payload delivery	Low	
SERVICE@EFAFX.DELIVERY	trickbot	3/20 6:11:46	TrickBot Malspam Run (2019-03-19) You have a new eFax message!	sending address		Payload delivery	Low	
IQONUDJUJIPIL1991@O2.PL	danabot	3/8 5:52:57	BrushLoader Malspam Run (2019-03-07) Informacja o zbliaVajA...cy...	Return Path: <iqonudjujipil1991...>		Payload delivery	Low	
JUSUCOOWISOZOVG@O2.PL	danabot	3/8 5:52:57	BrushLoader Malspam Run (2019-03-07) Informacja o zbliaVajA...cy...			Social network	Low	
MISWSWANG8107@GMAIL.COM	suspicious	5/31 12:09:04	US-CERT Alert (TA18-1494) HIDDEN COBRA &E Joana Backdoor Tro...	Enriched via the stximport module	Lazarus Group	Payload delivery	Low	
REDHAT@GMAIL.COM	suspicious	5/31 12:09:04	US-CERT Alert (TA18-1494) HIDDEN COBRA &E Joana Backdoor Tro...	Enriched via the stximport module	Lazarus Group	Payload delivery	Low	
BENOIT.FILION.2@BULVALA.CA	suspicious	10/25 20:51:00	OSINT: New Techniques to Uncover and Attribute Cobalt Gang Commo...	Spooft email sender	Cobalt	Payload delivery	Low	
BILL@VERTICALWEBMEDIA...	suspicious	10/25 20:51:00	OSINT: New Techniques to Uncover and Attribute Cobalt Gang Commo...	Spooft email sender	Cobalt	Payload delivery	Low	
CHRISTOPH.DANZ@DSKBAN...	suspicious	3/18 20:59:29	New suspected Cobalt campaigns		Cobalt	Payload delivery	Medium	
DOMINIQUE.DENIS-BERUBE...	suspicious	10/25 20:51:00	OSINT: New Techniques to Uncover and Attribute Cobalt Gang Commo...	Spooft email sender	Cobalt	Payload delivery	Low	
EVA.OLOFSSON@DSKBANK.UK	malspam	3/18 20:59:29	New suspected Cobalt campaigns		Cobalt	Payload delivery	Medium	
INFO@DSKBANK.UK	malspam	3/18 20:59:29	New suspected Cobalt campaigns		Cobalt	Payload delivery	Medium	
JAN.LARSSON@DSKBANK.UK	malspam	3/18 20:59:29	New suspected Cobalt campaigns		Cobalt	Payload delivery	Medium	
INFOCENTRE.GOV@BK.RU	suspicious	8/13 15:46:22	OSINT - Recent Cloud Atlas activity	Some emails used by the attackers	Cloud Atlas	Payload delivery	Low	
INFOCENTRE.GOV@MAIL.RU	suspicious	8/13 15:46:22	OSINT - Recent Cloud Atlas activity	Some emails used by the attackers	Cloud Atlas	Payload delivery	Low	
MIDDLEEASTEYE@ASIA.COM	suspicious	8/13 15:46:22	OSINT - Recent Cloud Atlas activity	Some emails used by the attackers	Cloud Atlas	Payload delivery	Low	
SIMB@2019@GMAIL.RU	suspicious	8/13 15:46:22	OSINT - Recent Cloud Atlas activity	Some emails used by the attackers	Cloud Atlas	Payload delivery	Low	
WORLD_OVERVIEW@POLITI...	suspicious	8/13 15:46:22	OSINT - Recent Cloud Atlas activity	Some emails used by the attackers	Cloud Atlas	Payload delivery	Low	
AKKLP@126.COM	apt	8/8 10:07:52	APT41: A Dual Espionage and Cyber Crime Operation		APT41	Payload delivery	High	
AKKLP@163.COM	apt	8/8 10:08:05	APT41: A Dual Espionage and Cyber Crime Operation		APT41	Payload delivery	High	

Suspicious Domain List @ ArcSight ESM

Name: Suspicious Domain List
Start Time : 15 Jun 2019 12:34:11 UTC
End Time : 13 Sep 2019 12:34:11 UTC
Last Update: 13 Sep 2019 12:32:57 UTC
Filter: No Filter

domain	indicatorType	lastDetectTime	description	actors	reference	threatLevel	mitreAttack
torrent-stel.space	suspicious	8/29 7:41:20	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
torrent-supd.space	suspicious	8/29 7:41:20	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
babyboyto-onli...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
center.nmsvllag...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
chart.healthcare-i...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
compasec.com	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
control.mimepan...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
control.mimepanel.org	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
daily.mailrent...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
dream.zepot.c...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
dsmfanpage.pr...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
dname.europe...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
finance.globaled...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
forcan.hausblow...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
grek.freetaxbr.c...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
info.audioexp.com	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
indicalization.com	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
item.amazonon...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
item.babytoy-o...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
item.burgenmap...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
login.allionhealth...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
nenorustru.com	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
missions.soporte...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
newflow.babytoy...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
press.premilist.com	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
promise.miniatu...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
rain.nmsvllag.c...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
store.usfsecr...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
support.slovakm...	apt	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
translate.europe...	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158
unv.inchiall.com	apt	7/18 12:55:31	Okrum: Ke3chang group targets diplomatic missions (OSINT) Mirage		Network activity	Medium	T1035 T1060 T1140 T107 T1158

Name: Suspicious Hash List
Start Time : 15 Jun 2019 12:41:28 UTC
End Time : 13 Sep 2019 12:41:28 UTC
Last Update: 13 Sep 2019 12:41:28 UTC
Filter: No Filter

Suspicious Filehashes @ ArcSight ESM

hashValue	indicatorType	lastDetectTime	description	extrainfo	actors	reference	threatLevel	mitreAttack
f628a0e9426713471421174f705e731c56ff8956cd840cd28c7c329	android banker [...]	9/4 7:59:41	Cerberus mobile banking malware			Payload delivery	Low	
f628a0e9426713471421174f705e731c56ff8956cd840cd28c7c329	android banker [...]	9/4 7:59:41	Cerberus mobile banking malware			Payload delivery	Low	
Saa2604926e214a4292fd0dddb278697a81aad183f18428faae40228998...	android malware	9/3 14:31:03	Popular Apps on Google Play fou...	note.idea.netopad.pro		Payload delivery	Low	
2749248ff72ab14b0650c041c8ea5	phishing/keylogger	9/3 7:50:53	Phishing - H Worm & Key Login...			Initial Payload	Low	
5d230636fa75d8f8d0d58811a129c73a385467d	phishing/keylogger	9/3 7:50:52	Phishing - H Worm & Key Login...			Initial Payload	Low	
f616a513222141f0d58acfd2b24280d07ced9c74e64d69c81b0bab3df6f	phishing/keylogger	9/3 7:50:52	Phishing - H Worm & Key Login...			Initial Payload	Low	
49c52ae8ab12b3a854ec72004f14	trojan	9/3 7:03:59	Threat Intel file report: 49c52ae8...			Payload delivery	Low	
c669e68c744d0f8073ea5dbaaa0ae3c139538470ca308d1f56d28f230c	orcus rat[reveng...	9/2 19:11:29	OSINT - RAT Ratatouille - Backdo...			ZIP Delivery hashes	Low	T1192 T1165 T1483...
d65ca75292ac3a6eaa08b59c11b3b2ad418998bee5e3c8f08b1ec8955d42a	orcus rat[reveng...	9/2 19:09:42	OSINT - RAT Ratatouille - Backdo...			ZIP Delivery hashes	Low	T1192 T1165 T1483...
b40909ac0b70b7bd82465cdf761a6b4e0df55b894dd42290e3f72cb4280fa...	suspicious	8/30 7:22:19	Inside the APT28 DLL Backdoor B...			Artifacts dropped	High	
28497c50d65c9f1d0233f193a43014497adddb1a8e75db0ceefb3d4ede02	more_eggs	8/29 12:50:33	More_eggs, Anyone? Threat Acto...	A70613FF7F5DE98.bt		Payload delivery	Undefined	
7887f540c17580c44cab78e25a3a186ef1e7439045e23e32057485...	more_eggs	8/29 12:50:33	More_eggs, Anyone? Threat Acto...	37831e465728a913acab31...		Payload delivery	Undefined	
807162a497398508dcd1c035e4bc2da3952769371b800c99e2aa2430f	more_eggs	8/29 12:50:33	More_eggs, Anyone? Threat Acto...	62522E98ECDD28459.bt		Payload delivery	Undefined	
b357371f054823836d9c5325603f01c38e549f813206af699ced8a...	more_eggs	8/29 12:50:33	More_eggs, Anyone? Threat Acto...	5795CA3C75F7F.bt		Payload delivery	Undefined	
d9a2451f0502606226c345a109025916e8f5f24ef75b87ada26eddc9	more_eggs	8/29 12:50:33	More_eggs, Anyone? Threat Acto...	Metasploit Shellcode Loader		Payload delivery	Undefined	
034fed3f3c66fd3d137caced77a06178926c63fa1a8c8db9d18540821	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layer...		Gamaredon Group	Payload delivery	High	T1106 T1053 T1064...
1093b834938d754718144832c3ca95211c75af98701745cd319e25144...	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layer...		Gamaredon Group	Payload delivery	High	T1106 T1053 T1064...

Name: Suspicious URL List
Start Time : 15 Jun 2019 12:24:57 UTC
End Time : 13 Sep 2019 12:24:57 UTC
Last Update: 13 Sep 2019 12:24:57 UTC
Filter: No Filter

Suspicious Full URL List @ ArcSight ESM

url	indicatorType	lastDetectTime	description	actors	reference	threatLevel	mitreAttack
http://my-work.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://spr-d.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://spread-new.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://spread.crimea.com	suspicious	8/29 7:36:34	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://sprs-files.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://sprs-updates.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://telo-spread.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://tor-file.ddns.net	suspicious	8/29 7:36:34	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://torrent-stel.space	suspicious	8/29 7:36:34	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://torrent-supd.space	suspicious	8/29 7:36:34	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://torrent-videos.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://torrent-vnc.ddns.net	suspicious	8/29 7:36:34	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://versiya-spread.myftp.org	suspicious	8/29 7:36:34	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://winrusk.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://winrotas.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://winrusk.ddns.net	suspicious	8/29 7:36:33	OSINT - SectorC08: Multi-Layered SFX in Recent Campaigns Target Ukrai...	Gamaredon Group	Network activity	High	T1106 T1053 T1064 T1060 T111...
http://bvs.a.in/publihdelliver/rmareur...	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
http://guidetti.se/wp-snapshots/tmp/...	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
http://pkusik.com/fkadmin/keditor/...	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
http://svsestheart-exhibition.com/upf...	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
http://rlny.cc/okubz	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
http://rlny.cc/oykbbz	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
https://blog.trendmicro.com/trendla...	trojan	9/6 14:32:54	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		External analysis	Low	T1100 T1110
https://dck.ru/HfBwo	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
https://dck.ru/HfCQ	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
https://dck.ru/HfCQ	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
https://cryptonation.theseccrtrack.p...	trojan	9/6 14:26:09	OSINT - Spam Campaign Abuses PHP Functions for Persistence, Uses Co...		Network activity	Low	T1100 T1110
https://134.209.103.152/update1	backdoor	9/6 13:41:09	OSINT - PowerShell based file-less malware		Network activity	Low	T1086 T1053 T1005 T1003 T106...
https://bloqs.quickheal.com/powersh...	backdoor	9/6 13:41:18	OSINT - PowerShell based file-less malware		External analysis	Low	T1086 T1053 T1005 T1003 T106...
dsmanufacture.privateidn.org	ant	7/18 12:55:30	Okrum: Ke3chang group targets diplomatic missions (OSINT)	Mirane	Network activity	Medium	T1035 T1060 T1140 T107 T1158

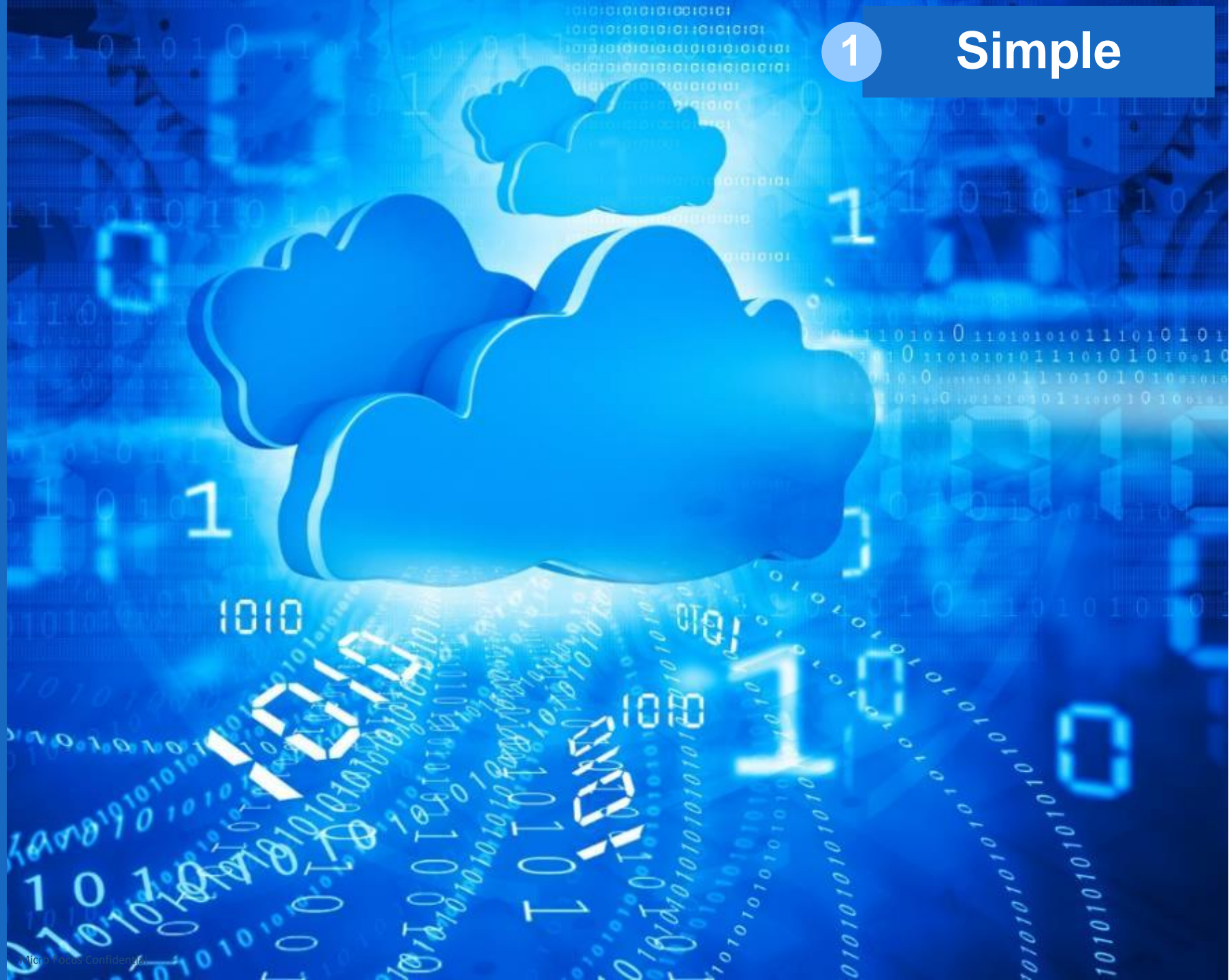
How we get there

Run In: AWS, Azure

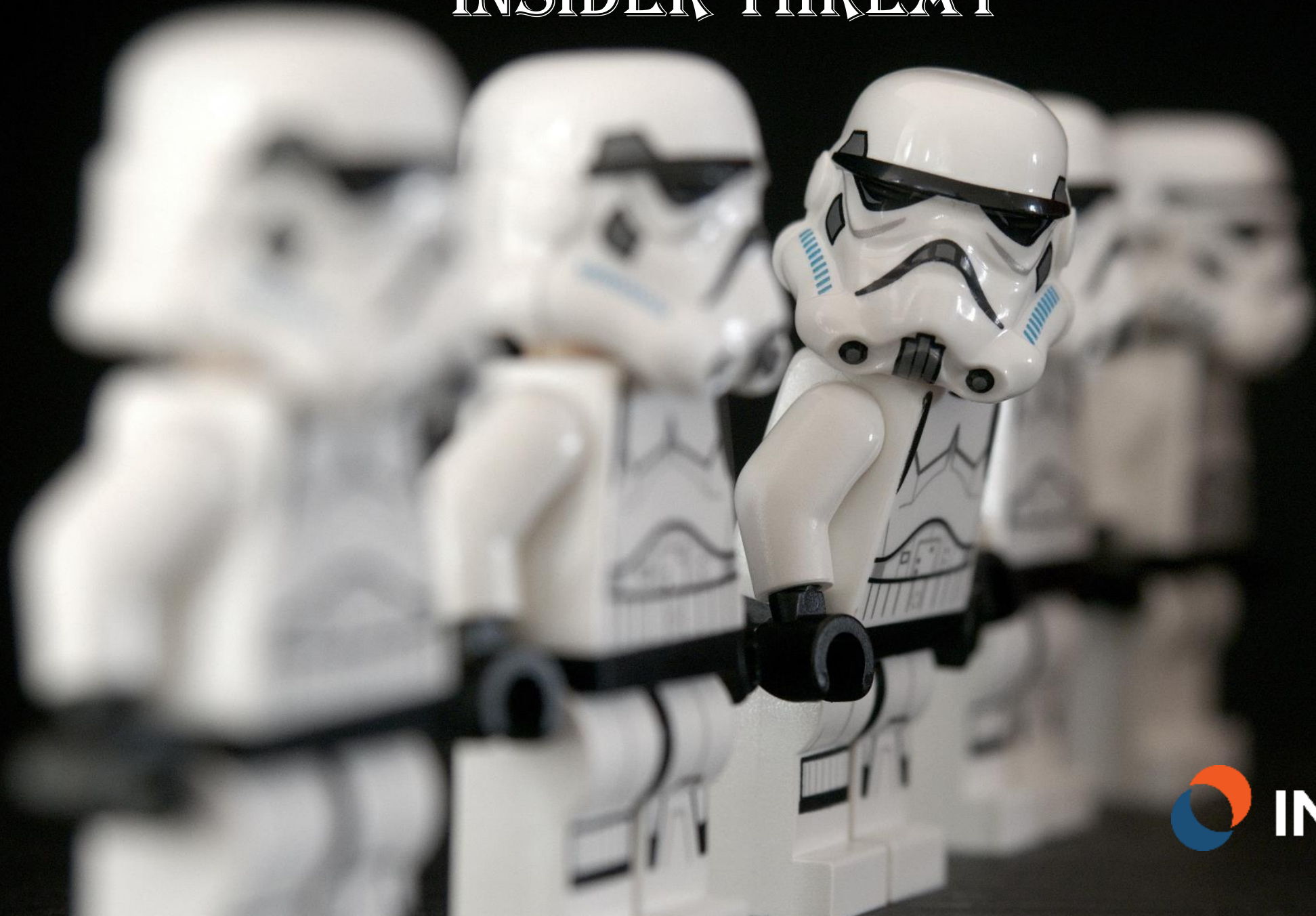
Monitor: AWS, Azure, Google, Oracle

Other key SaaS Apps: O365, G-Suite, Slack, Workday, Box

**Under Investigation
Micro Focus delivery
of ArcSight as SaaS
product in 2020**



INSIDER THREAT



About Intersect

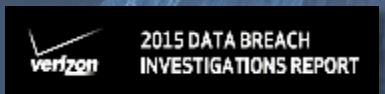
In-Q-Tel Portfolio
Company

Headquartered in
Ottawa, Canada

Data science &
analytics focused
on cybersecurity

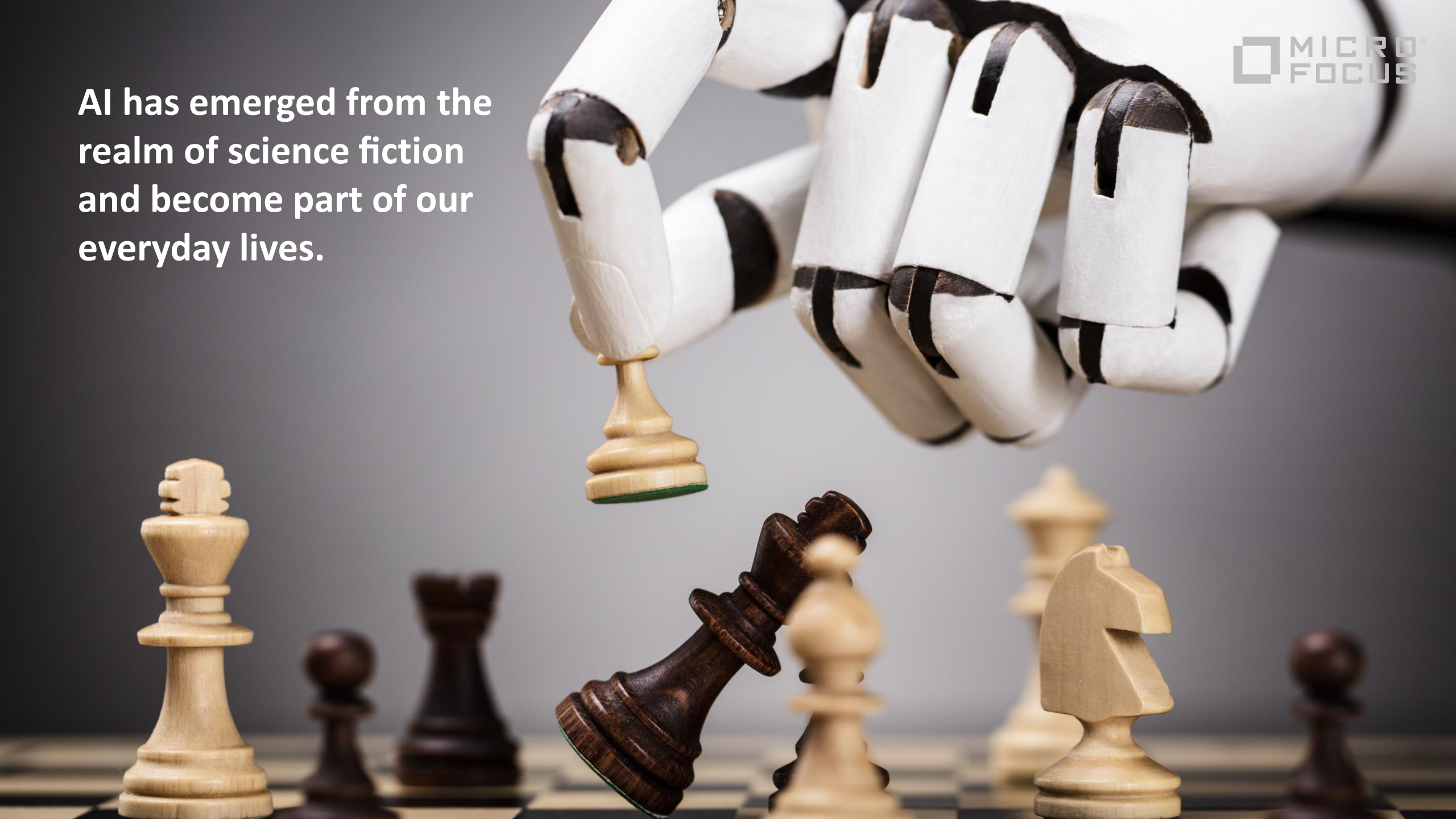
100 person-years of
security analytics
and anomaly
detection R&D

SECURITY ANALYTICS LEADER



USING DATA SCIENCE TO TRUST BUT VERIFY
Detecting misuse is also an area where the application of modern data-science practices may shine, according to Stephan Jou, CTO of Intersect. All you need is data, features, and math.

AI has emerged from the realm of science fiction and become part of our everyday lives.



Intersect for Insider Risk

We give you a short list of high-quality leads.

INTERSET

Many users...

...many servers, many websites...

Type Filter entities by name, tag, or type.

12,092 Users	12,789 Machines	25 Controllers	13,046 IP Addresses	10 Printers	632 Projects	39 Resources	104 Shares	1.37M Websites
--------------	-----------------	----------------	---------------------	-------------	--------------	--------------	------------	----------------

Top Risky Entities

22	60	173	1.41M
Extreme Risk	High Risk	Medium Risk	Low Risk

#	Current Risk	Entity	Potential Threat	Riskiest Anomaly/Violation
1	98	joshua.newman	Initial Access	JULY 15TH 2018, 3:29 AM Active 3-4 AM Jul 15, 2018 (5% anomalous)
2	98	vap3iad3.lijit.com	Exfiltration	JULY 14TH 2018, 1:00 AM Sent 767MB of data to vap3iad3.lijit.com
3	98	QA-WIN-7-CONN.local	Exfiltration	JULY 15TH 2018, 1:00 AM Sent 1.16TB of data to 204.212.170.14
4	97	shiela.mathis		
5	95	benjamin.mitchell		

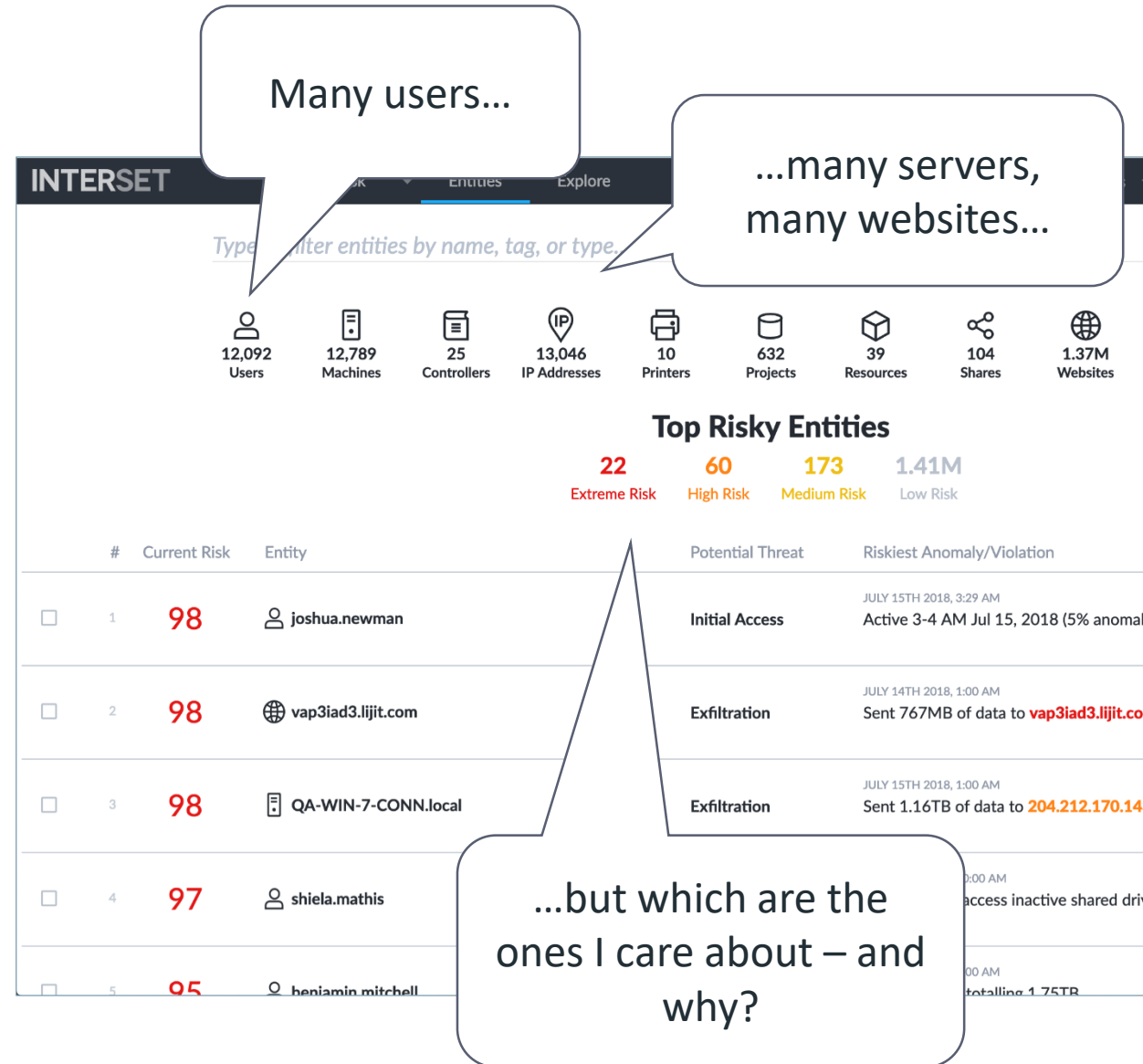
...but which are the ones I care about – and why?

Intersect for Insider Risk

Anomalous behavior for each entity is collected to build a case to describe its potential risk

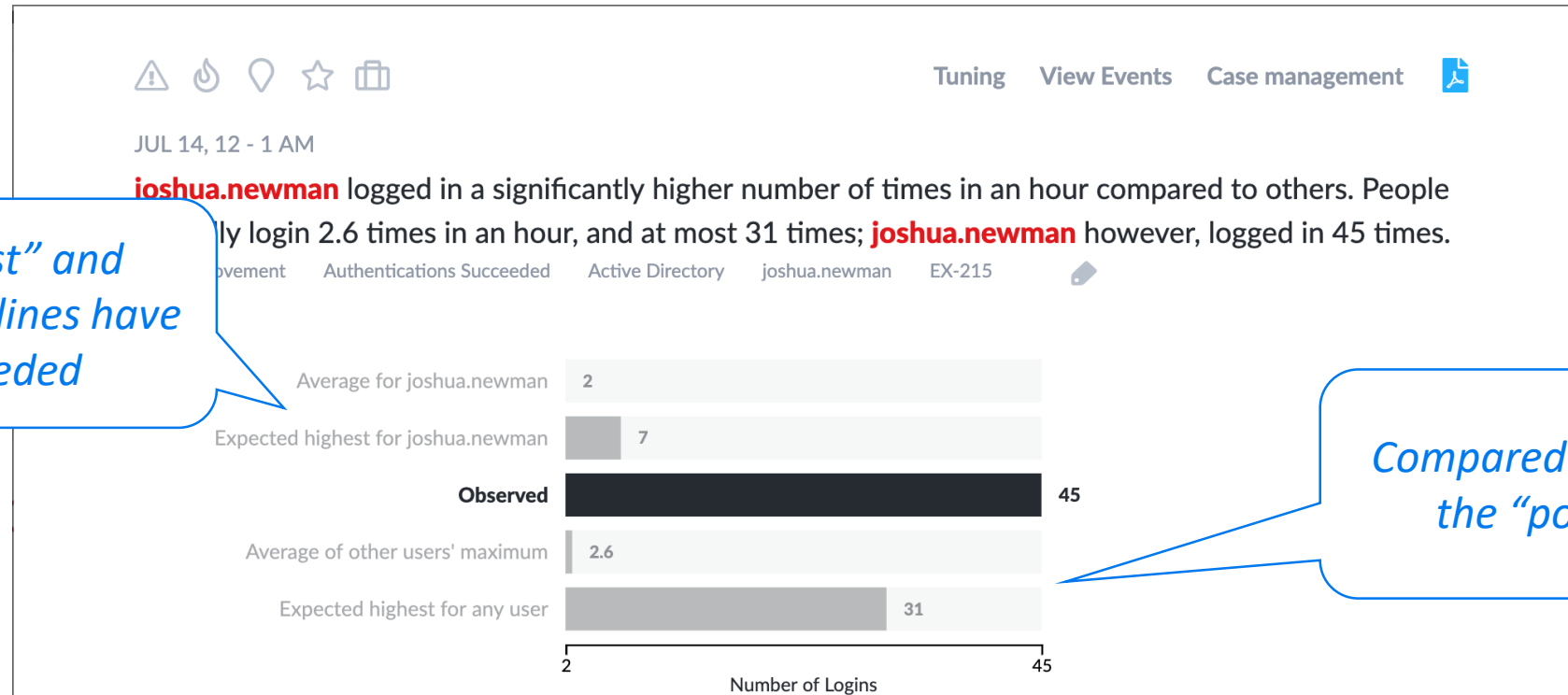
The priority of the entity in terms of potential risk is described on a scale from **0** to **100**

(from normal to **anomalous & risky**)



This Alert displays multiple Anomalies

Alerts “rollup” Anomalies so that a clear story emerges from the timeline



Both “highest” and “average” baselines have been exceeded

Compared to “self” and the “population”

When a user logs in an unusually large number of times, this may indicate that the user's account is being used for lateral movement.

“Number of Logins” is the number of times that authentication logs have recorded logins by this user's account to any domain controller destinations. The observed value reflects the number of a specific event type associated with successful logins in a timeframe for this user. The anomaly is based on the observed number of login attempts to any domain controller destination in comparison to normal behavior.

ArcSight: Enhance and combine use cases with anomaly findings

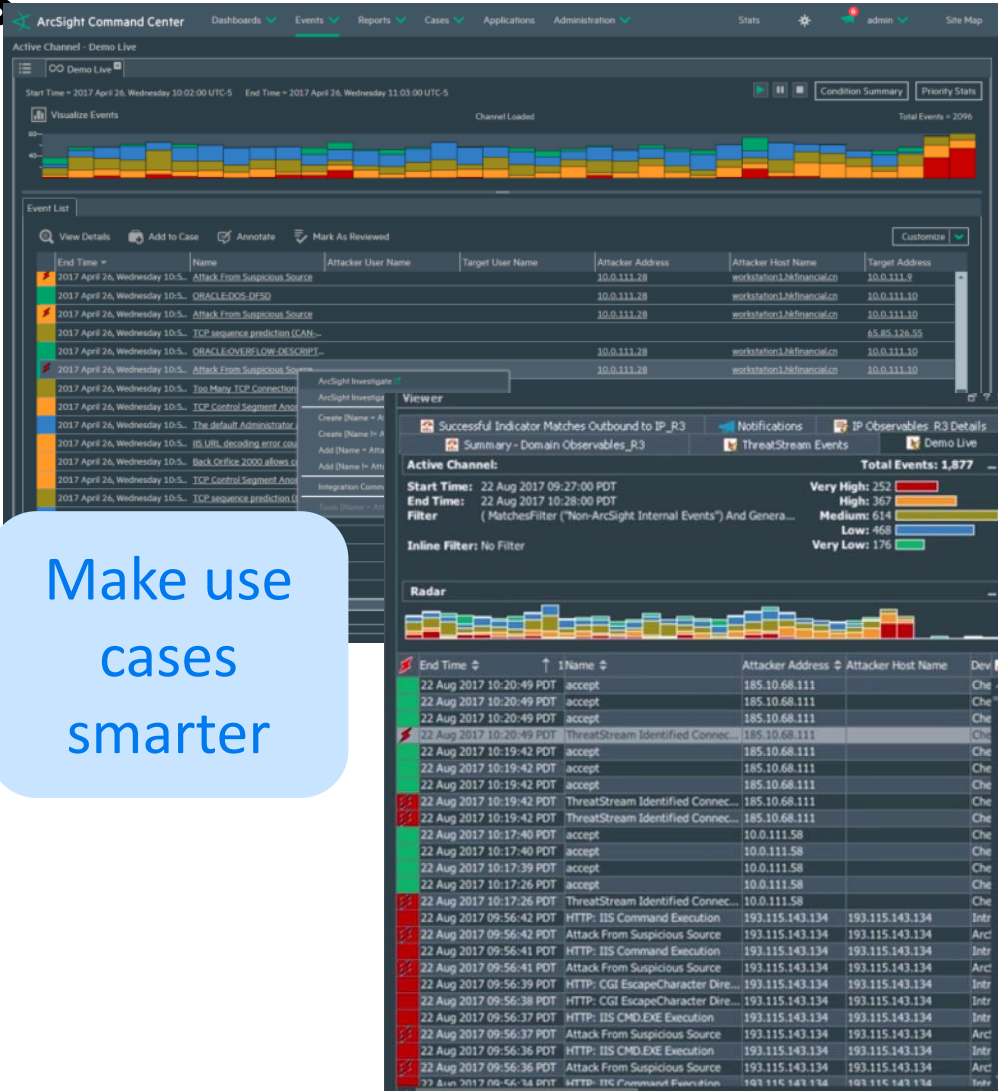


Behavioral Analytics

Dashboard & Hand-off

Make use cases smarter

Enrich event inspector details



Improved User Experience

One overarching solution dashboard

Immersive persona-driven design

Outcome centric, vs. monitoring centric

Provides proactive focus on high value work



Intersect and ArcSight in the Same Centralized SOC UI

Project name: Interfocus – Top Window

The screenshot displays the InterFocus SOC dashboard with the following components:

- Header:** InterFocus navigation bar with tabs for Interfocus, Angular, Entity List, Globe, Hello World, Matrix, and Sankey.
- Entity Count & Threat Leads:** A summary card stating "There are 22 entities with extremely high risk scores:" followed by a row of 11 entity categories with their respective counts: Users (3,138), Machines (76), Controllers (53), IP Addresses (150), Printers (10), Projects (46), Resources (21), Shares (137), Websites (75), Files (0), and Servers (0).
- Analytics Pipeline:** A flow visualization showing "Events Analyzed" (2,312,843) leading to "Anomalies & Violations Found" (793,640), which leads to "Active Risky Entities" (22). A note indicates the data was ingested between September 3 and November 2, 2016.
- Entity Risk Sparkline:** A table of risk sparklines for various entity types:

USERS	MACHINES	CONTROLLERS	IP ADDRESSES	PRINTERS	PROJEC
98 joshua.newman	99 QA-WIN-7-CONN.local	69 OTTAWADC.interset.com	79 10.10.11.13	69 dev4212bw	69 dev3,
97 shiela.mathis	92 DEV-MAC-MBP-102.local	69 MTM-WSRV01.interset-dev.qa	79 10.10.10.7	65 mkt6107color	69 dev3,
95 benjamin.mitchell	91 OTT-WIN-10-CONN.local	69 MDM-WSRV01.interset-dev.qa	69 17.249.76.18	65 eds7008	68 dev3,
95 marc.bassy	90 ARCH-WIN-10-CONN.local	66 FTXDC2.interset.com	67 204.212.170.143	65 mkt7029bw	68 dev3,
93 jude.clem	90 EDS-WIN-7-CONN.local	63 LM-WSRV02A.interset-lt.ext	67 72.1.205.200	65 acc5101color	67 dev3,
- Cyber Actor Insights:** A donut chart showing risk levels for different entity types: user (high), ip (medium), share (high), website (medium), machine (extreme), controller (high), project (high), and machine (extreme).
- Map Visualization:** A world map with red location markers and connecting lines, indicating global network connections.

- Interfocus UI**
- 1) SOC Analyst chooses the widget(s) of choice
 - 2) Drag and drop to provide the custom SOC dashboard that is both visually appealing and enabling the analysts to perform faster triage, remediation and response.
 - 3) The top 3 widgets are displaying Intersect Machine Learning results
 - 4) Bottom right widget is the ESM Front of the SOC dashboard widget.

Intersect and ArcSight in the Same Centralized SOC UI

Project name: Interfocus – Top Window

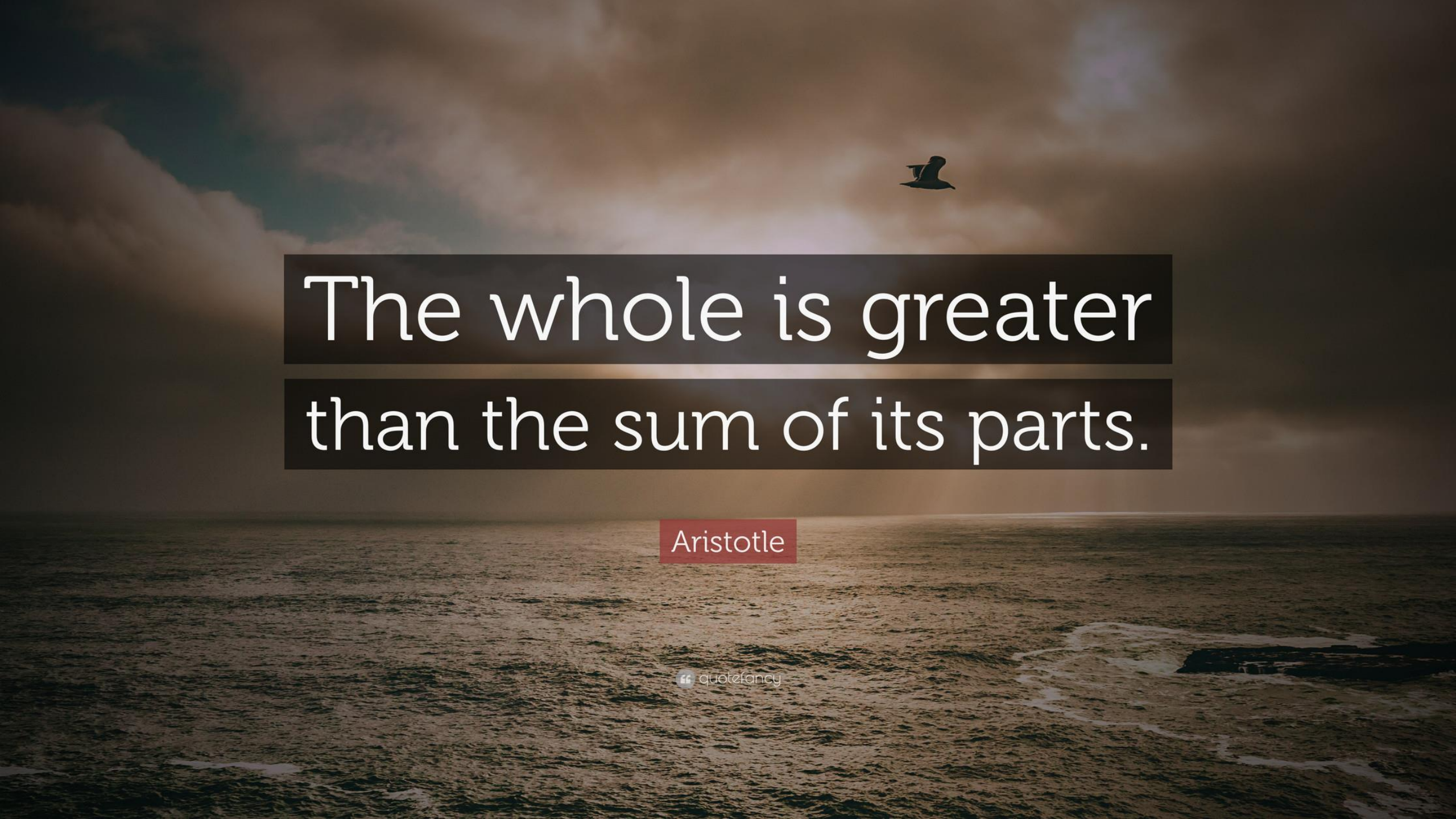
The screenshot displays the Interfocus SOC UI interface. At the top, there is a navigation bar with the 'InterFocus' logo and several menu items: Interfocus, Angular, Entity List, Globe, Hello World, Matrix, and Sankey. Below the navigation bar, the main content area is divided into three sections, each highlighted with a red border:

- Cyber Actor Insights:** A circular sunburst chart showing risk scores for various entities. The inner ring includes 'share', 'project', 'controller', and 'machine'. The outer ring includes 'user', 'website', and 'extreme'. Risk levels are indicated by colors: high (orange), medium (yellow), and extreme (red).
- Matrix Visualization:** A heatmap showing a rolling window of entity-based risk scores over time. The x-axis represents time from 09/23 to 09/29. The y-axis represents different entities. A white line graph is overlaid on the heatmap, and a callout bubble with the number '48' is visible on the right side.
- Events:** A table listing detected events with columns for Name, Active Channel, Attacker Geo Country Code, Category Custom Format Field, Category Device Group, Device Product, Device Severity, Device Vendor, File Name, Priority, Target Address, and Target.

Interfocus UI

- 1) Top left window is the Cyber Actor Insights widget.
- 2) Matrix Visualization widget provides a timeline (e.g. Last 30 days) rolling window of entity-based risk scores.
- 3) Bottom window is ESM Active Channel, providing the events of interest, as chosen from the widgets above.
- 4) All events are tagged with MITRE technique ID, name and tactic name.

NAME	ACTIVE_CHANNEL	ATTACKER_GEO_COUNTRY_CODE	CATEGORY_CUSTOM_FORMAT_FIELD	CATEGORY_DEVICE_GROUP	DEVICE_PRODUCT	DEVICE_SEVERITY	DEVICE_VENDOR	FILE_NAME	PRIORITY	TARGET_ADDRESS	TARGET
Exploit Attempt Detected b...	Mitre Attack	JP	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	Exploit Attempt Detected b...	8	1.2.230.58	T
Exploit Attempt Detected b...	Mitre Attack	JP	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	Exploit Attempt Detected b...	8	1.2.209.93	T
Exploit Attempt Detected b...	Mitre Attack	CN	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	Exploit Attempt Detected b...	8	1.4.179.6	T
Exploit Attempt Detected b...	Mitre Attack	TH	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	Exploit Attempt Detected b...	8	1.2.232.168	T
Successful Brute Force Lo...	Mitre Attack		/Attack Life Cycle/Activities:Expand Access	/Security Information Ma...	ArcSight	Warning	ArcSight	Successful Brute Force Lo...	9	10.0.111.5	
DoS Activity Detected by IDS	Mitre Attack	US	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	DoS Activity Detected by IDS	6	204.102.253.2	U
Exploit Attempt Detected b...	Mitre Attack	TH	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	Exploit Attempt Detected b...	8	1.2.52.154	C
Exploit Attempt Detected b...	Mitre Attack	TH	/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	Exploit Attempt Detected b...	8	1.2.186.223	T
DoS Activity Detected by IDS	Mitre Attack		/Attack Life Cycle:Exploit	/ADS/Network	ArcSight	Warning	ArcSight	DoS Activity Detected by IDS	6	10.0.112.119	



The whole is greater
than the sum of its parts.

Aristotle

Thank You

@ Cfir.homeri@microfocus.com

