



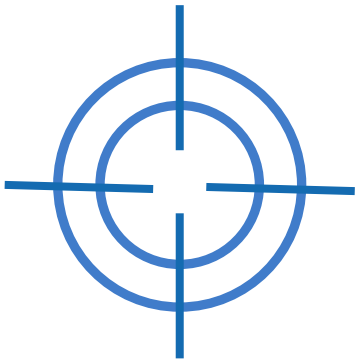
Harnessing the Power of Behavioral Analytics for Improving SOC Efficiency

Sep 4, 2019

Mel Shakir
SVP Product Development, Securonix

How to Improve SOC Efficiency?

Accurate
Threat Detection



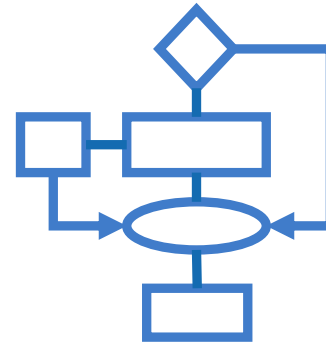
Low False Positives

Better Risk
Prioritization



Prioritizing Threats by
Impact & Stage of Attack

Rapid Incident Triage



Consistent, Automated
Workflows

Faster Hunting



Analyst Training
Derived IoC Relationships

Current State of Affairs

Delivering SOC Efficiencies with Security
Orchestration Automation and Response (SOAR)
General Dynamics Whitepaper, Jun 2018

Alert Fatigue

6 months

Average time before T1 analysts quit their jobs due to it's repetitive nature

Increased Risk Exposure

80%

Organizations receiving 500+ critical alerts investigate only 11 to 25 alerts/day

Slow Response Time

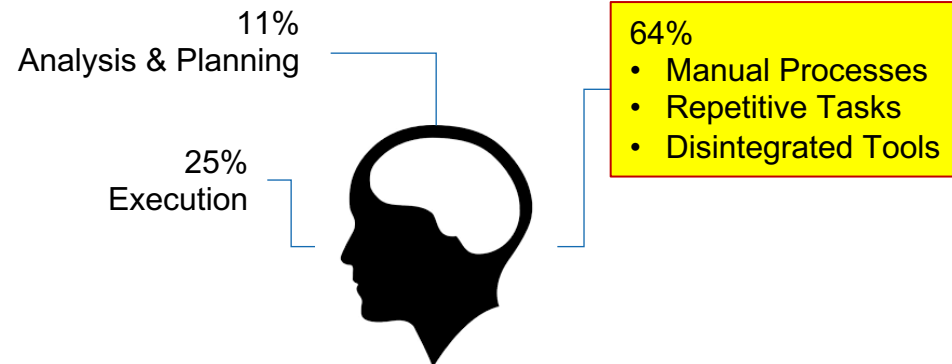
107 days

An adversary is able to survive in the enterprise due to missed alerts

Skill Shortage

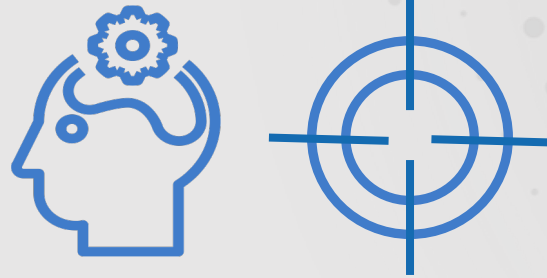
2 million

Shortage of cybersecurity professionals in 2019

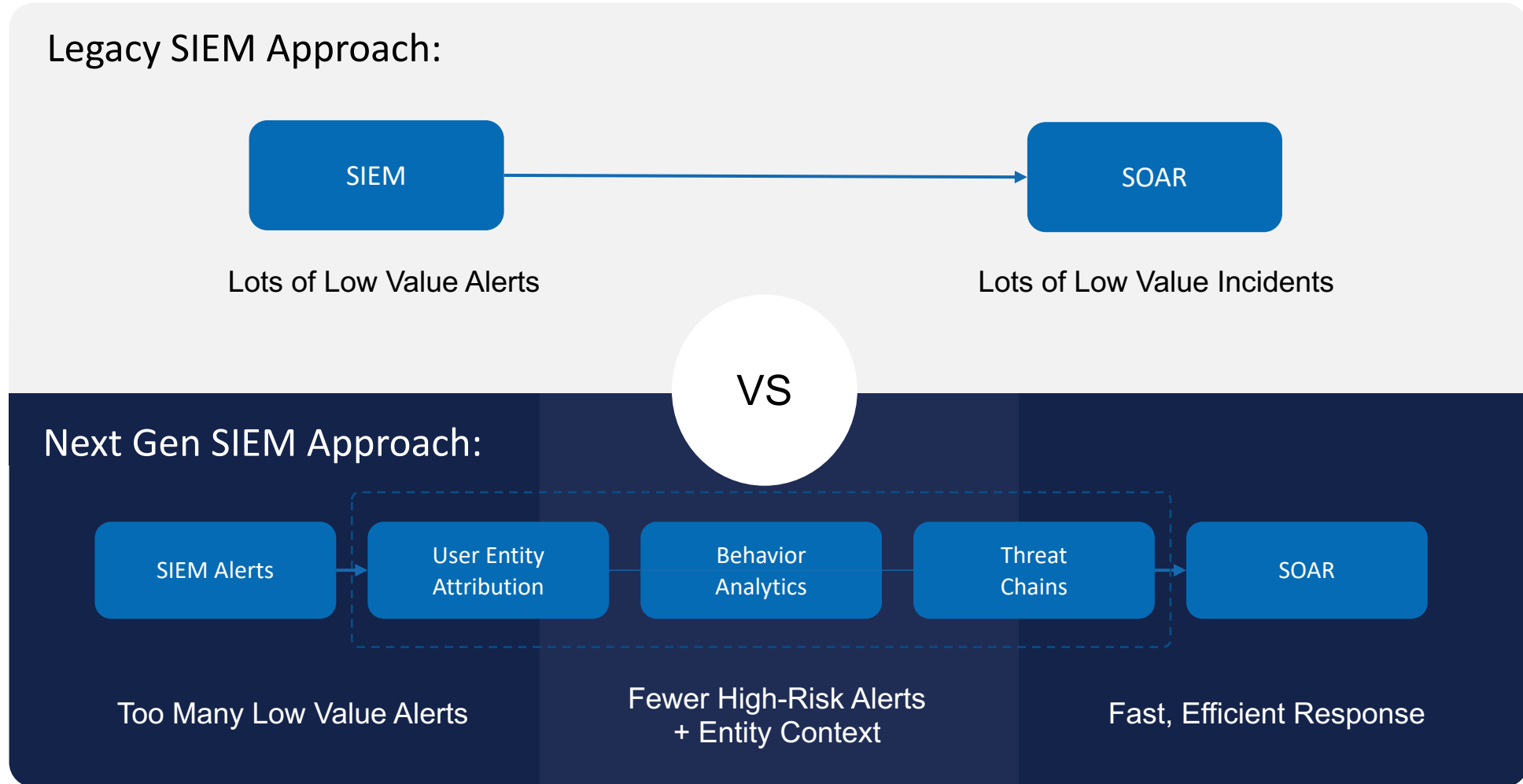




Analytics Driven Threat Detection



Fewer High-Risk Alerts + Entity Context



Sample Machine Learning Models



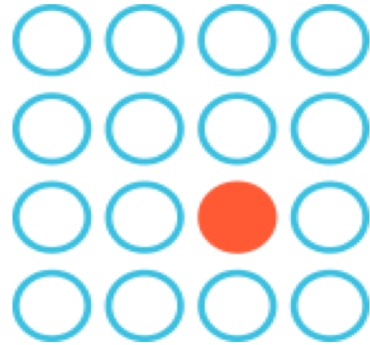
Model	Algorithm	Threats Detected
Rare behavior detection	<ul style="list-style-type: none"> MinMax clustering algorithm (Securonix Proprietary) Good-Turing Fuzzy Matching 	<ul style="list-style-type: none"> Zero day process/service execution Data exfiltration Account sharing Privilege escalation and misuse Network reconnaissance Account/Password Spraying Personal email account egress
Frequency/Amount spike detection		
Enumeration detection		
Peer outlier detection		
Land Speed Analyzer		
Traffic Analyzer	<ul style="list-style-type: none"> Random Forest Regression and Entropy estimation Online Kernel based clustering 	<ul style="list-style-type: none"> C2 Communication Domain Generation Algorithm (DGA) Lateral movement Network circumvention
Phishing Analyzer	<ul style="list-style-type: none"> Fuzzy Matching Weighted Levenshtein Distance 	<ul style="list-style-type: none"> Phishing detection Impersonation detection BEC (compromise)
Response Bot	<ul style="list-style-type: none"> Mondrian forests 	<ul style="list-style-type: none"> To learn from analyst case disposition for the application to prioritize threats for analysts going forward

Behavior Analytics Example 1



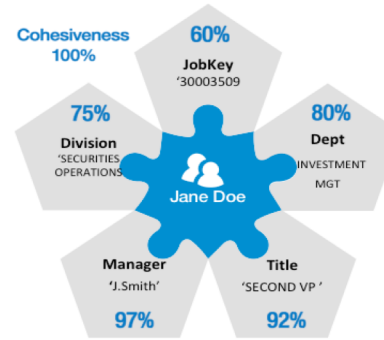
Super Enrichment

David is a contractor



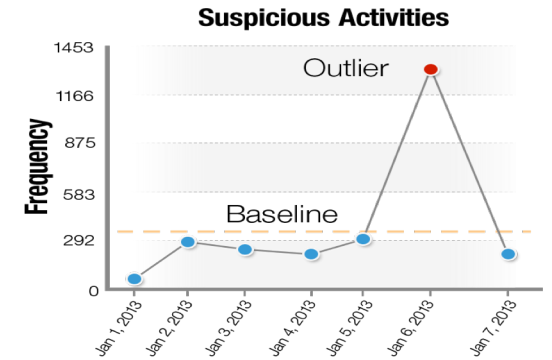
Event Rarity

User badges in at an odd time – 5 AM



Peer Analysis

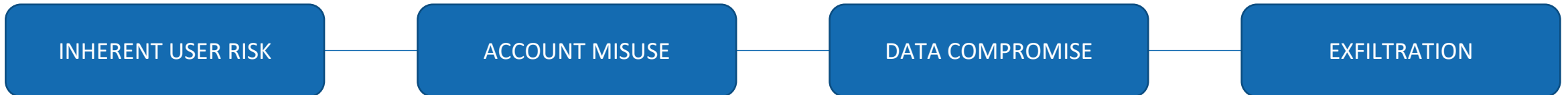
Access design files (IP) never accessed by peers



Behavior Analysis

Transfer data to USB – Spike in files copied

INSIDER THREAT MODEL (STAGES)

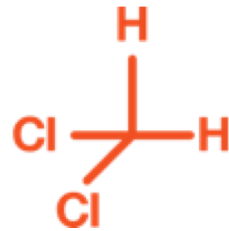


Behavior Analytics Example 2



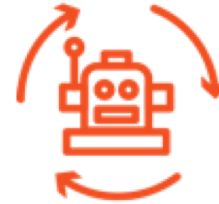
Rules Engine

John gets a phishing email



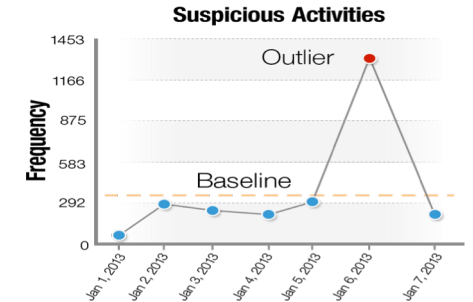
DGA + Third Party Intel

He clicks on it and is directed to a malicious site



Beaoning Pattern

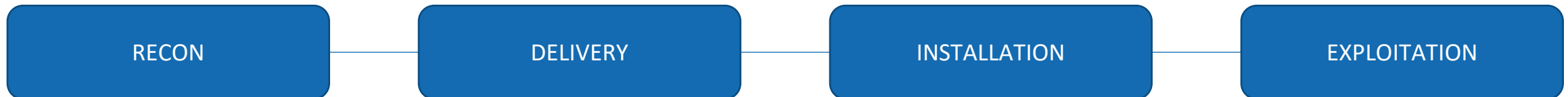
His machine is compromised and starts communicating with CNC



Spike in files accessed

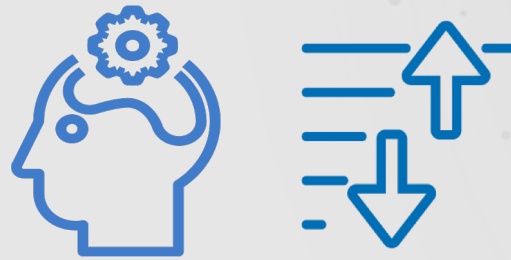
Large number of files accessed and modified (encrypted)

RANSOMEWARE THREAT MODEL (STAGES)





Analytics Assisted Risk Prioritization



Risk Prioritization by Scoring Entity Behavior



Security Center Security Command Center

LAST REFRESHED : MON, 18 FEB 2019 @ 21:27:53

34.8M TOTAL EVENTS

EVENTS TODAY @ EPS NOW

THREATS TODAY

VIOLATIONS TODAY

VIOLATORS TODAY

INCIDENTS

IN MY QUEUE 0

ASSIGNED TO GROUPS 3

TOP VIOLATORS

429 TOTAL VIOLATORS

Last year

Type text to filter..

NEW VIOLATIONS X NEW VIOLATIONS X IN PROGRESS X

	Patricia Macdonald Department: Credit Product Marketing and Sales	119.8 RISK SCORE
	Miranda Peck Department: Media Relations	112.1 RISK SCORE
	Walter Molony Department: Compensation and Bonuses	110 RISK SCORE
	Thane Pratt Department: Credit Product Marketing and Sales	104.4 RISK SCORE
	James Miller	103.9

SHOWING 10 OF 429 RECORDS

TOP THREATS

17 THREATS

Last year

Type text to filter..

89 Days Ago Wed, 21 Nov 2018 @ 22:19:29	Possible Cryptojacking Observed AWS This threat model aims to identify possible unauthorized use of assets to mine cryptocurrencies.	1 VIOLATORS
210 Days Ago Mon, 23 Jul 2018 @ 23:26:50	Patient Data Compromise This threat model aims to detect unauthorized activities associated with patient data which could be an indication of data exfiltration	1 VIOLATORS
211 Days Ago Mon, 23 Jul 2018 @ 19:03:49	Privileged IT User-Sabotage This threat model aims to identify users who misuse their privileges to create short lived or backdoor accounts to perform malicious activity	1 VIOLATORS
214 Days Ago	Advanced Cyber Threat	

SHOWING 17 OF 17 RECORDS

TOP VIOLATIONS

85 POLICIES

Last year

Type text to filter..

89 Days Ago Wed, 21 Nov 2018 @ 23:20:35	Communication from TOR Exit Nodes to AWS Suspicious network traffic	377 VIOLATORS
89 Days Ago Wed, 21 Nov 2018 @ 22:18:46	Log Tampering AWS Audit Log Tampering	1 VIOLATORS
89 Days Ago Wed, 21 Nov 2018 @ 21:53:01	High number of EC2 instances spawned in a short time AWS Authentication From Rare Geolocation	1 VIOLATORS
90 Days Ago Wed, 21 Nov 2018 @ 19:56:55	Self Privilege Escalation AWS Self privilege escalation	1 VIOLATORS
90 Days Ago	Rare Geolocation Login AWS	1

SHOWING 85 OF 85 RECORDS

Privileged Accounts

1 TOTAL VIOLATORS

Last year

Type text to filter..

	Thane Pratt Department: Credit Product Marketing and Sales	104.4 RISK SCORE
--	--	----------------------------

Service Accounts

1 TOTAL VIOLATORS

Last year

Type text to filter..

	SVC_SNYPR10 Datasource Name: Windows Data	101.4 RISK SCORE
--	---	----------------------------

Departing Employees

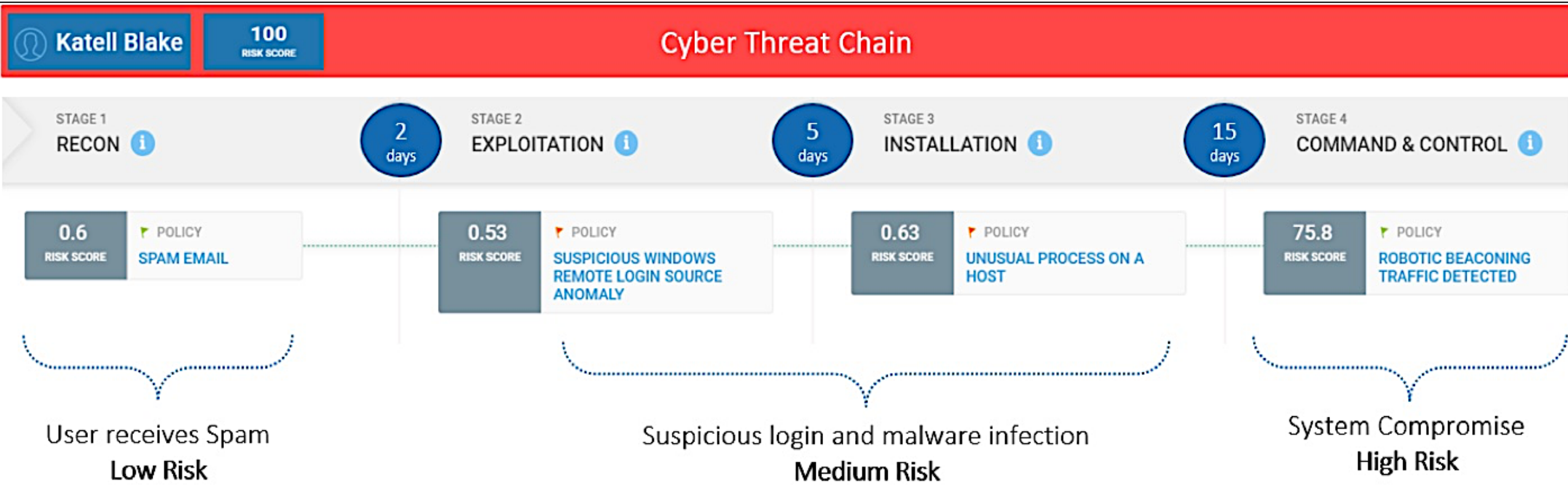
1 TOTAL VIOLATORS

Last year

Type text to filter..

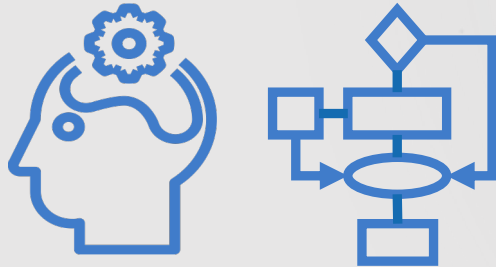
	HARRY OGWA Department: Mainframe and Midrange Administration	128.3 RISK SCORE
--	--	----------------------------

Risk Prioritization using Threat Chains

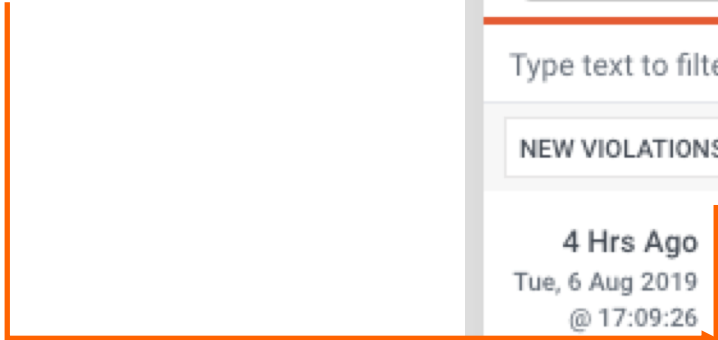




Analytics Driven Triage



- Securonix SIEM threats are mapped to SOAR playbooks



TOP THREATS

Last 90 days ▾

6 THREATS

Type text to filter..

NEW VIOLATIONS ✕ IN PROGRESS ✕

4 Hrs Ago Tue, 6 Aug 2019 @ 17:09:26	⚡ Traffic to Randomly generated domains-11 Traffic to randomly generated domains	H	1 VIOLATORS
6 Hrs Ago Tue, 6 Aug 2019 @ 15:03:04	⚡ Phishing Threat Model This threat model is for detecting email phishing attempts	M	1 VIOLATORS
6 Hrs Ago Tue, 6 Aug 2019 @ 14:55:41	⚡ Flight Risk User Exfiltrating Data This threat model		1 VIOLATORS

SHOWING 6 OF 6 RECORDS

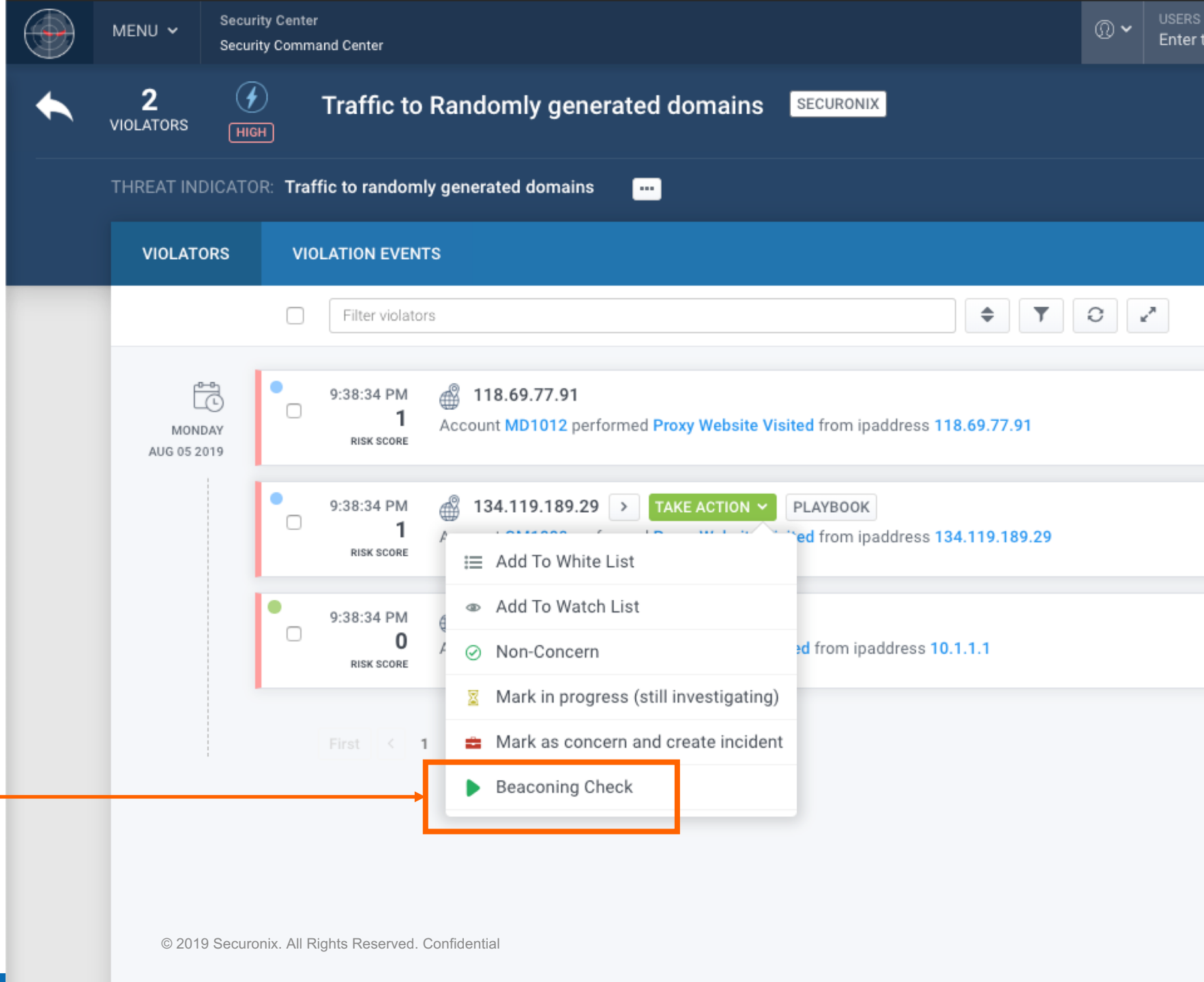
TOP VIOLATIONS

Last 90 days ▾

Type text to filter..

6 Hrs Ago Tue, 6 Aug 2019 @ 15:02:57	Traffic to Rare Domain Possible C2 Communication
6 Hrs Ago Tue, 6 Aug 2019 @ 15:01:47	Email from rare domains Possible phishing attempt
6 Hrs Ago Tue, 6 Aug 2019 @ 14:55:02	High number of email forwards DATA EGRESS VIA EMAIL
6 Hrs Ago Tue, 6 Aug 2019 @ 14:55:02	Email sent to self DATA EGRESS VIA EMAIL

SHOWING 4 OF 4 RECORDS









- Playbooks can be launched automatically or manually
- Securonix SIEM recommends playbooks to execute

Recommended Triage Actions



Replicating Analyst actions enables SOC to respond faster and consistently to threats while reducing the overhead on Analysts

- Learn Tier 3 Analyst actions
- Recommend actions to Tier 1 Analyst or take automated action
- Result → Consistent triage; Reduce number of escalations to Tier 2/3 Analyst

11:06:14 PM 0.2 RISK SCORE	 Bethany Codd Account BETHANY.CODD@SCNX.COM performed SharePoint-Events for filetypeConfidential	 Mark as concern and create incident  OR TAKE OTHER ACTIONS ▾
11:06:14 PM 0.2 RISK SCORE	 Carly Wells Account CARLY.WELLS@SCNX.COM performed SharePoint-Events for filetypeNonConfidential	 Non-Concern  OR TAKE OTHER ACTIONS ▾



Recommended Triage Actions

The screenshot displays the Security Center interface. On the left, a 'VIOLATORS' panel shows a list of events with timestamps and risk scores. An orange arrow points from this panel to the main 'PLAYBOOKS' view. The 'PLAYBOOKS' view shows a list of executed playbooks, with one entry highlighted in an orange box. This entry is 'Investigate Brute Force Attempt', which is 'FINISHED'. Below it, a detailed 'PLAYBOOK log for Beaconing - Child' is shown, listing the steps of the playbook execution, all of which are marked as successful with green checkmarks.

VIOLATORS

Time	Risk Score
10:10:01 AM	2
10:09:04 AM	1
10:09:04 AM	1

PLAYBOOKS

CyberSponse - Get Playbooks

Tue, 27 Aug 2019 @ 05:12:54

Type text to filter playbooks...

- Investigate Brute Force Attempt **FINISHED**
Fri, 26 Jul 2019 @ 10:45:26 | 2 Child Playbook
- Scan Nessus and Qualys **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44
- Observable (Type All) > Get La... **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44
- Generate Node Graphs #Alerts #Inci... **FAILED**
Thu, 25 Jul 2019 @ 17:05:46 | 2 Child Playbook
- Scan Nessus and Qualys **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44
- Observable (Type All) > Get La... **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44
- Generate Node Graphs #Alerts #Inci... **FAILED**
Thu, 25 Jul 2019 @ 17:05:18 | 2 Child Playbook
- Scan Nessus and Qualys **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44
- Observable (Type All) > Get La... **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44
- Investigate Brute Force Attempt **FINISHED**
Thu, 25 Jul 2019 @ 13:57:16 | 2 Child Playbook
- Scan Nessus and Qualys **FINISHED**
Thu, 29 Aug 2019 @ 11:26:44

PLAYBOOK log for Beaconing - Child

STEPS

- START **✓** Show output
- GET VIOLATION OBJECT **✓** Show output
- CONFIGURE **✓** Show output
- CHECK REPUTATION **✓** Show output
- SET POLICY LISTS **✓** Show output
- POLICY VIOLATION **✓** Show output
- IF REPUTATION GOOD OR BAD **✓** Show output
- CHECK MALICIOUS LIST POLICY VIOLATION **✓** Show output
- SCAN FOR VULNERABILITIES **✓** Show output
- CHECK FOR KNOWN VULNERABILITIES **✓** Show output
- CREATE INCIDENT **✓** Show output

- Multiple Playbooks can be launched simultaneously
- Status of Playbook(s) is seen from the SIEM UI



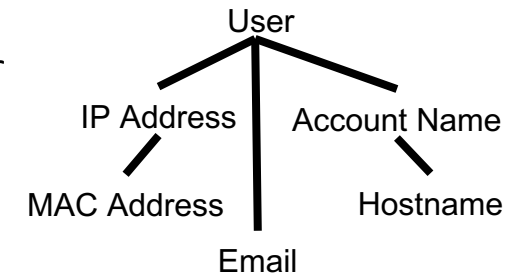
Analytics Assisted Hunting



Actionable Context: Derived IoC Relationships



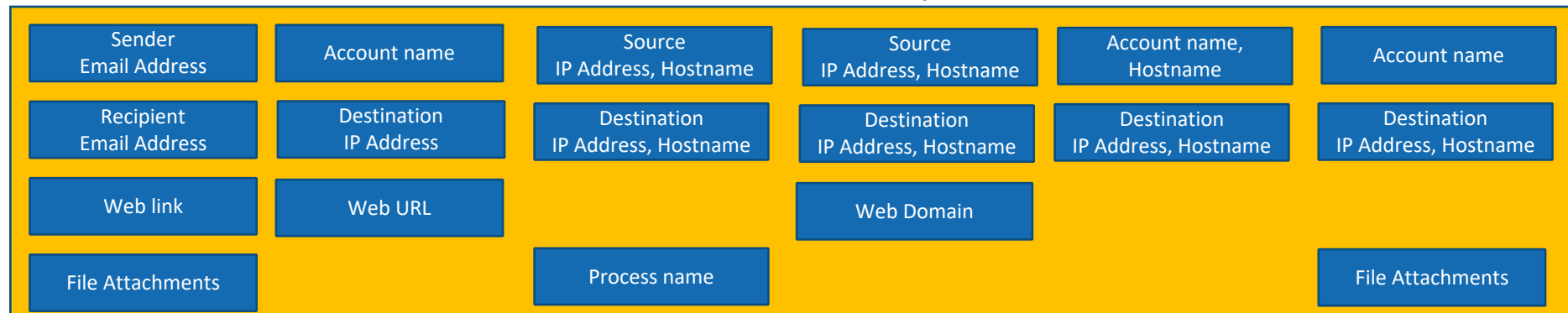
Improved tracking of relationship of IoC's linked to the same violator



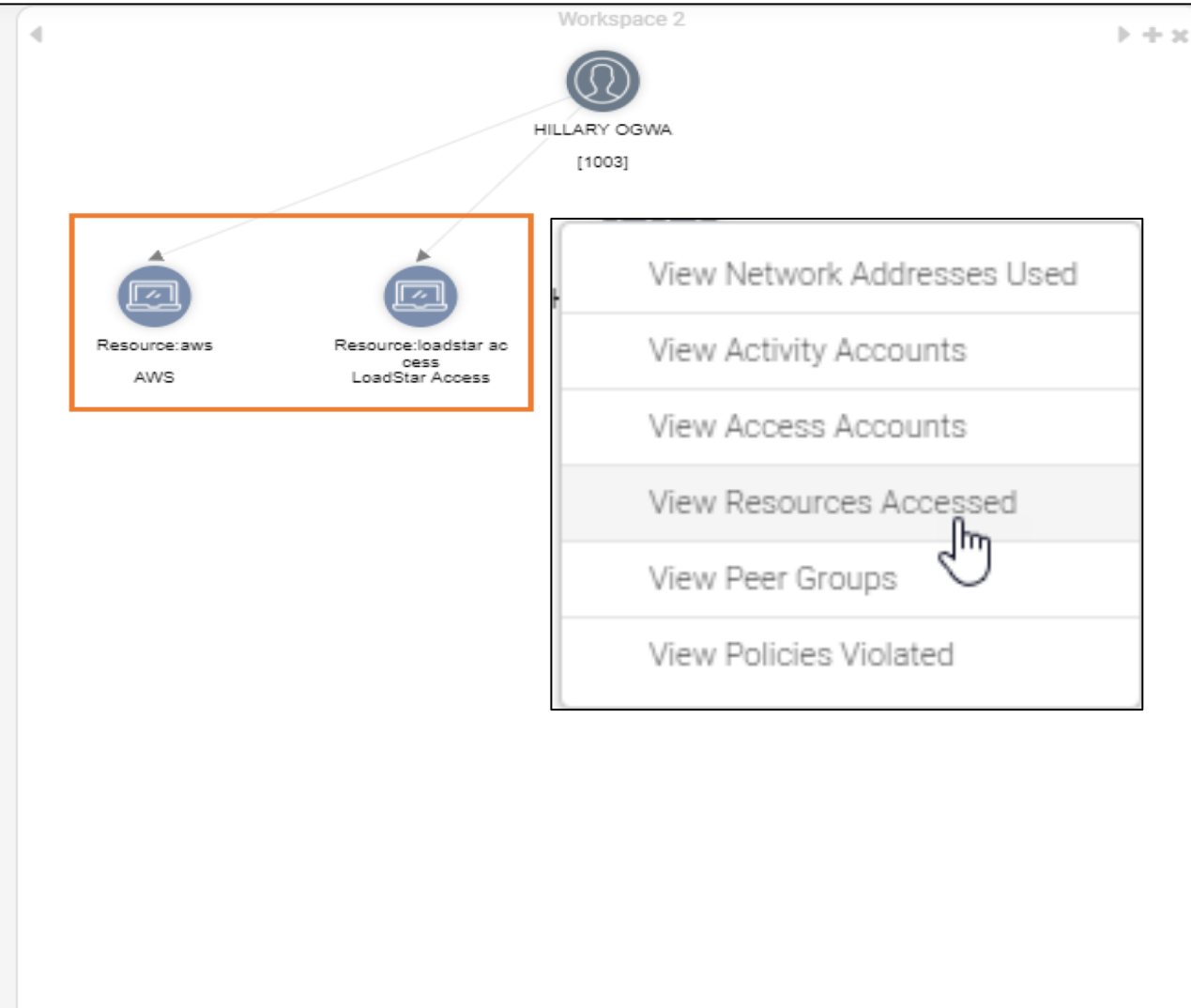
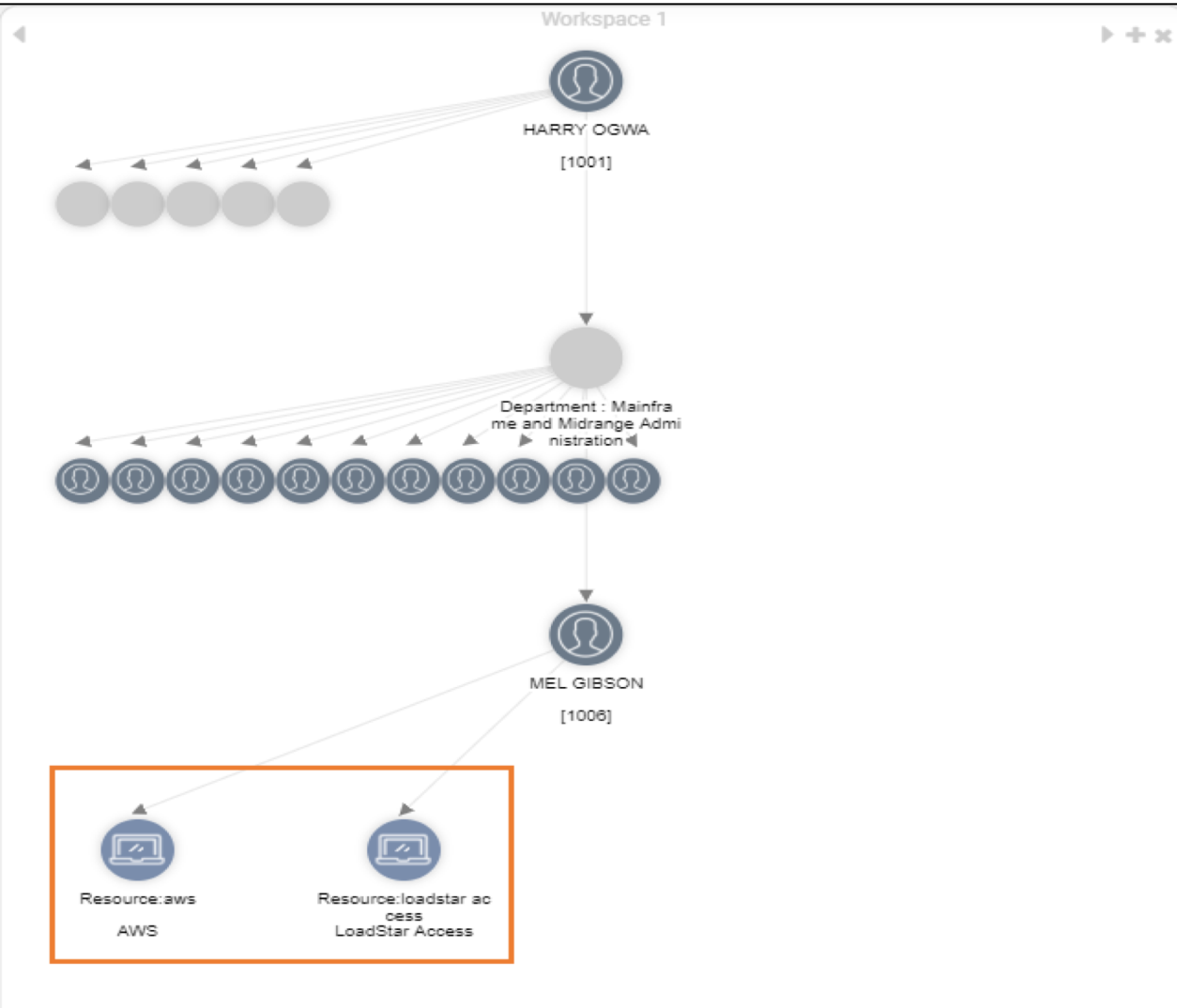
ATT&CK™ Technique



Observed Indicators of Compromise

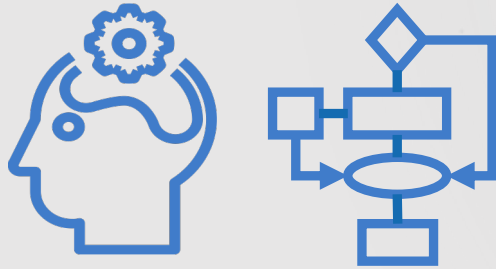


Link & Graph Analysis





Securonix Solution Overview



Securonix Solution

Features best MTTR from detection to remediation

- Single Integrated Solution → Securonix Next Generation SIEM with UEBA, and SOAR add-on



Rapid, Playbook-Driven Investigations w/ Adaptive Learning



Advanced Threat Detection



User Entity Attribution
Context for faster investigations



Machine Learning
High-fidelity alerts reduce false positives

Prioritized Threats



Threats Chains
Prioritize threats using MITRE kill-chain



Response Bot
Learns L3 analyst actions eliminating L1 guesswork

Faster Hunting



Rapid Searching
Of evidence with integrated SDL platform



Link Analysis
Connects IoC's for visual investigations

Rapid Incident Triage



Automated Playbooks
Mapped to Securonix threats for fast, consistent threat triage



275+ Connectors
And 3000+ actions provides more automation and rapid TTV

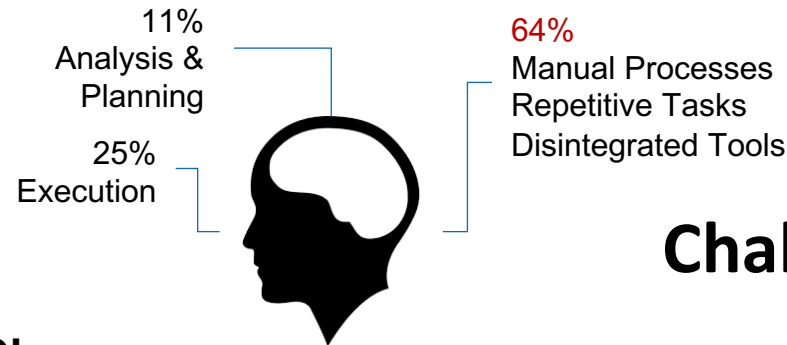
Multi-tenant support for On-premise and Securonix Cloud
Privacy Features for GDPR compliant SOC workflows

Securonix Solution Benefits

Maximizes cost savings through integration, automation and higher efficiency

Solution Benefits

- ✓ **Faster Investigations / Measurable ROI**
 - SIEM with UEBA and SOAR automation results in less operational overhead in training and enablement
 - Measure and boost SOC efficiency with SLA tracking
- ✓ **Prioritized Threats / Improved Efficiency**
 - High fidelity alerts allow a SOC to scale with fewer analysts
- ✓ **Rapid Time to Value (TTV)**
 - Large number of OOTB connectors and integrations allows new use cases to be rapidly implemented



Challenges Addressed

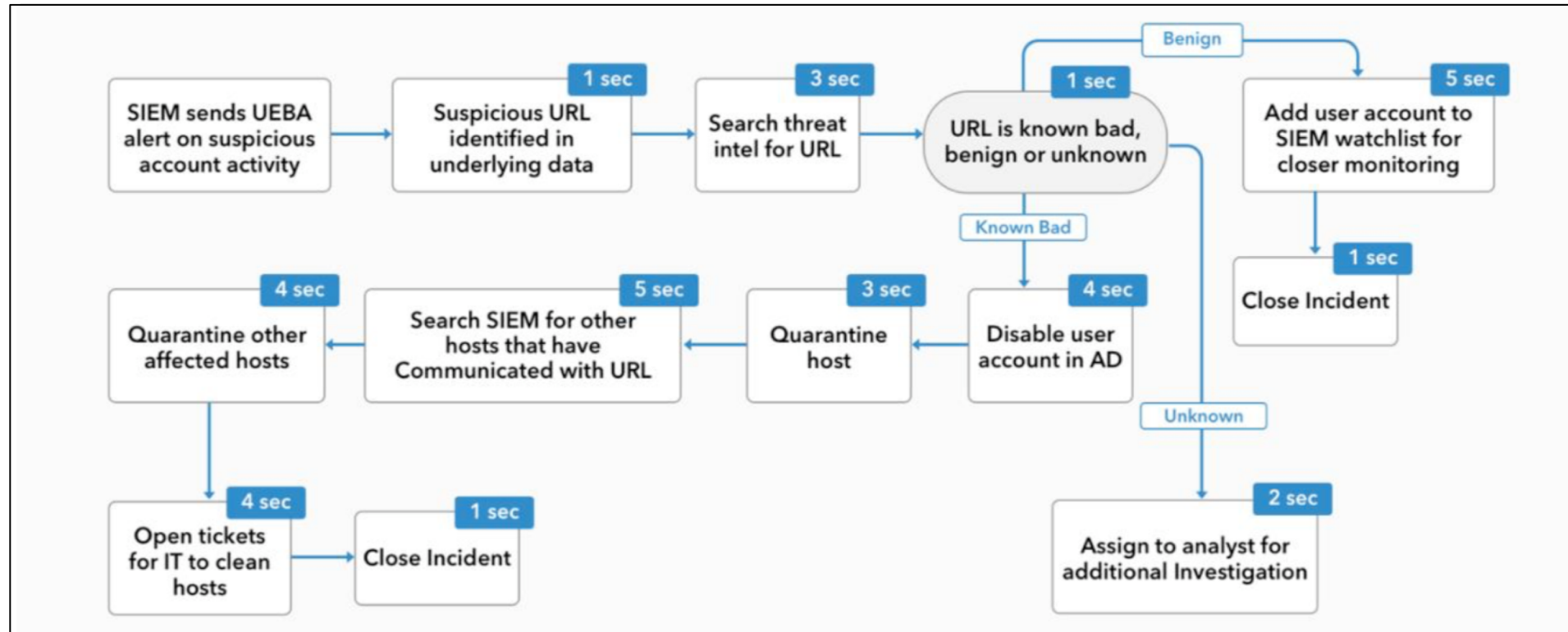
- Alert Fatigue**
Average time before T1 analysts quit their jobs due to it's repetitive nature
6 months
- Slow Response Time**
Organizations receiving 500+ critical alerts investigate only 11 to 25 alerts/day
80%
- Increased Risk / Exposure**
An adversary is able to survive in the enterprise due to missed alerts
107 days
- Lack of skilled professionals**
Predicted shortage of cybersecurity professionals by 2019
2 million

Delivering SOC Efficiencies with Security Orchestration Automation and Response (SOAR)
General Dynamics Whitepaper, Jun 2018

Faster Investigations



- Automated playbook reduces “Suspicious activity” triage time from **19-37** min to **11-26** seconds



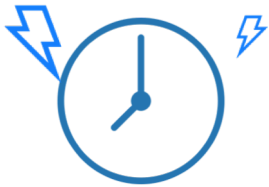
Delivering SOC Efficiencies with Security Orchestration Automation and Response (SOAR)
General Dynamics Whitepaper, Jun 2018



Measurable ROI

- Solution Metrics Include:** Resolved incidents, Mean dwell time (MDT), Mean time to resolve (MTTR), Full time employee (FTE) Gained, Playbooks & Actions Run, Time saved, Dollars saved (\$)

FASTER RESPONSE



INCREASE MORALE



MANAGE ALERTS



	Time Per to Complete	Weekly Incidents	Time Spent	Time	Time	Cost Savings
			Annually	Savings (Hours)	Savings (%)	(\$150/h)
	45	50	390	0	0%	\$0.00
Manual	minutes	Incidents	hours	hours		
	22	75	190	200	75%	\$180,000
Semi-Automated	minutes	Incidents	hours	hours		
	1.4	100	12	378	98%	\$472,800
Automated	Minutes	Incidents	hours	hours		

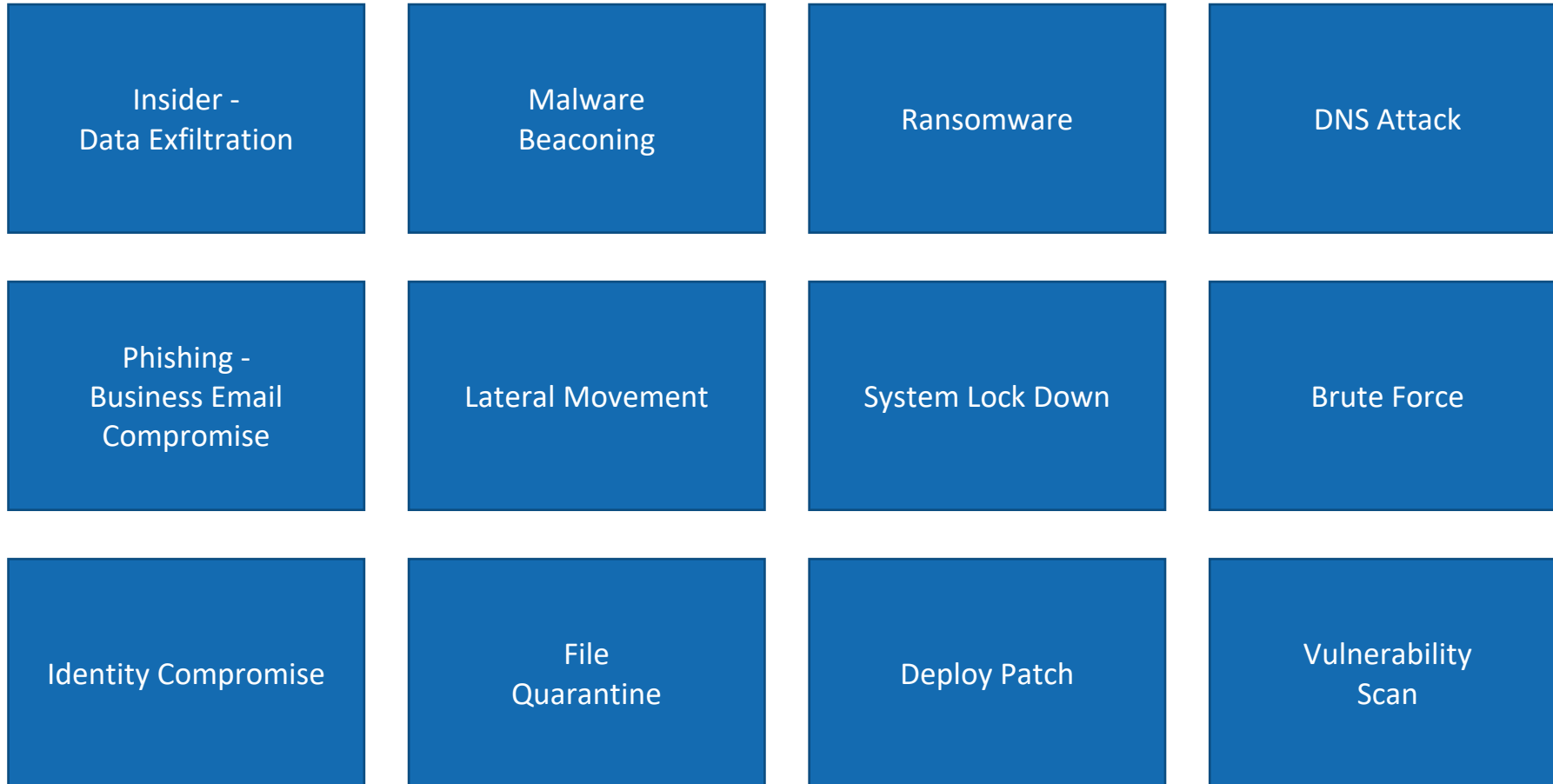
Cost Savings

Threat Window

Rapid TTV with OOTB Threats & Playbooks



- **Securonix Insider and Cyber threats / use cases mapped to Securonix SOAR Playbooks**

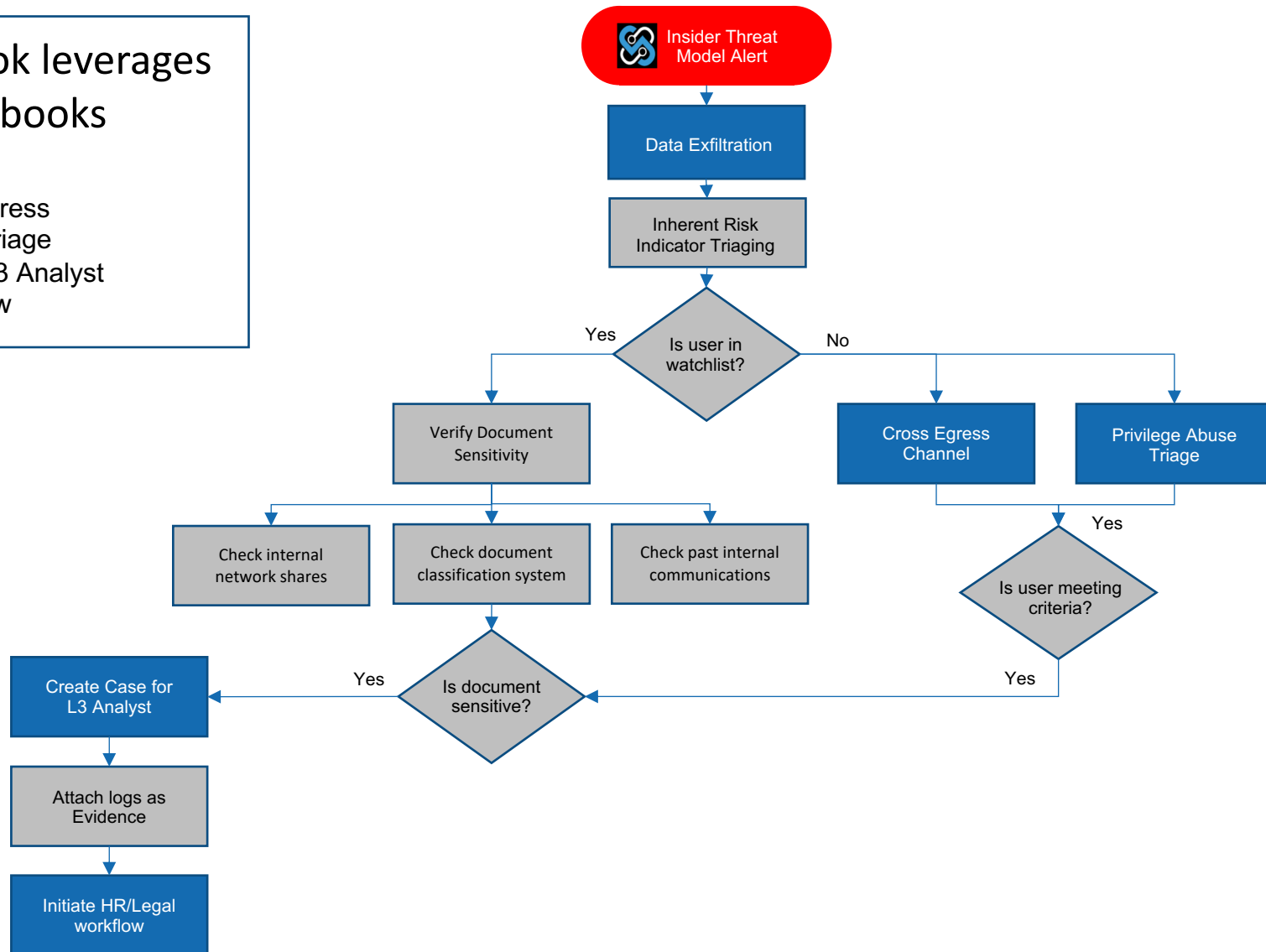
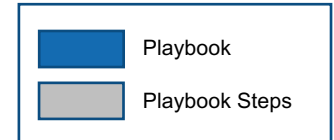


Sample Playbooks

Insider – Data Exfiltration Playbook

Insider Playbook leverages additional playbooks

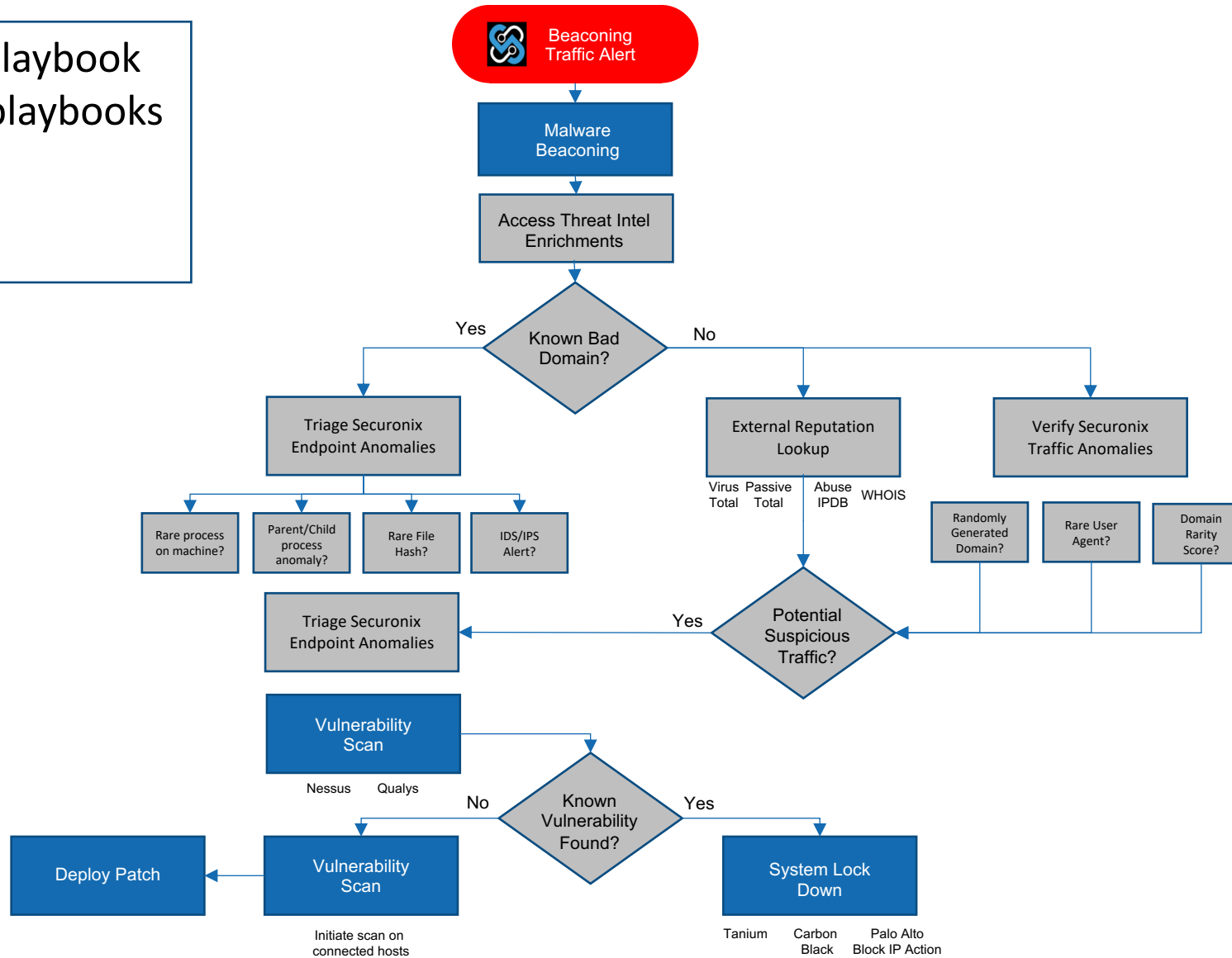
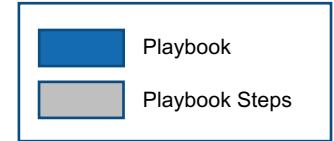
- Data Exfiltration
- Cross Channel Egress
- Privilege Abuse Triage
- Create Case for L3 Analyst
- HR/Legal Workflow



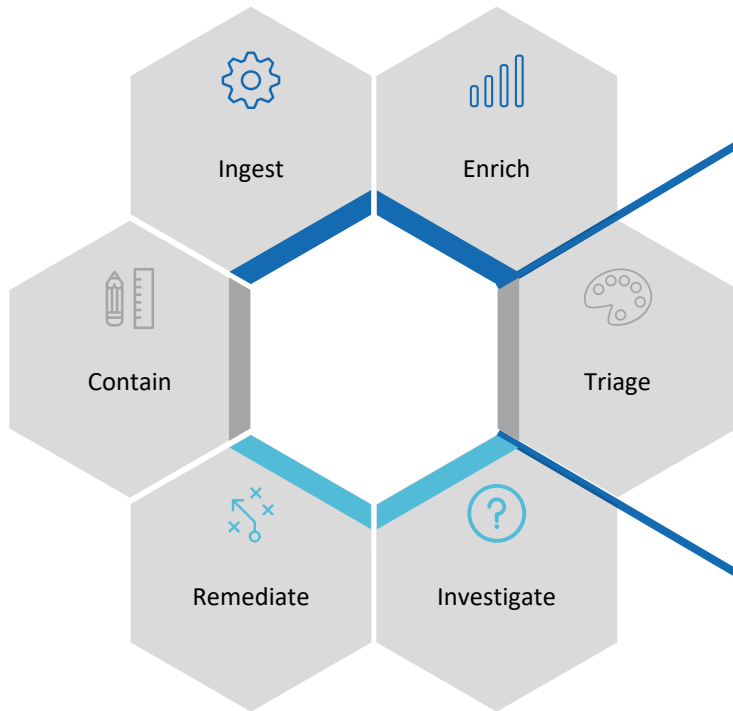
Cyber - Malware Beaconsing Playbook

Malware Beaconsing Playbook leverages additional playbooks

- Vulnerability Scan
- System Lock Down
- Deploy Patch



Rapid TTV with Wide-Ranging Integrations

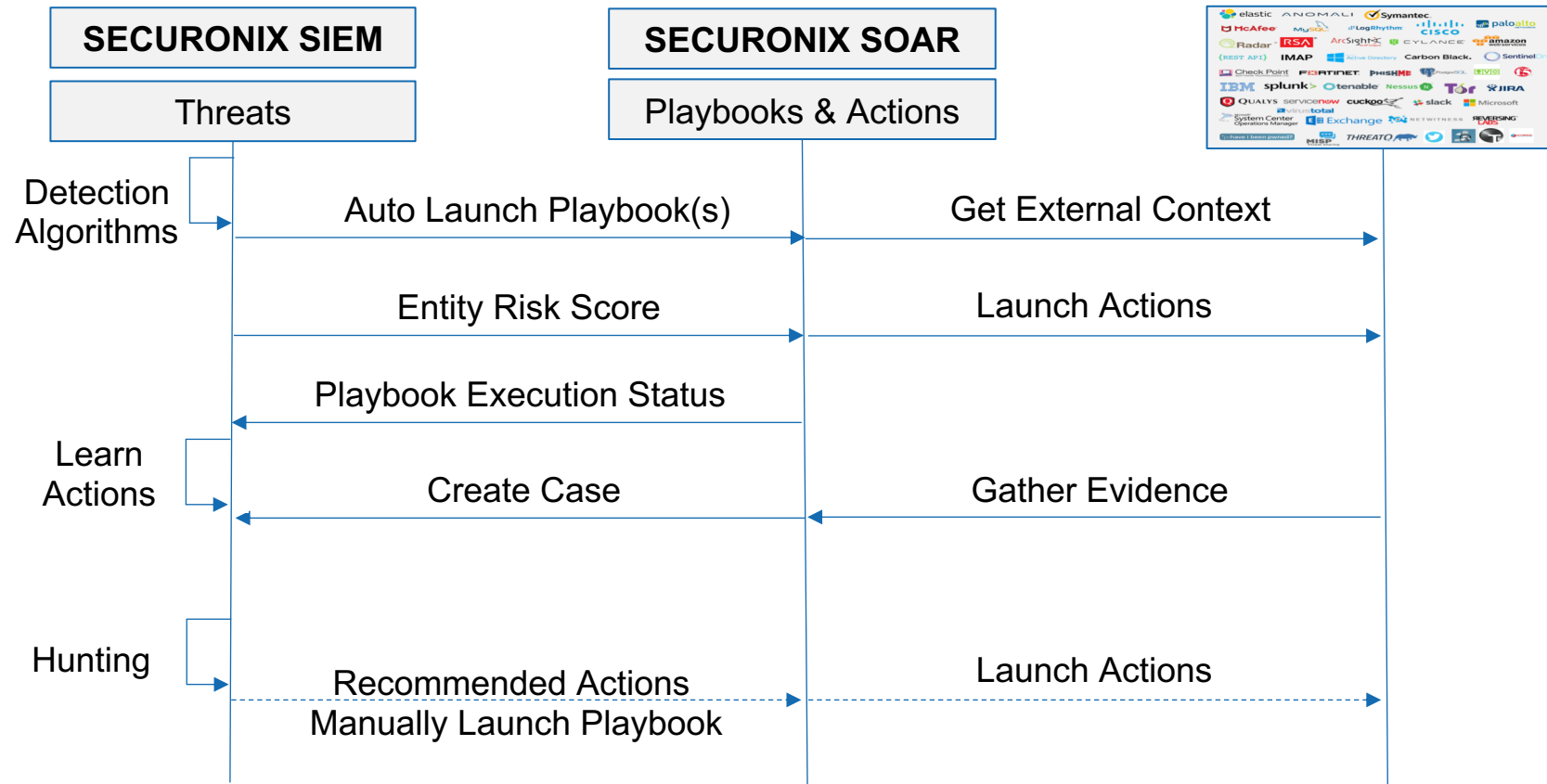


- 275+ Connectors and 3000+ actions
- List grows every 3 weeks
- Latest List at <https://documentation.securonix.com/connectors/>

Securonix Solution Flows

Multifaceted bi-directional integration improves analyst experience

- Securonix SIEM launches Securonix SOAR playbooks - automated or manually
- Securonix SOAR attaches context, launches actions, attaches evidence in SIEM UI
- Securonix utilizes advanced machine learning to learn actions and make recommendations





Demo Video (2 min)



Questions?

Thank You!