# $\mathbf{CIO100}$ Symposium & Awards



## Integrated AI Approach to Better Security Operations with Secureworks<sup>®</sup> Taegis<sup>TM</sup>

Nash Borges, PhD VP Software Engineering



Produced by CIO = DC



CIO100 | Secureworks

Produced by  $CIO \models DC$ 

AI Vision: AI Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

**Detect** malicious activity in events (e.g., processes, netflow, DNS, file modifications) and create alerts. Al used to **find** patterns of malicious activity.

**Triage** alerts using AI to **predict** which are most likely to require more in-depth investigation.

**Investigate** aspects of those high priority alerts automatically with AI-generated summarizations of detection/telemetry/alerts and **draft** key findings.

**Respond**: Automatically **resolve** the problem when customers have opted-in to "Proactive Response"



CIO100 | Secureworks

Produced by CIO | EIDC

Our Hands on Keyboard Detector was trained on 2+ years of historical data to find a variety of advanced threat actors at incredibly low false alarm rate



Primary ML Model Score

CI0100 Secureworks

- 3.3 Trillion Events of training data from XDR Data Lake
- Ensemble Machine Learning approach (many models) to increase accuracy
- High & Critical (Purple Box):
  - 280 True Positives
  - 5 External Red Teams
  - 2 False Alarms
  - 99.3% Precision @
     False Alarm Rate below
     1 in 150 Million (6.6E-9)
     machine-username-hours
- Medium (Green Box):
  - Lower severity, but often worth investigating when seen with other indicators



## AI Vision: AI Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

Detect malicious activity in events (e.g. processes, netflow, DNS, file modifications) and create alerts. Al used to find patterns of malicious activity.
Triage alerts using Al to predict which are most likely to require more in-depth investigation.
Investigate aspects of those high priority alerts automatically with Al-generated summarizations of detection/telemetry/alerts and draft key findings.
Respond: Automatically resolve the problem when customers baye onted in to "Proactive Response"

CIO100 | Secureworks

Produced by CIO | EIDC

## Ransomware Crisis: Dwell Times Plummet to 24 Hours, Demanding Rapid Defensive Response

"Ransomware continues to be the primary threat facing organizations, because of the scope of disruption it can cause and its prevalence. Average dwell times between initial access and ransomware payload delivery have dropped significantly to a median figure of just 24 hours. This year may be the most prolific year for ransomware attacks to date."

- Don Smith, VP Threat Research



2 Secureworks 2023 State of the Threat Report



Produced by CIO | eDC

### **Investigation Predictor**

Using supervised machine learning, we can build a predictive model for investigated alerts

#### **Supervised Machine Learning – Use Cases:**

- Assign a threat score for every High/Critical alert.
- Automatically close alerts with a low threat score.
- Automatically create investigations for alerts with a high threat score.



## AI Vision: AI Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

Detect malicious activity in events (e.g. processes, netflow, DNS, file modifications) and create alerts. Al used to find patterns of malicious activity.
Triage alerts using AI to predict which are most likely to require more in-depth investigation.
Investigate aspects of those high priority alerts automatically with AI-generated summarizations of detection/telemetry/alerts

**Respond**: Automatically **resolve** the problem when customers have opted-in to "Proactive Response"

and draft key findings.

CIO100 Secureworks



RESPOND

#### Generative AI Drives 80%+ Reduction in Investigation Time

Generative AI Capabilities in Taegis

#### **Security Incident Summarization**

UTCLE Sector	n Copultante Ins Tangis XDR Universe source   NISDR				R. Gait back						
mages	a - 2023-09-19 - Physical Space() instances the	the based and the	contrat_								
2023-4	9-19 - [Playbook OpenAl] In	trusion Det	ection - HoneyToken Account A	ccessed /	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)						
-	an ensert metter										
Salar.	Averagione	NETTINGINGS			× 10						
August	(TENE Souths Cognitions into a Dargiture of										
Natio	Madian .	Incident Summary									
		Tangs has detected	d namendul signine in a honory taken unor RC associt by	w2021 ground and herestidenamiant.							
1000	Among Revelopment	Incident De	Incident Details								
Cose .	44	Two advects where to	and to according to a to a being taken our AC a	amouths will be and and homestakerastours. The anishese suggests potential surgers	mine, as the activity is hold, place of an attached attempting to gain oraclifusional						
10	10100073	****									
		Recommend	lations								
Contail Re	API Date Ramp/9306405402946431a.	3. Danie the last	we taken user All annuarts								
Couleé											
United By	Ter Mhite	Mitigations	3. United to the second s								
Linisted	2020/10/20 19:41:00 -072	1. Inpictual last									
-	-	<ul> <li>A segment revenue enzy segment passes previous.</li> <li>E conduct regular rescalar previous finishing for all antistenses.</li> </ul>									
100		Technical Details									
Trise.	PAC3013044 0		and the second se								
Ten	monage - Add Top	and read	teres in the second sec								
		Sec. 1	NAME OF TAXABLE PARTY OF TAXABLE PARTY								
		Conceptor	Particular and a state of the s								
		Theorem .	will be and								
		Same In									
		Chemanan	with an and, have been start								
		Command the taut									
		16/1									
		Reference	References								
i		32.19	Charles (M								

Taegis automatically summarizes incidents reducing one of the most time intensive tasks for Security Analysts.

#### **Command-line & Code Explanation**

Command Line:

"C:\Windows\system32\cmd.exe" /c start azohlcqkbk.vbs&start explorer sofware&exit

Command Line Explanation:

The command string is:
"C:\\Windows\\system32\\cmd\\.exe" /c start azohlcqkbk\.vbs&start
explorer software&exit

This command will open a Windows Command Prompt, execute the VBScript file at "azohlcqkbk\.vbs", open the explorer window at the "software" folder, and then exit the Command Prompt.

Taegis generates easy to understand explanations for command-lines and scriptblocks that it sees within security telemetry keeping analysts within Taegis and reducing overall time-to-respond.

#### Alert Explanation

**1** 

Taegis Playground Principe Response 11	Managed XDR Elite	9, Quick Search	e 💿						
Alens / RESEARCH	t Encoded PowerShell Intrusion Module								
RESEARCH	I: Encoded PowerShell Intru	sion Module ex Copy Link	Actions +						
SUMMARY	EVENTS (##) JSON THREAT INTE	LLIGENCE DETECTOR HISTORY							
States	Open +	Alert Description     Covener	weat Unit**						
Status Resourc Vint Activity Last Activity	None 2023/08/14 13:53:22 UTC (25 days apri) 2023/09/03 07:09/44 UTC (5 days apri)	A process event suscitation with their use of Power/Staff by an introduct model was shortford. This may indicate threat actions are attempting to execute an encoded Power/Staff models on a host in the environment. Modelso can implained functionality such as a result shell.							
Instanting Adv	2023/09/03 07:10:06 UTC (5 days ago)	External References							
Tenere:	Se2, LLC - Red Clock (10271)	Reference title goes here Learn More 🖄							
Detector:	Taegis Watchist, Q.	View Examples							
Ruly ID:	3x8ax5d7-6xx6-6660-9c16- 3x8x27b14c19.()								
Sensor Types	G Red Cloak Q	<ul> <li>Detection Logic Explanation</li> <li>Browned</li> </ul>	ly TeighAl						
Username	SBGLANT\schwart Q	Generated by an Al luared on the assessment of the alert,							
Hostnames;	Toped1631p 9. Toped1631p 9.	This alert is designed to detect a potential infrusion attempt via an encoded PowerShell module, which can be used by attackers to remetely control a system or execute malificaus operations, such as data estituation or system damage.							
Agent/Senuer ID	925c866a6607x0550x6a31141a00 Q, 977c	The detection logic works by examining process events for specific patterns that indicate a use of Powerfibeli indicative of an tookit. The regular expressions used to detect these activities include 'RDLMemorySenant,' convert', and 'powershell'.com'	intrusion In the						
film:	108699_65765_1it_fs2c0x68639a.em powershell.em	scen promis contraction, and partners or excused vaid uses that might normally involve similar contracials for highlighted the scence promision parent image path, to avoid failur positive detections.	indoces (s)						
MD5:-	bc901e61144ded632565013482319868	Muse specifically							
state: trentgations	eb3%26a364ecd0691a5%ca661a90334 112617e This alert has not been added to an	The system is looking for process command lines involving "IOLMensoryDream", "convert", and "powershell', own". These test occar when Powershell is used to a suppliate way. "IOLMensoryDream" and "convert" are often associated with factors user multitum. Powershell commands for proceeding and decoding them.	s aftes I to hide						

Taegis generates contextual alert explanations based on alert logic, alert details, and associated events bringing clarity and context to 10s of thousands of unique detectors.

### CI0100 | Secureworks



## Al Vision: Al Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

**Detect** malicious activity in events (e.g. processes, netflow, DNS, file modifications) and create alerts. Al used to **find** patterns of malicious activity.

**Triage** alerts using AI to **predict** which are most likely to require more in-depth investigation.

**Investigate** aspects of those high priority alerts automatically with AI-generated summarizations of detection/telemetry/alerts and **draft** key findings.

**Respond**: Automatically **resolve** the problem when customers have opted-in to "Proactive Response"



CIO100 | Secureworks

Produced by CIO | OC

### **One Click Automation Setup**

🎁 Ta

0 0

Simplifying Pro-Active Response

- Faster playbook action setup with one click response actions.
- Simplify configuration of common Actions that are shown in the UI throughout various workflows
- Improves automated response experience in Taegis

	2	Configure Actions							1	Apply Settin
		RESPONSE CONTEXT	INVESTIGATIV	E						
arch		Q Search for a keyword or na	× = Show: All +							
ents		RESPONSE ACTIONS 🛛 🔳	STATUS =	ON WHAT CO		ENABLE WHEN	=	SET AS SUBTENANT DEFAU	.⊤ =	ACTIONS
		Isolate Host	On On	Custom		Always		Yes		1
	<u> </u>	Undo Isolate Host	Off Off	All		Always		No		1
	>	Block IP	Off Off	Custom		Only When		Yes		1
	•	Unblock IP	On On	All		Only When		Yes		1
	•	Disable User	On On	Custom	Isolate Host					
		Enable User	On	Custom		n a late et severa a sol 7 2 2				
		Lorem Ipsum	On On	All	Customise Action Name Isolate Host		ACTIVITY CONNECTIONS			
		Lorem Ipsum	On On	All			Select the activities which will run within each execution of this playbook.			
		Lorem Ipsum	Off Off	All	Helper text On what connections?  Custom All		Taegis.BlockiP:1.0.0			
		Lorem Ipsum	Off	Off Custom						
		Lorem Ipsum	On On On	Custom			U	NAME		
		Lorem Ipsum		Custom			0	Block IP Cisco Meraki	Ico Meraka	
								Block IP PaloAlto Networks PAN	OS	
					Enable whe	n?		Block IP Secureworks iSensor		
					Always					
					This playb	ook runs every tim	e an alert is	created		
					O Common	Filters				
					When	the asset has Tag	Flag ISOLATION_APPROVED			
					Only When This playback only curs when the conditions you define are met					
						oon only rons into		and for active and meet		
					Write your own CEL expressions for trigger conditions in the box above.				e. View	
					CEL Syntax.					





### AI & Automation Delivering on Security Outcomes

124

#### **Customers protected** by Hands-on-Keyboard investigations

Patented detector finding Threat Actors "living off the land" even if zero days are used as initial access vector.

### 50%+

#### **Noisy Alerts Auto-Remediated** by Machine Learning

Patented Alert Prioritization that learns hourly reduced analyst workload by over 50%, which along with other automations led to reduction in customer response time by 80%.

## 40-60% 80%

**Fully Automated** Investigations

Orchestration engine fully automating nearly half of all investigations and response actions.

**Reduction in** Median Time to Notify

Variety of AI and automation use cases leveraged to reduce analyst workload, automate triage, explain complex telemetry, draft investigation summaries.

### CIO100 Secureworks

Produced by CIO =DC





Produced by CIO | **EDC**