
CIO 100
Symposium & Awards
Produced by CIO | IDC

Integrated AI Approach to Better Security Operations with Secureworks® Taegis™

Nash Borges, PhD
VP Software Engineering

CIO 100 | Secureworks® Produced by CIO | IDC

Secureworks Uniquely Positioned to Excel in AI

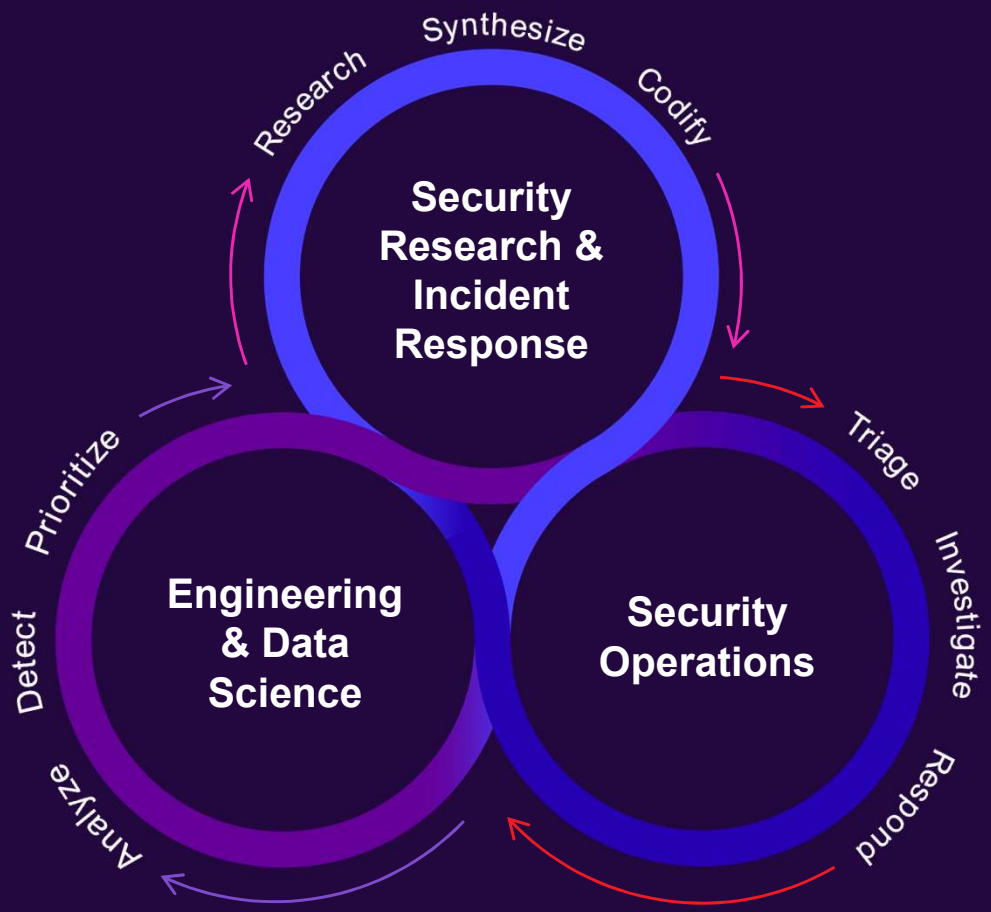
Volume & Variety of Data

+

Security Experts
Investigating What Matters

+

Data Science Expertise
to Leverage It



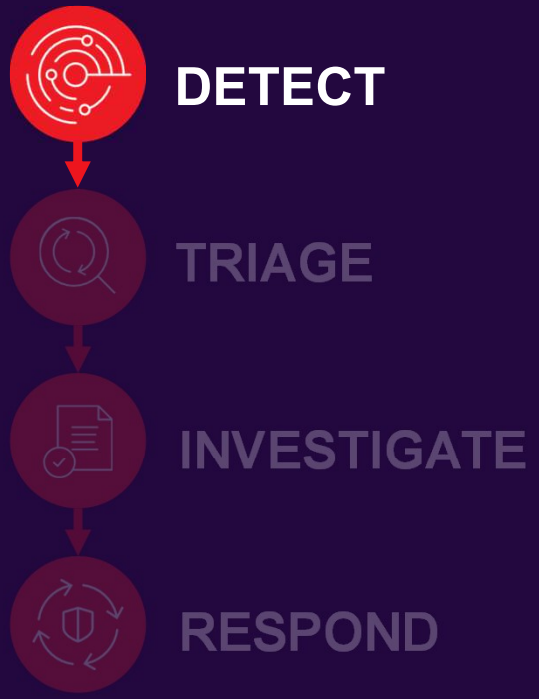
AI Vision: AI Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

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

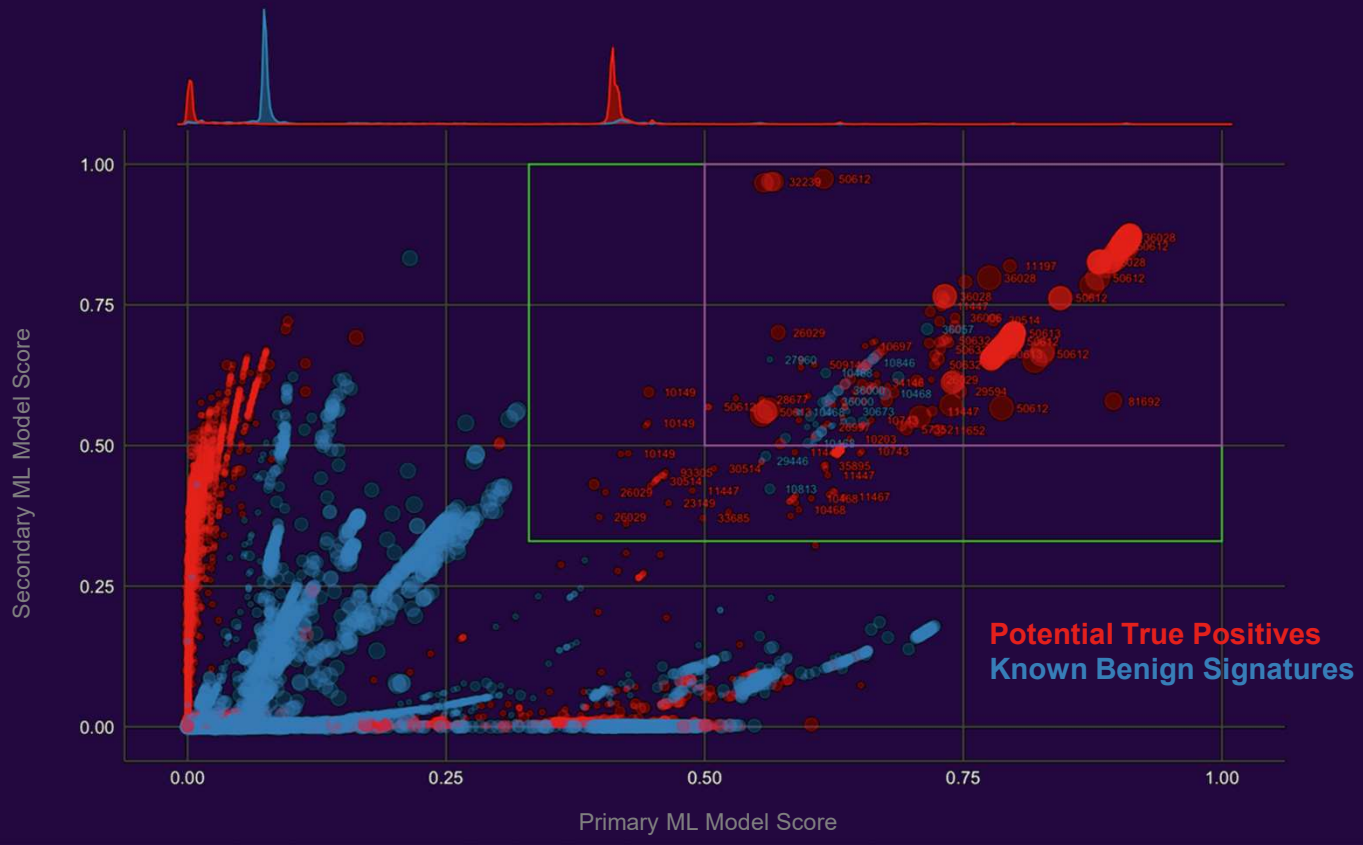
Triage alerts using AI to **predict** which are most likely to require more in-depth investigation.

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"



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



- 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

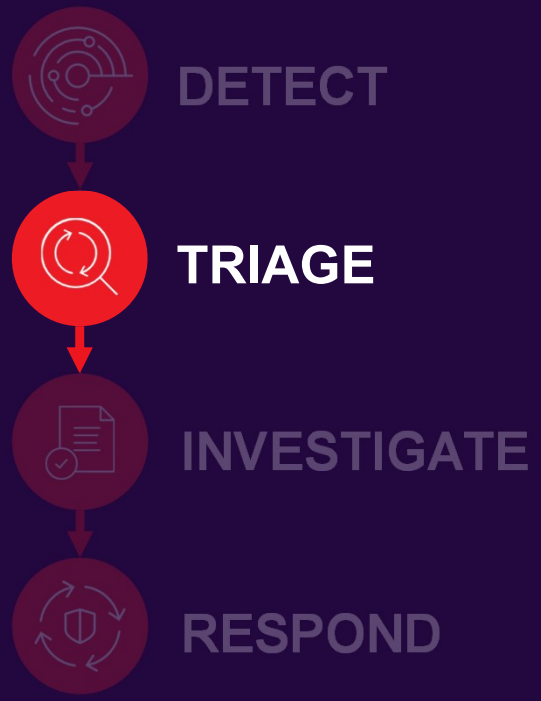
AI Vision: AI Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

Detect malicious activity in events (e.g. processes, netflow, DNS, file modifications) and create alerts. AI 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"



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

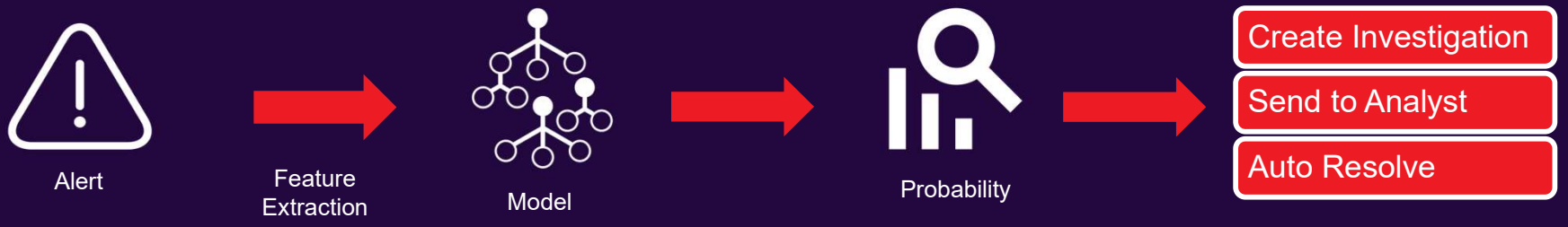
2 Secureworks 2023 State of the Threat Report

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.



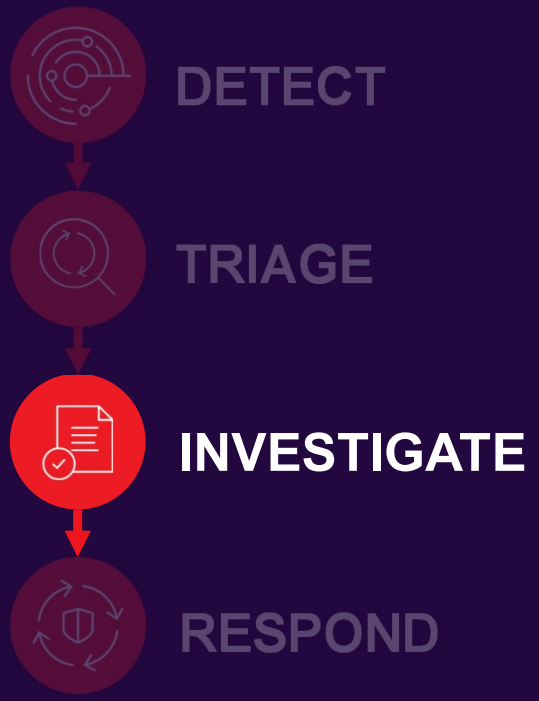
AI Vision: AI Leveraged Across Threat Detection & Response Lifecycle for Efficiency, Coupled with Human Expertise to Stay Ahead of the Adversary

Detect malicious activity in events (e.g. processes, netflow, DNS, file modifications) and create alerts. AI 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.

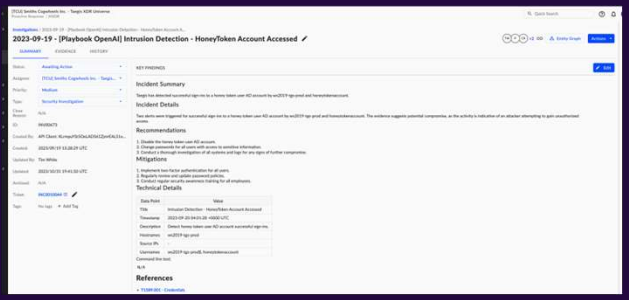
Respond: Automatically **resolve** the problem when customers have opted-in to "Proactive Response"



Generative AI Drives 80%+ Reduction in Investigation Time

Generative AI Capabilities in Taegis

Security Incident Summarization



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

Command-line & Code Explanation

Command Line:

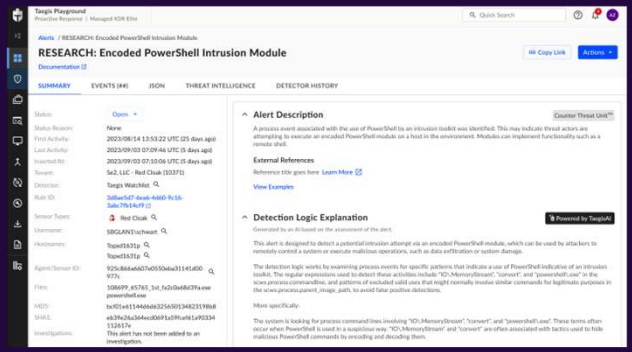
```
"C:\Windows\system32\cmd.exe" /c start azohlcqkbk.vbs&start explorer sofware&exit
```

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 script-blocks that it sees within security telemetry keeping analysts within Taegis and reducing overall time-to-respond.

Alert Explanation



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.

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. AI used to **find** patterns of malicious activity.

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

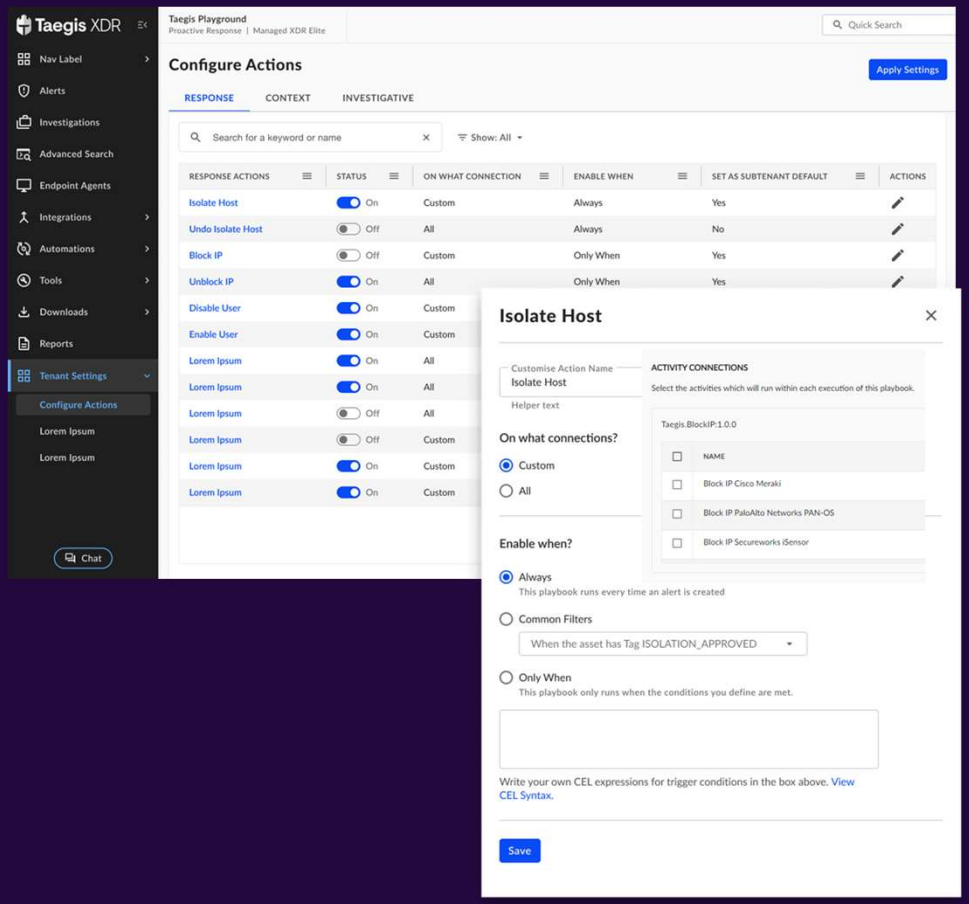
Investigate aspects of those high priority alerts automatically with AI-generated summarizations of detection/telemetry/alerts and **draft** key findings.

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

One Click Automation Setup

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



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%

Fully Automated Investigations

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

80%

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.

Q&A