Conduct faster, context-driven investigations into active cyberattacks with Vectra and Chronicle

CHALLENGE

Cyberattackers easily circumvent network perimeter security to spy, spread and steal assets inside networks.

As a result, cybersecurity teams are saddled with manual, time-consuming threat investigations and costly forensic analysis, often after damage is done.

SOLUTION

The Vectra threat feed provides real-time, correlated attack detections to enhance the operational intelligence from Chronicle Backstory.

Integrating the Cognito platform's AI-based detection algorithms with Chronicle enriches the context of threat investigations and speeds-up incident response.

BENEFITS

- Quickly mitigate and stop cyberattacks before damage is done
- Gain greater context into every attack by prioritizing infected hosts that pose the highest risk and correlate threats with security telemetry
- Search and analyze threat detections more easily

It's time for a new cybersecurity approach

Modern cyberattackers with sophisticated hacking tools or the right stolen password can easily evade perimeter security to spy and steal inside the network, going largely undetected.

This gap leaves security teams manually chasing down security alerts and events. The inability to determine which alerts pose the highest risk to an organization complicates the task even further.

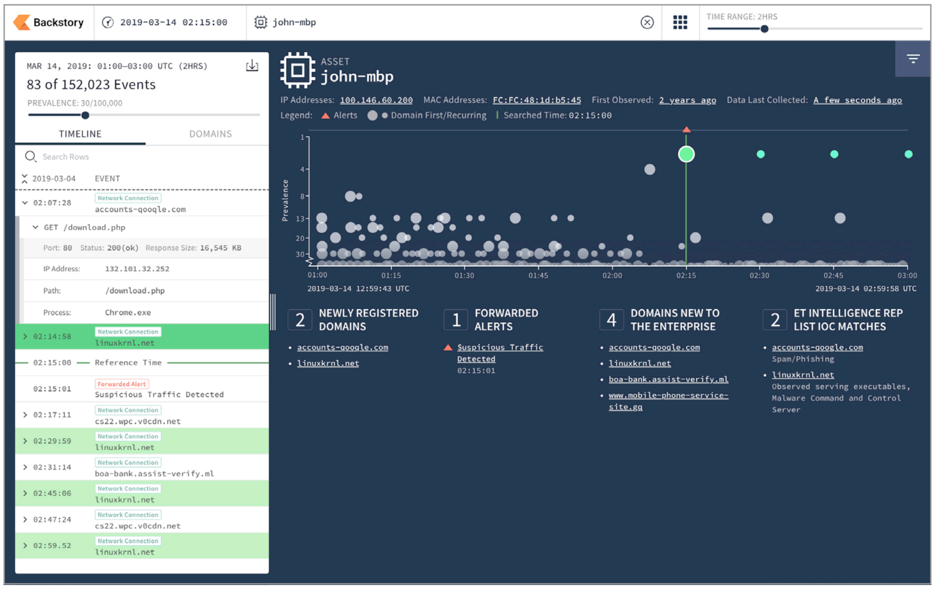
In practice, this often means breaches are discovered and reported by an external third-party after theft or damage has occurred. This can result in a debilitating post-breach investigation that can cost upwards of millions of dollars, not to mention unwanted negative publicity and brand damage.

The Cognito™ threat detection and response platform from Vectra® seamlessly integrates AI-based threat hunting and incident response of Chronicle Backstory, a global security telemetry platform, for increased context during investigations and hunts and greater operational intelligence.

Together, Vectra and Chronicle deliver a practical solution to the most persistent problem facing today's cybersecurity teams—finding and stopping active cyberattacks.

Integration creates a superior threat detection model

The Cognito platform uses supervised and unsupervised AI models to detect cyberattacks across all phases of the attack kill chain, ranging from command and control, internal reconnaissance, lateral movement and data exfiltration, without depending on signatures or reputation lists.



MAR 14, 2019: 01:00–03:00 UTC (2HRS)

83 of 152,023 Events

PREVALENCE: 30/100,000

```
2019-03-04   EVENT
02:07:28     Network Connection
             accounts-qooqle.com
  GET /download.php
    Port: 80   Status: 200(ok)   Response Size: 16,545 KB
    IP Address:   132.101.32.252
    Path:         /download.php
    Process:      Chrome.exe
02:14:58     Network Connection
             linuxkrnl.net
02:15:00 — Reference Time
02:15:01     Forwarded Alert
             Suspicious Traffic Detected
02:17:11     Network Connection
             cs22.wpc.v0cdn.net
02:29:59     Network Connection
             linuxkrnl.net
02:31:14     Network Connection
             boa-bank.assist-verify.ml
02:45:06     Network Connection
             linuxkrnl.net
02:47:24     Network Connection
             cs22.wpc.v0cdn.net
02:59.52     Network Connection
             linuxkrnl.net
```

ASSET
john-mbp

IP Addresses: 100.146.60.200   MAC Addresses: FC:FC:48:1d:b5:45   First Observed: 2 years ago   Data Last Collected: A few seconds ago

Legend: ▲ Alerts ● ● Domain First/Recurring | Searched Time: 02:15:00

2019-03-14 12:59:43 UTC   2019-03-14 02:59:58 UTC

2 NEWLY REGISTERED DOMAINS
- accounts-qooqle.com
- linuxkrnl.net

1 FORWARDED ALERTS
- ▲ Suspicious Traffic Detected 02:15:01

4 DOMAINS NEW TO THE ENTERPRISE
- accounts-qooqle.com
- linuxkrnl.net
- boa-bank.assist-verify.ml
- www.mobile-phone-service-site.gq

2 ET INTELLIGENCE REP LIST IOC MATCHES
- accounts-google.com Spam/Phishing
- linuxkrnl.net Observed serving executables, Malware Command and Control Server

Cognito detects these threats by analyzing the underlying behavior of attackers from the objective viewpoint of the network. All threat detections are correlated with the hosts involved in the attack, while Cognito's risk and certainty scores prioritize the hosts posing the highest risk.

This enables security teams to detect new and unknown threats, as well as discover attacks that do not rely on malware, such as malicious insiders or compromised user accounts.

The integration pulls the Cognito metadata-enriched detections directly into the Chronicle Backstory dashboard. Now, organizations can incorporate high-value detections from Cognito into their existing workflows and automate correlation in the Backstory security telemetry, providing greater context to threats and attacks.

Faster investigations and response

The Cognito platform scores and ranks network hosts by risk. To enable faster investigation and response, all malicious behaviors are automatically associated to the physical network host, even if the IP address changes.

Integration of the Cognito and Backstory platforms provides an interactive dashboard to quickly show the number of hosts classified as critical, high, medium and low risk.

These scores help security teams prioritize events, eliminating the need to manually triage every event and vastly improving response time.

Full visibility and enhanced threat intelligence

By analyzing all cloud and on-premises enterprise traffic, the Cognito platform reveals threats in all phases of an active cyberattack.

Cognito provides this extraordinary range of threat intelligence and security telemetry to the Chronicle machine-data repository, including detections of unknown malware and attack tools, threats that hide in common applications and encrypted traffic, and in-progress threats across every phase of the attack kill chain.

This visibility allows security teams to instantly distinguish opportunistic botnet behaviors from more serious targeted threats, enabling quick action before assets are stolen or damaged.

Real-time correlation, additional context and searchable repositories

The Vectra approach to detection enables security teams to detect threats that were missed by other security solutions.

The Cognito integration with Chronicle Backstory easily connects and correlates Vectra's findings with other third-party solutions, pulling in additional context for the security team.

Chronicle also captures, indexes and correlates Cognito threat detections in real time, making them available in a searchable repository so security teams can generate graphs, reports, alerts, dashboards and visualizations.

Key features

Together, Cognito and Chronicle:

- Enable fast, efficient investigations and response
- Provide full visibility and context into threats across the kill chain
- Connect and correlate findings across security solutions to create a searchable repository

About Vectra

Vectra® is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. For more information, visit vectra.ai.

About Chronicle Security

Chronicle was born in 2016 as a project within X, Alphabet's moonshot factory. As an Alphabet company, we bring unique resources and talent to the goal of giving enterprises, and the people within them, the tools to win the fight against cybercrime.

We see a future where enterprise security teams can find and stop cyberattacks before they cause harm. By applying planet-scale computing and analytics to security operations, we provide the tools teams need to secure their networks and their customers' data. We turn the advantage to the forces of good. For more information, visit chronicle.security.

VECTRA®
Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai