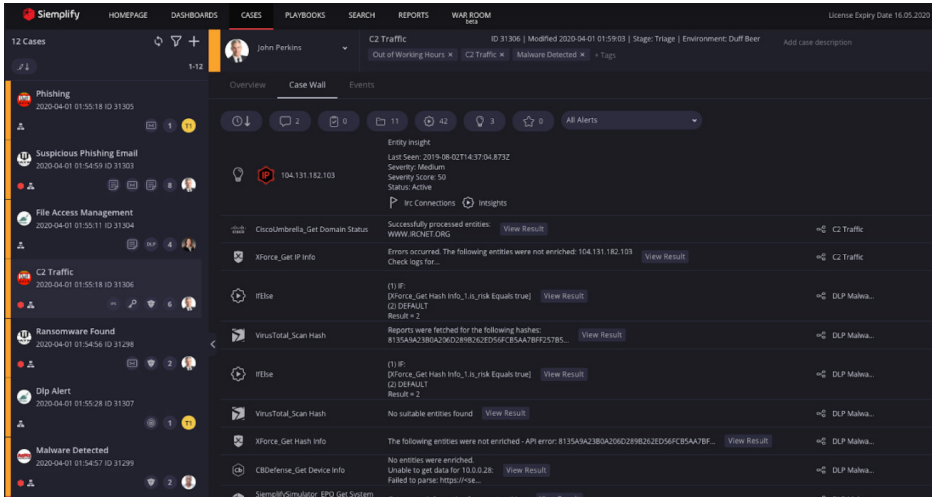
VECTRA SECURITY THAT THINKS® | Siemplify

SOLUTION BRIEF

# Automated, actionable intelligence stops threats faster

## Work threat-centric cases instead of meaningless alerts.

Reduce caseload by working prioritized threat-centric cases instead of trivial alerts. The integration with Vectra enables creation and continuous analysis of alerts created from Vectra threat detections, identifying and grouping related security alerts into cases.




Equip SOC teams with tools, processes and context to drive smarter investigations and response.

## CHALLENGE

Visibility into threats across the organization is in short supply. Countless security tools, processes, and interfaces compete with each other for attention and add complexity and manual work to an already overburdened SOC team, increasing the risk of an incident.

## SOLUTION

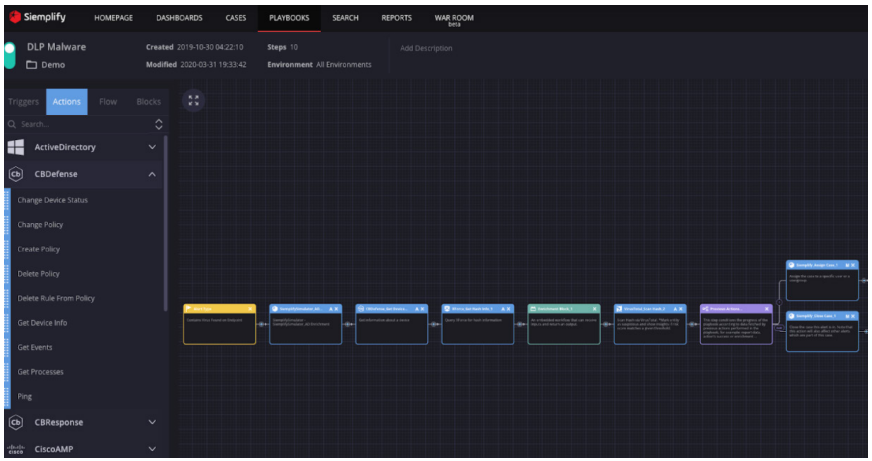
Vectra's Cognito integration with the Siemplify security orchestration, automation and response (SOAR) platform enables automatic threat detection enrichment, context-driven investigations and the ability to create repeatable responses.

## BENEFITS

- Reduce alerts by as much as 80% through grouping and prioritization.
- Increase analyst caseload capacity by 300% through automation and playbooks.
- Reduce mean time to respond with enriched alert data.

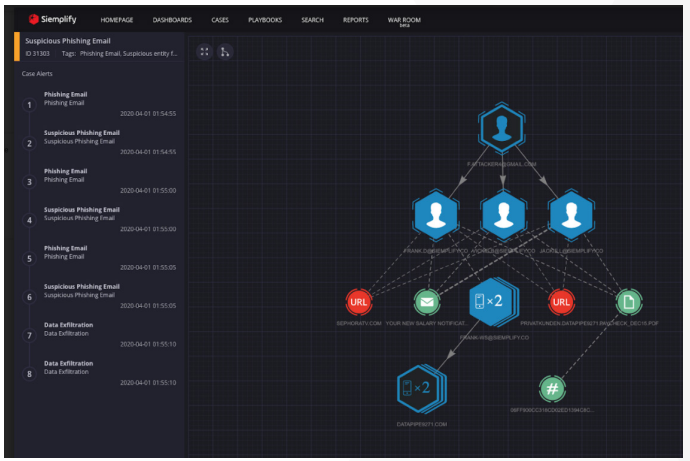
## Create repeatable, automated response processes.

Transform alerts into customizable playbook processes that can automate everything from case enrichment to response.



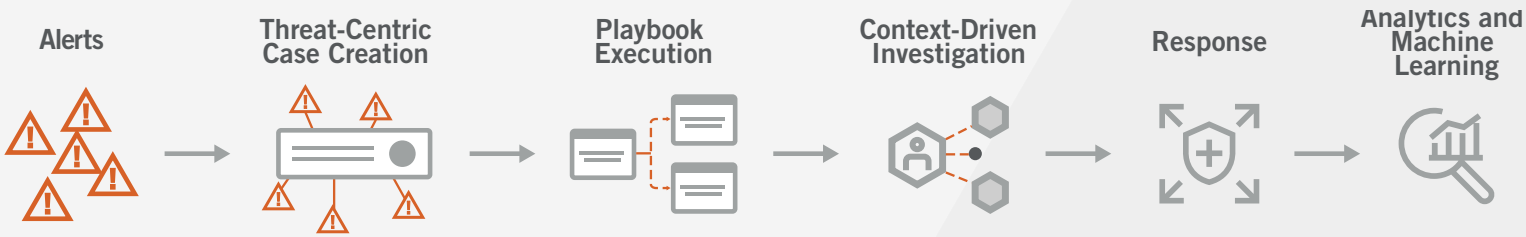

## Conduct context-driven investigations.

Siemplify enriches individual alerts generated from Vectra threat detections with data from across the environment, grouping related alerts into cases to give analysts the context needed to focus on truly malicious activity.




## How it works

Simply download the Vectra integration, configure and you're on your way! As Vectra Cognito detects threats on the network, Siemplify will ingest those to create Siemplify alerts and enable orchestration with playbooks or manual analysis.



## About Vectra

Vectra® is a leader in network detection and response – from cloud and data center apps and workloads to user and IoT devices and accounts. Its Cognito® platform accelerates threat detection and investigation using AI to enrich network metadata and cloud logs it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers four 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. Cognito Detect for Office365 and Azure AD™ finds and stops attacks in enterprise SaaS applications and the Microsoft 365 Ecosystem.

## About Siemplify

Siemplify, the leading independent security orchestration, automation and response (SOAR) provider, is redefining security operations for enterprises and MSSPs worldwide. The Siemplify platform is an intuitive workbench that enables security teams to manage their operations from end to end, respond to cyber threats with speed and precision and get smarter with every analyst interaction. Founded in 2015 by Israeli Intelligence experts, with extensive experience running and training security operations centers worldwide, Siemplify has raised $58 million in funding to date and is headquartered in New York, with offices in Tel Aviv. Visit us at siemplify.co and follow us on Twitter and LinkedIn.

**For more information please contact a service representative at info@vectra.ai.**

Email info@vectra.ai vectra.ai