SOLUTION BRIEF

SWIMLANE & ATTIVO NETWORKS EMPLOYEE ACCESS AUDITING

BUSINESS CHALLENGE

Did you know that cybersecurity attackers average over 56 days in a network before detection? This head start gives attackers plenty of opportunities to complete their mission. Today's attackers are smart. They don't fall for emulated or low interaction decoys or credentials that don't appear to be legitimate. With malicious threats growing at an alarming rate, enterprises need a way to detect, diffuse, and misdirect attackers quickly.

WHY WE WORK BETTER TOGETHER

Cybersecurity attackers have the uncanny ability to get inside a network and linger for days. Enterprises need to be able to identify the attack and have the ability to respond at machine speed. By working together, Attivo can detect even the most hidden attacker with their ThreatDefend platform, and Swimlane can load a response that is ready to take action. This coordinated response from Attivo and Swimlane can really be a game-changer, especially as it relates to zero-day attacks and never before seen exploits.

SOLUTION OVERVIEW

Both the Attivo ThreatDefend platform and the Swimlane platform are potent tools, but their strengths can be even greater through this joint integration. With the ThreatDefend platform's ability to deploy decoys and collect intelligence on attacks, it collects tremendous data that would be actionable within Swimlane if ingested. The ThreatDefend platform can also spin up decoys if they detect suspicious activity, or launch playbooks of its own to aid in a speedy response.

Swimlane can connect to the Attivo API and pull in many of these capabilities that the ThreatDefend platform offers, giving users a centralized management platform across all of their integrated tools. This connection also allows for Attivo events and data to trigger automated workflows for triage across any of your Swimlane integrated products. It enables security teams to extend the playbooks Attivo offers and create some of their own via workflows. In addition, security personnel can also use or correlate enrichment coming back from Attivo to other cases to help make automated or single click decisions on severity. All of these benefits lead to less time spent by analysts on remediation, centralized management for maximizing time, and to enable teams to respond across product silos with machine speed.

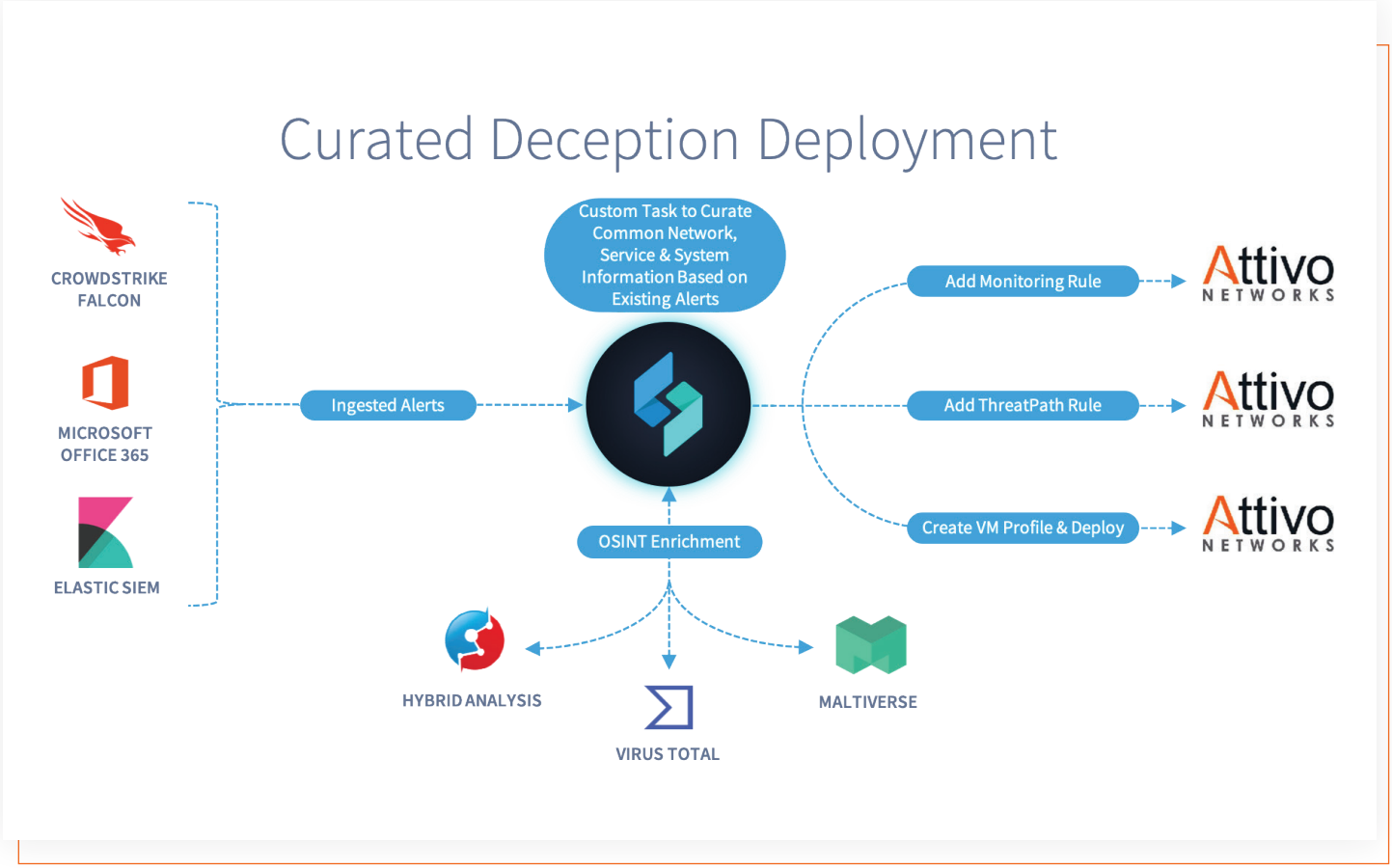
BENEFITS

- Early detection of threats with automated responses
- Activate actions based on the type of threat, risk, and certainty
- Reduction of alert triage and backlog

SOLUTION AT A GLANCE

- Attivo BOTSink increases visibility across your network
- Swimlane can ingest events from Attivo to trigger automated responses
- Enables responses at machine speeds
- Centralize case management
- Fewer product silos

HOW IT WORKS



BETTER TOGETHER

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and attack lateral movement detection, provides scalable protection, detection, and data concealment solutions for endpoints, Active Directory, and network devices. Comprehensive coverage is available for on-premises, clouds, remote worksites, and specialized attack surfaces. Automated attack analysis and third-party integrations accelerate incident response.

www.attivonetworks.com

ABOUT SWIMLANE

Swimlane was founded to deliver scalable innovative and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane is at the forefront of the growing market for security automation and orchestration solutions that automate and organize security processes in repeatable ways to get the most out of available resources and accelerate incident response.

www.swimlane.com