SWIMLANE

Solution Brief

Swimlane and Darktrace

Improving threat detection and response to empower teams to jumpstart remediation.

Challenge

Businesses face the threat of novel and advanced attacks moving at machine speed and hitting parts of their digital infrastructure that they are not prepared to secure. At the same time, cyber security teams are facing a staffing and skills shortage, and they must manage disparate security stacks that more often than not present too many alerts to triage appropriately – leaving the real threats unnoticed or improperly managed.

Solution

Leveraged together, Darktrace and Swimlane improve threat detection and response, ensuring even new and novel attacks can be stopped, and empowering your team to jumpstart remediation. The Darktrace Cyber AI Platform gives you the enterprise-wide visibility and powerful detection ability of self-learning AI, while Swimlane lets you integrate the Platform with your existing technologies, automating and orchestrating the workflows that work best for your particular organization and use cases.

Benefits of Integration

- Resolve attacks with accurate and efficient threat management
- Detect the full range of cyber-threats and ensure optimal response and remediation.
- Accelerate threat management without adding time or effort to your workday.

Face any attack with highly accurate and efficient threat management.

Cyber-threats are evolving, and the volume of these ever more sophisticated and novel threats will not stop increasing. Moreover, as businesses continue leveraging diverse cloud and IoT environments, the expanding complexity and scale of their digital infrastructures make it difficult for already overworked security teams to ensure complete protection and proper implementation of security protocols.

To defend every extent of their enterprise, organizations require cyber security solutions that empower them to consistently identify real threats and respond intelligently – no matter where, when, or how the attack is made manifest. Together, Darktrace and Swimlane do just that.

Solution at a Glance

- Gain enterprise-wide visibility
- Detect novel and advanced attacks
- Connect insights across your infrastructure
- Accelerate threat management

DARKTRACE

Connect insights across your infrastructure with Cyber AI and SOAR.

Swimlane is your solution for automating and orchestrating the many manual, recurring, and repetitive tasks that come with managing an increasingly diverse security stack. Swimlane accelerates threat management by correlating alerts across security tools and automating your incident response workflows, giving your team time to concentrate on threat hunting and more critical security decision-making. With Swimlane, you can integrate your people, technology, and processes to fit the distinct requirements of your enterprise.

The Darktrace Cyber AI Platform is the world's leading solution for early threat detection and Autonomous Response. The platform uses machine learning and AI to understand the unique 'patterns of life' for every user, device, and technology that touches your digital infrastructure, building a bespoke knowledge of 'self' for your business. This allows Darktrace to recognize malicious behavior without a pre-configured definition of 'good' or 'bad,' spotting even the most subtle anomalies that may point to a novel or advanced cyber-attack.

A fundamentally unique element of the Cyber AI Platform is its ability to correlate insights from across your organization, whether in the cloud, industrial control system, or on-premise network. This rich, enterprise-wide context ensures that the workflows Swimlane automates and orchestrates for your security team are as effective and intelligently executed as possible.

With the power of the Darktrace Cyber AI Platform and Swimlane's security orchestration, automation, and response (SOAR) technology behind you, you can detect the full range of cyber-threats and empower your team to ensure optimal response and remediation.

Empower your team with early detection and robust response.

The Darktrace Cyber AI Platform is the world's first and only security solution that learns 'on the job', adapting as your business evolves. While traditional defenses rely on pre-programmed and retrospective controls, Darktrace's Cyber AI is designed to immediately pick up on novel or advanced threats that inevitably get through.

With this joint solution, should Darktrace detect the signs of a zero-day attack that no other security tool in your stack can see, the Platform can send detailed information about the threat to Swimlane. Swimlane can then trigger a workflow that your team has already decided is appropriate for responding to that particular situation – say, to reconfigure a firewall, or to search and collect possible Indicators of Compromise from your other tools.

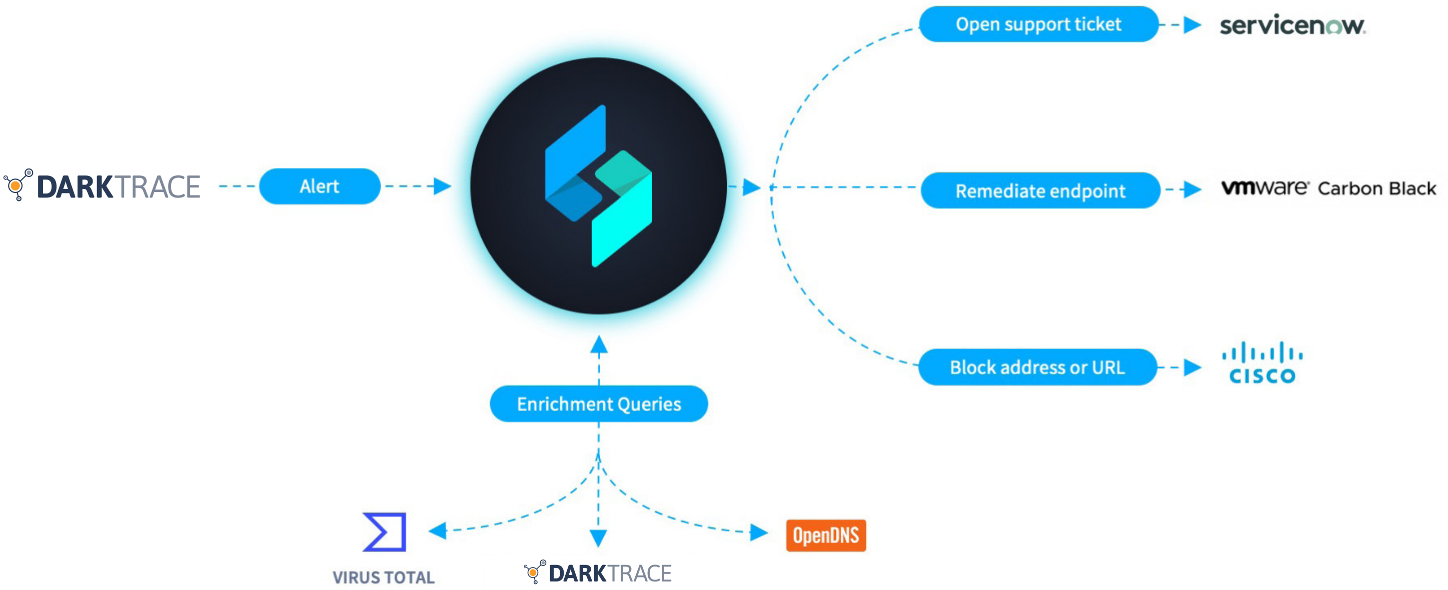
Swimlane's dynamic correlation capabilities can also be used to trigger a defined protocol based on receiving multiple alerts from specific sources. For instance, if alerts come from both Darktrace and another tool that you know signify a breach of company policy when seen together, Swimlane could trigger a workflow to immediately send an email to certain stakeholders.

By feeding the broad visibility and deep insight of Darktrace's self-learning AI into Swimlane's automatically orchestrated workflows, you can ensure that even the stealthiest threats will be detected and responded to appropriately. Together, Darktrace and Swimlane empower your team to accelerate threat management – without adding time or effort to your workday.

With this joint solution, you can be confident that you'll catch every genuine threat in real time, while enhancing analyst capacity and augmenting decision-making.

How it works

The Darktrace Cyber AI Platform correlates insights from across your digital infrastructure to detect even the stealthiest threats, while Swimlane integrates your people, processes, and technology for optimal response and remediation.



Better Together

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 3,500 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems. This includes insider threat, industrial espionage, IoT compromises, zero-day malware, data loss, supply chain risk and long-term infrastructure vulnerabilities.

About Swimlane

Swimlane is the leading independent SOAR solution created by analysts for analysts. It delivers scalable security solutions to organizations struggling with alert fatigue and analyst burnout.