

Preview

Enterprise Immune System V4

Including Cyber AI Analyst

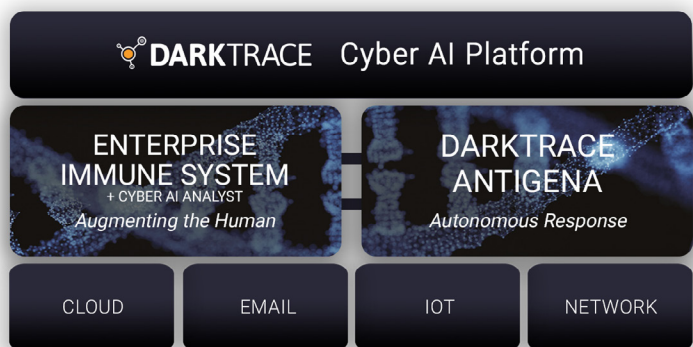
Cyber AI Analyst is the product of a research initiative from Darktrace's R&D Center, which combines analyst intuition with the consistency, speed, and scalability of AI during investigations. In addition to Cyber AI Analyst, new features of V4 include native cloud and container support, increased flexibility and control of Autonomous Response capabilities, and enhanced executive reporting.

Over 70 new enhancements, including:

- Darktrace Cyber AI Platform with Enterprise Immune System and Antigena Autonomous Response
 - Featuring Cyber AI Analyst technology from Darktrace's R&D Center
 - Significant cloud improvements including:
 - New AWS VPC Traffic Mirroring and Azure vTAP support
 - New support for modeling containerized systems (Docker, Kubernetes)
 - New support for SharePoint, OneDrive, and coverage of multiple Office 365 domains
 - Enhanced Antigena flexibility and control from the Enterprise Immune System across network, email, and cloud
 - Enhanced executive reporting with new metrics and features
 - Mobile App improvements including easier configuration, real-time push notifications, and new Cyber AI Analyst outputs
 - New Darktrace App for ServiceNow which creates custom entries in ServiceNow for each incident
-

Announcing the Darktrace Cyber AI Platform

Darktrace's mission is to make the world more secure in the face of machine-speed threats and targeted human-driven attacks. By augmenting human security teams and autonomously responding to attacks, the Darktrace Cyber AI Platform reduces the risks of data theft and technology disruption that organizations face on a daily basis. The software is offered on a SaaS subscription-based model that spans cloud security, email security, IoT/OT security, and network.



The Darktrace Cyber AI Platform is composed of two tightly integrated flagship products: the self-learning Enterprise Immune System and Antigena Autonomous Response technology. Our customers benefit from uniquely effective algorithms that are operating across thousands of organizations.

With Darktrace Antigena, we created the first Autonomous Response solution capable of fighting back at machine speed, and this technology is stopping an attack every 3 seconds around the world. Now with the Enterprise Immune System Version 4, the Cyber AI Analyst is augmenting human security teams by automating threat investigations at speed and scale, and dramatically reducing 'time to meaning' in the context of a fleshed out understanding of the nature and root cause of a security incident.

The Cyber AI Analyst

Human analysts investigate threats by finding patterns, forming hypotheses, reaching conclusions, and sharing their findings with the rest of the business. These are labor-intensive steps that take time and expertise. Yet by learning how expert humans investigate threats, the Cyber AI Analyst is able to form hypotheses and reason to conclusions at a speed and scale that no human ever could.

The Cyber AI Analyst is powered by various forms of machine learning, such as deep learning, as well as a large, complex, and ever-growing data set that captures the various ways that Darktrace's world-class analysts investigate threats detected by the Enterprise Immune System.

By combining this rich data set with AI, the Cyber AI Analyst can conduct expert investigations into hundreds of parallel threads simultaneously, stitching together a constellation of alerts and indicators and developing a meaningful understanding of incidents at machine speed. It then communicates its results and recommendations in the form of a meaningful security narrative that can be reviewed and actioned by executives and end-users alike.

92% reduction
in time to triage

The fact that the Cyber AI Analyst conducts investigations before surfacing anything to the human allows it to discard low-priority or benign events from the start, presenting only a few high-priority incidents at any one time. This empowers users to spend less time trawling through alerts and more time prioritizing strategic work – from focused incident response and threat hunting, through to security modernization and risk mitigation across the business.

Crucially, the Cyber AI Analyst is able to adapt to new and unique situations on the fly, automating thoughtful tasks rather than pre-defined play-books or encoded human knowledge. This is AI that never sleeps, that can intelligently correlate and understand disparate data points at machine speed, and that can communicate its findings to the human in a way that quickly illuminates the presence of an emerging threat.

Key Benefits

- Augments human teams by investigating threats detected by the Enterprise Immune System
- Buys back time so teams can focus on more strategic work and mitigating risk
- Forms hypotheses and reasons to conclusions at a speed and scale that no human ever could
- Automatically communicates incidents with contextual security narratives
- Harnesses the expertise of our world-class analysts and makes it available to everyone

“

We've seen amazing results. The AI Analyst found a channel to an AWS attack where the data leaked out slowly over two weeks. It showed the human analysts how the attacker shaped the route.

”

Mike Beck,
Global Director of Threat Analysis,
Darktrace

Cyber AI Analyst Investigation

