Industry Spotlight: Government and Defense

DARKTRACE

AT A GLANCE:

- Protects more than 270+ government and defense organizations globally
- Detects in-progress attacks with Self-Learning AI technology
- Stops emerging cyber-threats in an average of 2 seconds
- Operates across SaaS, cloud, IoT, email, endpoints, OT technology, and the traditional network.

With state-sponsored attacks increasing in speed and scale, cyber security is a top priority for government and defense organizations. Darktrace uses AI to detect and respond to novel and sophisticated threats – from fast-moving ransomware to low-and- slow data exfiltration.

Industry Challenges

Government and defense organizations are targeted by a wide range of cyber threat actors, from well-organized cyber-criminal groups with financial goals, to hacktivists and state-sponsored groups with geo-political motivations. In recent years, the public sector has become increasingly targeted by ransomware, with threat actors capitalizing on outdated technology and operating systems across local and central government.

These organizations are often tasked with defending complex and interconnected digital infrastructures, where access to systems often has to be shared with think-tanks, trusts, and third parties for collaboration.

This interconnected digital infrastructure has also led to an increasing adoption of cloud technology and SaaS applications, which broaden the attack surface and offer cyber-criminals new avenues for entry. Maintaining connectivity and visibility over these diverse digital estates often involves the use of multiple security tools, which work independently and are unable to give the full picture of activity that spans across multiple silos.

Further complicating the situation is the adaptation these organizations have made to hybrid working. With employees working from offices and homes, hotels and coffee shops, endpoint devices face a broad range of cyber-threats, and present another point of entry for attackers, who are constantly developing new techniques to exfiltrate and encrypt the information these devices hold.

With cyber-threats increasing in complexity and intensity, government and defense organizations require security technology that can keep up with the modern threat landscape, protect every corner of their complex digital infrastructure, and respond at machine speed to fast-moving attacks.

Darktrace Self-Learning AI

Proven to protect hundreds of government and defense organizations, Darktrace's Self-Learning AI defends digital data and vital systems from threat - no matter how novel or sophisticated.

> ***As a Self-Learning technology, Darktrace is able to identify and respond to fast-moving ransomware at an early stage without relying on prior attack data, and operates across SaaS, cloud, IoT, email, endpoints, OT technology, and the traditional network.***

Darktrace works by learning what 'normal' looks like for every user, device, and virtual machine in an organization's dynamic workforce. Darktrace spots indicators of malicious activity as they emerge, instantly flagging them to security teams, and autonomously responding to neutralize the threat at machine speed.

Cyber AI Analyst optimizes threat investigation by continuously examining every security threat that arises. It spotlights the highest priority threats at any one time and rapidly synthesizes the context around an attack into a natural language report. This ultimately reduces time-to-meaning and time-to-response, allowing security team members time to use their expertise where it really matters.

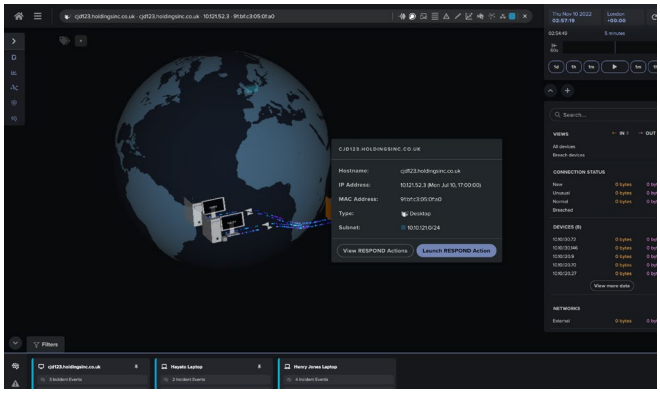

Figure 1: Darktrace RESPOND acting on an identified threat.

> Darktrace enables us to identify threats across our network in a timely manner. There's a huge benefit to having the AI look at data across email, SaaS, and the network. With this cross-platform visibility, we can see every stage of an attack from initial phish all the way through to impact.
>
> / Chief Information Security Officer, Government & Defense

Attack Case Study: Eking Ransomware

At a governmental organization in APAC, Darktrace detected a Ransomware-as-a-Service (RaaS). With Darktrace, the defenders were able to recognize the anomalous behavior as soon as it occurred and stop the threat from advancing, while Cyber AI Analyst autonomously investigated and reported on every stage of the incident.

The attack started when a corporate device was infected with Eking, a RaaS. Darktrace's Self-Learning AI detected and alerted on this threat immediately, picking up on internal reconnaissance activity, SMB enumeration, and extensive scanning.

Once the scanning was complete, files were encrypted on a second server, with the infected device transitioning from making just a few internal connections per day to making thousands in less than an hour.

While Darktrace's alerts and investigations empowered the team to take action straight away, this all this occurred late at night local time – when the security team were out of office. As it was, they were still able to act faster than they otherwise would have and limit the damage when they arrived in the morning.

Had Darktrace RESPOND been deployed, the AI would have autonomously taken action at the first stage of the attack and prevented encryption occurring.

> One of the great features that we're utilizing as part of our continuous monitoring is Cyber AI Analyst. It gives us clear, high-fidelity information containing actionable intelligence, enabling us to make effective decisions. Also, we've seen a reduction in unwanted noise, which allows the team to pivot on more strategic work.
>
> / Head of Security Operations and Resilience, Government & Defense

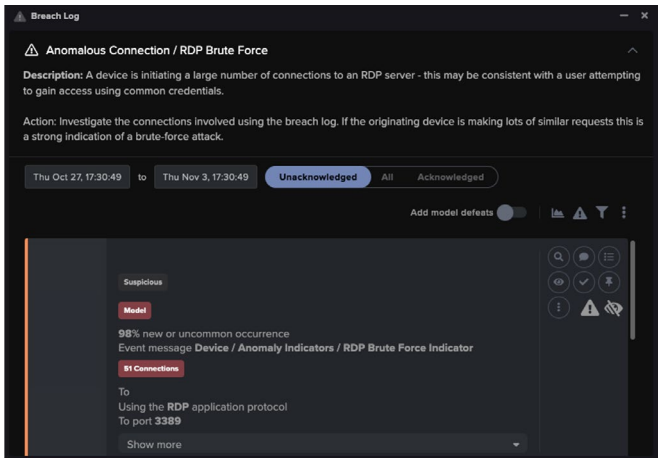

Figure 2: Darktrace DETECT alerting to a threat.