Darktrace Cyber AI: Cloud Misconfigurations

Configuring security controls in hybrid and multi-cloud environments is a complex and overwhelming process, and if not done right, it can easily expose your critical systems and data to compromise. Misconfigurations inevitably occur, whether due to a developer spinning up a cloud instance in minutes and bypassing the security team, or simply because diverse and incompatible security controls often lead to overly relaxed permissions and simple mistakes. As organizations continue to adopt new and unfamiliar cloud services, it's no surprise that almost all successful cloud attacks to date have been the result of critical misconfigurations.

This problem is fundamentally a symptom of a conventional approach to cloud security, one reliant on humans to constantly adjust and monitor a wide range of native and third-party security tools. These tools are static, disjointed, and lack enterprise-wide insight, which often means that gaping misconfigurations can go unnoticed for months.

Cloud misconfigurations introduce the potential for serious data compromise and damage to critical infrastructure, at an unprecedented speed and scale. Yet despite this danger, a majority of organizations still do not have unified visibility over their disparate cloud environments. The blind spots created by cloud misconfigurations can give threat actors easy access to the most valuable parts of a digital ecosystem - and cyber-criminals know this better than anyone.

Figure 1: Darktrace's Threat Visualizer correlating activity across an organization's global cloud, SaaS, industrial, and on-premise digital infrastructure

Darktrace Cyber AI: Total Enterprise Coverage

Artificial intelligence has now emerged as the leading solution for enterprise-wide security coverage, illuminating blind spots in the cloud and beyond. The Darktrace Cyber AI Platform leverages self-learning AI to understand the normal 'patterns of life' for every user, device, and container across hybrid and multi-cloud environments, recognizing the subtle behavioral shifts associated with a misconfiguration without relying on a pre-defined representation of 'good' or 'bad'.

Delivering a fundamentally unique approach in this area, Darktrace Cyber AI analyzes all cloud traffic in connection with wider network activity, enabling it to see that a behavior viewed in isolation in one part of the digital ecosystem may point to a greater picture of malicious activity. It is the only security solution that learns 'on the job', continuously adapting as your business evolves.

Darktrace's complete, real-time visibility and bespoke understanding of normal patterns give organizations the necessary knowledge of complex cloud environments to catch hidden threats due to misconfigurations in their nascent stages — before they escalate into crises.

Case Study 1: Shodan Attack on Cloud Misconfiguration

Darktrace Cyber AI was crucial when a financial services organization faced a breach due to a misconfiguration of firewall settings. The company was hosting several critical applications on virtual machines in the cloud, some of which were meant to be public-facing and some of which were not. When configuring their native cloud controls, they mistakenly left one of these important applications exposed to the Internet, when it was meant to be isolated behind a firewall.

The application and its valuable data could have been left vulnerable because of a quick and chaotic migration, or due to a lack of familiarity with the native controls offered by the Cloud Service Provider. Regardless, their lack of visibility left the security team completely unaware of the critical misconfiguration.

The exposed application was eventually discovered and targeted by cyber-criminals using Shodan, a search engine that catalogs all Internet-connected assets. When the application began receiving an unusual amount of incoming connection attempts from a wide range of rare external sources, Darktrace Cyber AI saw it immediately and alerted the security team to the threat within seconds.

This unusual volume of rare connections might well have been normal for a different company or a different application. However, given Darktrace Cyber AI's bespoke and continuously adapting knowledge of normal 'patterns of life' for the company, it was clear that this behavior was anomalous – the result of a misconfiguration that could have had drastic consequences had Darktrace not detected the attack.

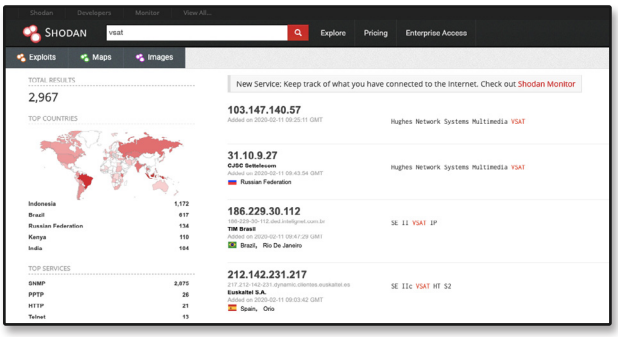

Figure 2: The Shodan website was used for vulnerability scanning

Case Study 2: Crypto Mining Malware Inadvertently Installed

At a multinational organization with a massive digital infrastructure, Darktrace Cyber AI detected an attack that revealed an alarming hole in the company's cloud security configuration – all due to a single mistake made by a junior DevOps engineer.

The junior engineer accidentally downloaded an update that included a cryptocurrency mining malware. After the initial infection, the malware started beaconing out to an external control center, which delivered attack instructions for the malware to spread rapidly across the organization's expansive cloud infrastructure.

The malware moved incredibly fast, infecting 20 of the company's cloud servers in under 15 seconds – but Darktrace Cyber AI moved at machine speed, too. Thanks to Darktrace, the security team was able to contain the attack within minutes, rather than hours or days.

Without Darktrace Cyber AI's ability to provide real-time visibility and control to the entire digital infrastructure, the company could have hosted the crypto miner for months. Instead, the Cyber AI Platform's dynamic and unified view across the organization's sprawling hybrid and multi-cloud infrastructure identified the attack immediately, stopping the threat well before the costs could start to mount.

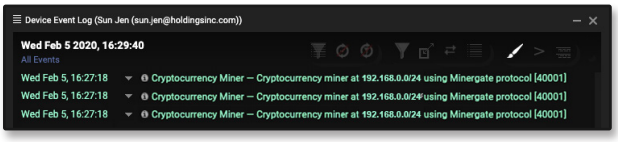

Figure 3: The crypto mining malware detected in real time