Terra

At a Glance

- AI reveals hidden devices on the corporate network
- Surgically neutralizes malicious activity
- Detection and response across the entire network

Terra is one of the largest and oldest companies in Mauritius, providing products and services across the agricultural, food and drink, power, property, and leisure industries. Its popular brands include Grays, a producer of high-quality wines, spirits and liqueurs.

Darktrace Lights Up a Wide-Ranging Business

Terra is a large and multifaceted organization, with a variety of business areas and interests to protect from cyber-threats. The security team relies on Darktrace to not only detect the threats targeting their business, but to neutralize them in seconds with Autonomous Response. Darktrace does this by learning a normal 'pattern of life' for every user and device across Terra's organization and revealing the anomalous activity which indicates an emerging attack, wherever in the digital environment it is striking.

This comprehensive approach to security has made a big difference for Terra's Group IT Manager, Ashwan Seeparsad, and his team, who do still see value in their existing perimeter defenses like firewalls, scanning tools, email security and next generation anti-virus. These tools contribute in addressing the organization's perimeter security, however as attacks are advancing with the utmost sophistication it was critical the team add another layer of autonomous defence to their digital estate using Cyber AI technology.

Adding Darktrace has given the team a deeper level of visibility which now means they can respond quicker to advanced attacks on their organization more quickly, and prevent lateral fast-moving attacks on the network.

Terra tried out numerous tools before deploying Darktrace's AI-driven technologies, and were immediately impressed. Seeparsad recalls, "We expected there were around 400 devices in our network. But then we plugged in Darktrace, and it revealed that there were many more we weren't aware of."

As soon as it had visibility over the digital environment after a very quick POV setup, Darktrace detected a couple of devices on the guest network that were behaving in a highly unusual way. The AI was able to quickly stop this behavior and keep the business moving without disruption or further damage to Terra's brand.

Proactive Security with Autonomous Response

The team at Terra used to feel stretched by the range of their responsibilities, and lost a lot of their time sorting through minor incident alerts and false-positives. Now, Darktrace surfaces the highest priority incidents so that the team can spend its time where it matters most. "The way the Darktrace UI presents us with the information is immediately understandable," Seeparsad says, "It's clear what action, if any, needs to be taken."

Most of the time, no action is required of the team, and they simply review AI-generated reports on threats which have autonomously been stopped by the technology. This is because of Autonomous Response, which addresses threats as they arise, rather than relying on Seeparsad's team to see alerts and take action before damage is done. This not only saves time for the team, but offers a more effective, timely response to fast-moving threats like ransomware. Autonomous Response takes action at machine speed the moment an attack is detected, saving Terra from the costs associated with lengthy remediation efforts.

For Seeparsad, the power of Autonomous Response is most valuable in the precision of its actions. "Before Darktrace, if we suspected something was wrong with a laptop, we would just quarantine it," he recalls. "It was disruptive and it was time consuming." Now, Autonomous Response uses Darktrace's knowledge of Terra's normal business operations to differentiate between malicious and benign activities and take targeted action. This means that a compromised device can continue to conduct its normal activities while the threat is neutralized. "We're moving toward a system where we don't log in to the user interface," Seeparsad says, "we just let Darktrace work completely autonomously and have the Mobile App which alerts us on actions taken."

Protecting Complex Cloud Environments

Having embraced a hybrid cloud environment to better support its growing business, Terra had already adopted platforms like Microsoft 365, Microsoft Azure and Oracle. Seeparsad hopes to make the most of Darktrace's dedicated cloud and SaaS modules, and incorporate these new areas of the digital estate into Darktrace's unified Threat Visualizer very soon. Darktrace analyzes data gathered from cloud platforms and applications alongside activity from across the rest of the digital environment, including network, email, and endpoints, in order to piece together the full story of an attack, whatever the geographic source – even if an employee is traveling internationally. This level of visibility is simply not possible with the tools in place currently.

> "We're moving toward a system where we don't log in to the user interface. We just let Darktrace work autonomously and have the Mobile App which alerts us on actions taken."
>
> Ashwan Seeparsad, Group IT Manager, Terra

> "The way the Darktrace UI presents us with the information is immediately understandable. It's clear what action, if any, needs to be taken."
>
> Ashwan Seeparsad, Group IT Manager, Terra