Sefalana Group

Sefalana Group is Botswana's second largest food retailer, also operating in the manufacturing, motoring, and property industries. Since its founding in 1974, it has expanded to over 86 stores across 3 countries, with a workforce of over 3,400 employees.

At a Glance

- Darktrace AI identified a targeted attack during the trial
- Autonomous Response technology stops threats in seconds
- Security team benefits from additional services from Grove

> "I don't think we could live without Antigena's Autonomous Response."

David Levin, Head of Corporate Services, Sefalana Group

Facing a New Era of Cyber-Threat

Like many organisations in the region, Sefalana Group was being targeted by increasingly sophisticated ransomware threat actors using new tools, techniques and procedures to evade traditional defences. The team already had measures in place to deal with known threats, but with the speed of attacker innovation, needed something which could stop novel and sophisticated attacks.

Sefalana Group decided to trial Darktrace in early 2019, via Grove, the Darktrace partner of the year (2020 & 2021), to see the value of its Self-Learning AI in their own environment. The installation was quick and easy, and immediately the technology began autonomously learning a sense of 'self' for every user and device within the organisation.

During the 30-day Proof of Value, run by Grove and Darktrace together, Sefalana Group was hit by an attempted ransomware attack that targeted the domain controller and moved laterally using TeamViewer. Despite the attacker using legitimate tools that were regularly used by the organisation, Darktrace's AI detected the anomalous nature of this activity, and immediately raised a clear, high-confidence alert. The security team was also contacted by Darktrace's 24/7 SOC, to ensure they were aware of this highly concerning activity.

Darktrace's Cyber AI Analyst launched an automatic investigation, and surfaced the wider context of the incident, including the origin and full scope of the attack. This allowed the Grove and Sefalana Group security teams to quickly dismantle the attack, saving the company from a serious and potentially very costly incident.

Autonomous Response with Darktrace Antigena

The team were so impressed with Darktrace's ability to shed meaningful light on a serious incident undetected by other tools, that they immediately turned on Darktrace Antigena – Darktrace's Autonomous Response technology. Now, when Self-Learning AI detects the early stages of a cyber-threat, Antigena will take targeted action, in seconds, to stop the threat in its tracks, without disrupting the rest of the business.

The team have greatly benefited from this machine-speed response. "Antigena is genius because it literally disrupts the threat in a couple of seconds," commented David Levin, Head of Corporate Services at Sefalana. This speed of response gives the Sefalana team peace of mind that they are protected around the clock from disruptive ransomware and other cyber-attacks – particularly as threat actors deliberately strike at night or on weekends, when they know human response time will be slower.

To test the organisation's cyber security posture, Head of Corporate Services David Levin regularly conducts his own tests, and is relieved to find that Antigena consistently takes action to curtail any threatening activity. "My computer is kicked off the network in seconds," he says. "I don't think we could live without Antigena's Autonomous Response".

When Antigena takes action, the team receive a notification via the Darktrace Mobile App, allowing them oversight of what's taking place in their digital environment, wherever they are in the world.

Cyber Support Services from Grove

The team continues to benefit greatly from additional cyber support services provided by Grove, who have partnered with Sefalana Group to deliver a layer of local support, early indicators of compromise and ask the expert services. These services offer proactive alerts from the Grove cyber security team to help Sefalana Group keep on top of any early indicators of compromise or compliance risks. If there is an incident then Sefalana Group can ask one of Grove's certified Darktrace cyber support engineers to deliver an event log report to help with further investigations.

Sefalana receives daily emails from Grove's cyber support team revealing the major security events that Darktrace's AI has discovered in the past 24 hours and offering continuous best practice advice and threat hunting services for critical incidents flagged by both Darktrace and Grove.

This complements Darktrace's 24/7 SOC services to ensure that at any given point, there are always eyes on the activity occurring within Sefalana Group's digital enterprise, allowing the IT team and executive leadership to have better levels of peace of mind around advanced cyber-threats.

> "Antigena is genius. It literally disrupts cyber-threats in a couple of seconds."
>
> David Levin, Head of Corporate Services,
> Sefalana Group

"Darktrace's ground-breaking approach to cyber security has disrupted the global marketplace and it's been an exciting journey to be part of the process and enjoy such success alongside customers like Sefalana Group," says Johann de Wet, General Manager at Grove. "Our role as a leading Darktrace partner is to help customers like Sefalana Group maximise their investment in mitigating cyber risk and this is where we have focused on building a rich customer experience to complement Darktrace's powerful technology.

"Working alongside the Darktrace teams around the world has been fantastic and it has been great to see how the strong collaborative relationships between us have added significant value in ensuring happy customers. We look forward to continuing this journey with Darktrace as we look to further our investment and to help more organisations like Sefalana Group mitigate the latest cyber-attacks."

The Darktrace Threat Visualizer