EV Group

EV Group is a leading supplier of high-volume production equipment and process solutions for the manufacture of semiconductors, MEMS, compound semiconductors, power devices and nanotechnology devices. It supports an elaborate network of global customers and partners all over the world, with more than 1100 employees worldwide.

At a Glance

- Security team sought packet-level visibility and aimed to reduce time to response
- Trialled Darktrace alongside other technologies and witnessed accuracy of detections first-hand
- Developed a trust in the AI's decision making and implemented Autonomous Response to fight threats around the clock

> "Darktrace is about a year and a half ahead of the pack in terms of the sophistication of the technology."
>
> Josef Buttinger, Corporate IT & Security Manager, EV Group

Packet-Level Insight and AI Detections

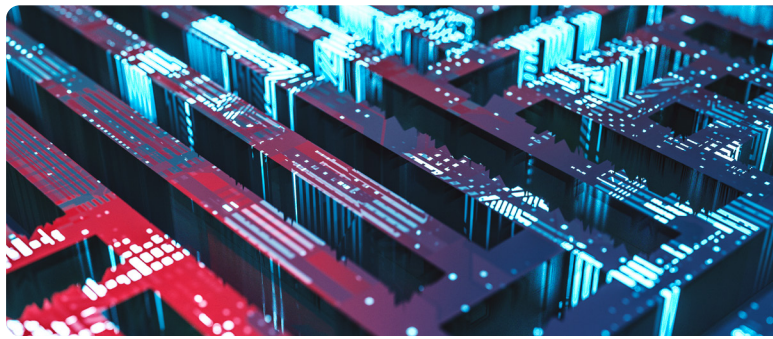
As the digital infrastructure at EV Group became more complex, the team sought to improve their security stature by going beyond the log-based analysis that its existing security tools relied on. Their log-based SIEM technology gave a good overview of the digital estate, but a lack of packet-level insight at the network traffic layer meant that security incidents were not being recognized and controlled fast enough.

"It's not enough just to look at transactions; a deeper understanding of the communications between devices is necessary," commented Josef Buttinger, Corporate IT & Security Manager at EV Group. "With log-based tools, by the time we see that there is a significant security incident, it's too late – it's already happened."

The primary aim was to minimize the time between an event happening and it being acknowledged. "In an ideal world, this time to response would be less than 10 minutes," said Buttinger.

The team therefore trialled Darktrace in a side-by-side bake-off with other tools, deciding on Darktrace's Self-Learning AI primarily because of the accuracy of its detections. "Darktrace doesn't swamp you with benign alerts because it knows 'normal'," says Buttinger, referring to the AI's ability to learn the 'patterns of life' for every user and device in the organization and spot subtle deviations indicative of a threat. "It is far more advanced; about a year and a half ahead of the pack in terms of the sophistication of the technology."

Darktrace shone a light on the organization's digital estate, revealing a host of issues that the team were not previously aware of. "With Darktrace you are able to see all of the configuration errors that could represent a backdoor into our digital estate. I mean all of them. Every event is interesting, but some events are particularly interesting for us when proactively identifying any vulnerabilities," commented Buttinger. The technology has helped the security team become more strategic in cleaning up their digital infrastructure and ensuring more robust security in the long term.



The Day-to-Day Use of Darktrace

Darktrace is the principle go-to technology for the security team at EV Group. They set the technology to surface only the events that have occurred in the last 24 hours, and every anomaly is looked at to ensure that the Darktrace dashboard is clean at the end of every day.

"If Darktrace thinks that an event is something worth looking at, we have to assess it. That is our level of confidence in the AI technology," says Buttinger. Darktrace's alerts are clear and precise, and the AI self-prioritizes security events according to urgency. This means the security team stay proactive and motivated. "If you look at the same thing every day, if you don't clear the noise, you see the same noise every day".

> "Autonomous Response is the crown jewels of information security. It can trigger a broad range of actions; each targeted according to the nature of the threat."
>
> **Josef Buttinger, Corporate IT & Security Manager, EV Group**

Extending to Autonomous Response

Whilst EV Group is working towards having operational security 24/7 – for now, with a security team comprising of five people, they are unable to keep a permanent overwatch around the clock. And with threat actors often striking at nights or on weekends, it was necessary to add autonomous response to the security stack, to take targeted and proportionate action against threats, whenever they come in.

Darktrace's Autonomous Response is powered by Self-Learning AI that learns the digital estate – every user and every device, analyzing hundreds of signals and applying advanced AI to surface only anomalies that exceed a certain threshold.

"Autonomous Response is the crown jewels of information security," says Buttinger, "It can trigger a broad range of actions; each targeted according to the nature of the threat, safeguarding the confidentiality, integrity, and availability of systems. Our confidence in the technology is so high that when an Antigena model is breaches, we know it really is something bad."

Antigena is synced up with the security team's existing alarm system, which wakes team members in the middle of the night in the case of a serious incident, with text-to-speech alerts. This ensures the team is able to rapidly respond to emerging cyber-threats, regardless of when they occur.

EV Group recognizes the power of Darktrace's technology as a practical application of artificial intelligence to solve real-world, day-to-day challenges. Buttinger commented: "AI is a term that has suffered a lot of inflation, but I truly believe Darktrace is real AI. The system really trains itself, I never have to interact with any of the models. The system is astonishingly accurate."

The group is now trialling Autonomous Response in its email environment to protect its employees from sophisticated phishing attacks.

> "Darktrace is real AI. The system really trains itself, I never have to interact with any of the models. The system is astonishingly accurate."
>
> **Josef Buttinger, Corporate IT & Security Manager, EV Group**

For More Information

- Book a free trial
- Read the Blog
- Visit our YouTube channel