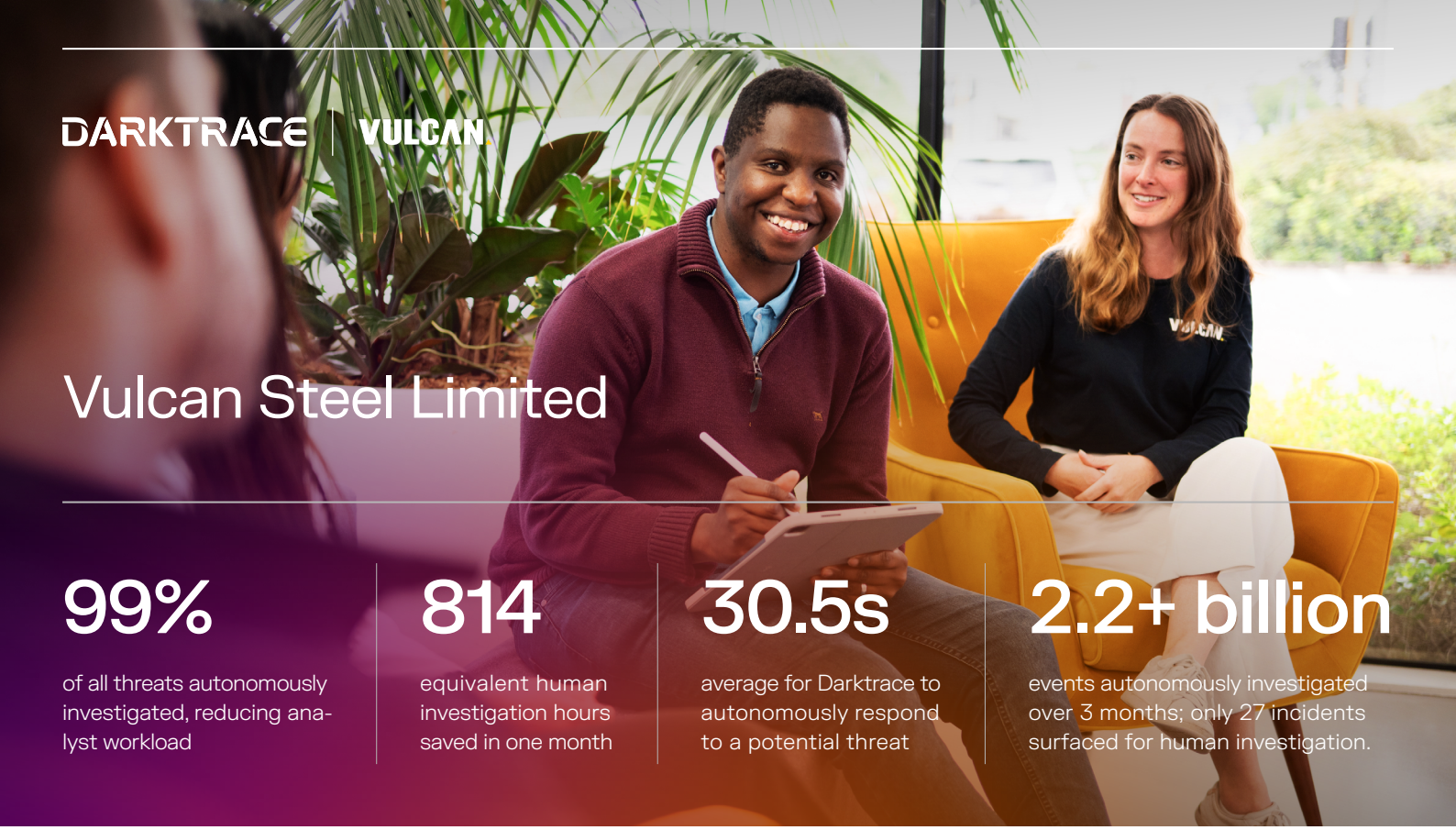

Vulcan Steel Limited

99%

of all threats autonomously investigated, reducing analyst workload

814

equivalent human investigation hours saved in one month

30.5s

average for Darktrace to autonomously respond to a potential threat

2.2+ billion

events autonomously investigated over 3 months; only 27 incidents surfaced for human investigation.

Founded in 1995, Vulcan is a leading distributor and processor of steel and aluminum, including roofing and roll forming, across Australia and New Zealand.

Operating numerous sites across both countries, the company supplies carbon steel, stainless steel, engineering steel, and aluminum products to industries including engineering, construction, manufacturing, agriculture, and mining.

"We take pride in delivering customer orders in full on time. Customers reward us for our high service level. **Disruption minimization is key.**"

■ **Bob Kombora, Head of IT Operations and Cyber**
Vulcan

Securing a rapidly expanding and distributed business

With a reputation built on trust and reliability, Vulcan accelerated its growth and market presence through a combination of organic expansion and strategic acquisitions. Operating seven business divisions and **82 facilities across Australia and New Zealand,** Vulcan has made securing its distributed footprint a top priority. But with rapid growth came complexity, and with complexity came increased risk. Striking a balance between protecting the business and ensuring operational resilience grew more difficult.

Inherited complexity creates visibility gaps

Over the years, the company absorbed multiple businesses, each bringing its own systems, network architectures, and security postures. With numerous divisions operating across different locations and functions, the IT team had lacked full visibility across the network.

Protecting operations where downtime isn't an option

Vulcan's processing plants leverage operational technology (OT) A cyber-attack could have significant downstream consequences, affecting customers. With only a handful of competitors in the market, an OT breach could create unnecessary disruption to its customers.

AI-driven security designed for complex IT and OT environments

In an environment of rising threats and more advanced attacks, like most companies, Vulcan was seeking to enhance its security through a solution that could:

Autonomously detect and respond to threats at scale

Deliver **real-time** insights to security analysts

Integrate with the company's existing Microsoft investment rather than replace it

Deliver OT **visibility and protection** without the enormous cost and disruption of re-architecting an entire industrial environment

After evaluating several options, Vulcan deployed Darktrace / NETWORK™ and Darktrace / EMAIL™ to enhance prevention, detection, and response to both known and emerging threats across its network and email environments.

The deployment complemented Vulcan's existing security stack, creating a layered defense model with broader visibility and coverage.

Self-Learning AI a key differentiator

Vulcan was particularly impressed by Darktrace's Self-Learning AI, an AI-native technology that continuously learns the unique patterns of behavior of users, devices, applications, and systems across the organization. Unlike other solutions that rely on known threats and signatures, Darktrace Self-Learning AI continually analyzes Vulcan's unique environment to understand what "normal" behavior looks like across users, devices, systems, and more.

When Darktrace detects subtle deviations and anomalous activity, **it stops threats in their tracks**, providing rich behavioral context that helps security teams prioritize risks and make more informed decisions.

Proven OT expertise

Another key decision factor was Darktrace's track record of success in OT security and its ability to deploy across a complex, mixed IT/OT environment without requiring a full architectural overhaul.

Across Vulcan's distributed operations, the convergence of business systems, cloud applications, remote access technologies, and production environments means that vulnerabilities originating in IT can quickly propagate into OT systems, creating risks that can directly impact production availability, operational continuity, and uptime.

With Darktrace, Vulcan gains a **unified view across both IT and OT environments**, helping teams identify potential issues earlier and respond before they can disrupt critical operations.

"The Darktrace engineers were very knowledgeable; It definitely wasn't their first rodeo. We felt like we were guided along on the journey while also being empowered. **They worked alongside us like a partner.**"

- **Brendon Satram, Infrastructure Lead**
  Vulcan

A trusted, hands-on partner committed to success

From evaluation, to deployment, to production, to support, Darktrace has partnered with Vulcan each step of the way to ensure its success. To secure the complex, hybrid infrastructure that included a virtual environment, Microsoft Azure footprint, and assets, Darktrace engineers collaborated with Vulcan to create a detailed and tailored deployment plan.

That collaborative spirit extended to going live. Satram admits he was nervous about flipping the switch to fully autonomous response.

The possibility of a false positive taking down a production line was the nightmare scenario. To help address concerns specific to Vulcan's environment and operational requirements, Darktrace worked closely with the team to build confidence ahead of deployment. "When Autonomous Response did go live, no legitimate processes were blocked. It was very, very smooth," he says. "Since that day, it's been running like a well-oiled machine."

To accelerate the team's capabilities during the first year, Darktrace provided access to its managed detection and response team, giving Vulcan an extension of expert support **while the team grew more confident with the technology.**

Then came a test nobody planned for. Vulcan ran an unannounced cyber drill; no vendors were told. Darktrace spotted the alert and immediately mobilized a response team. "I felt bad when we told our Darktrace account manager it was a drill," Kombora laughs. "But he understood; that responsiveness is important."

Modern cybersecurity delivers speed, scale, and resilience

Security at machine speed

Using Darktrace, Vulcan has significantly strengthened and scaled its cyber defense operations while enabling the IT team to focus on more strategic, proactive initiatives. Central to this transformation is Darktrace's Cyber AI Analyst™, an AI-powered investigation capability that autonomously conducts end-to-end investigations across thousands of anomalous and high-risk events, surfacing the incidents most likely to impact the business.

Combined with Darktrace Autonomous Response, the technology has accelerated threat detection and mitigation while helping reduce operational strain on the security team. "Cyber AI Analyst is exceptionally effective at identifying threats," says Kombora. "It takes a significant burden off our engineers by reducing the volume of incidents they need to manually investigate. That means less fatigue, less noise, and more time focused on what truly matters."

The numbers tell a striking story:

Over a three-month period, Darktrace autonomously investigated more than 2.2 billion events, **containing suspicious incidents within just 30.5 seconds, on average.**

Of those billions of events, Darktrace **surfaced just 27 critical threats to analysts for further investigation.**

Within a single month, Darktrace delivered the equivalent of **814 hours of investigative capacity,** allowing the IT team to dedicate more attention to proactive threat hunting and strategic priorities.

Phishing-related incidents have all but been eliminated. "There's literally a graph where it just dropped off when we turned Darktrace on," says Kombora.

Maximizing ROI of Microsoft investment

Because Vulcan's ecosystem sits inside Microsoft, the organization sought an integrated solution that could optimize that investment while providing clearer and expanded telemetry.

/ NETWORK

Is **deeply integrated** with Vulcan's security stack and other tooling to create a seamless NDR-EDR visibility continuum.

/ EMAIL

Enhances detection sensitivity and expands the threat detection spectrum of Defender for Office 365, improving overall resilience to known and unknown email attacks.

"It feels like we have two teams working for us all the time," says Satram. The combined, complementary AI approaches establish a cybersecurity environment that is complete, continuous, and contextual.

A security posture that enables the business

Because their industry is very traditional, Kombora acknowledges people worry AI is going to get it wrong, create false positives, and bring chaos to their operations.

"My experience with Darktrace has been the complete opposite," he shares. "Since we began running Darktrace in autonomous mode three years ago, it has never had a false positive blocking a legitimate process. Not once. It just works. And I think that's a testament to the capability."

That invisible, frictionless protection is precisely what Vulcan was looking for, says Satram. "We believe cybersecurity should be an enabler. Ideally, people shouldn't even know it's there." He encourages others in his industry to embrace change. "The technology landscape has shifted; the traditional way of doing things isn't going to cut it. Using the right AI can deliver incredible efficiencies and advantages to the business."

Securing the future of AI with AI

Vulcan is an ambitious company, committed to continuous innovation. The company regularly reviews its infrastructure and emerging technologies to ensure it's using the latest and best solutions to stay ahead of evolving threats.

That posture will matter more than ever as AI reshapes the threat landscape. The team is already thinking carefully about what AI means for the attack surface:

- Phishing emails written by AI are indistinguishable from genuine communication.
- Deep fakes raise new questions about identity verification.
- Greater adoption of AI-powered tools across business functions will continue to expand risk exposure
- The democratization of software development, where every employee now has access to AI coding tools, is creating new governance challenges.

Kombora says, "The questions we have to ask ourselves are, 'How do I protect that? How do I give people access to those tools but securely?'" The answer is the same philosophy Vulcan has always applied: enable people with the right guardrails, rather than restrict them with rules that don't make sense. "We needed to secure the edge; then we enabled it. I think the same thing will happen with AI."

As an early adopter of AI for cybersecurity, Vulcan is already leading the industry when it comes to balancing a modern defense with operational resilience. In a recent discussion about preparing for AI, Kombora was asked how he planned to secure further AI adoption and defend against evolving AI-powered attacks. **The answer was simple:**

"We're already doing that with Darktrace."

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com