CYDEF secures its first patent for its unique approach to Managed Detection and Response (MDR)

CYDEF's SMART-Monitor technology earns the first of several patents filed in the US.

OTTAWA, ONTARIO, CANADA, November 10, 2022 / EINPresswire.com/ -- CYDEF is pleased to announce that US Patent no. 11489851 for our managed detection and response (MDR) technology, SMART-Monitor, was approved by the US Patent Office on November 1, 2022.

> We didn't want to create something only to be marginally better. We genuinely wanted to find a better way to keep businesses safe."
>
> *Tiago de Jesus, PhD, co-founder and Chief Innovation Officer at CYDEF*

This is the first of several US patents filed by the Canadian cybersecurity company. The patent is related to the meshed network of sensors used in the monitoring process.

This patent validates the innovation CYDEF has brought to the market, which not only vastly improves upon traditional MDR outcomes, but also provides a defense in depth cybersecurity solution that is attainable for all – from small- and medium-sized businesses to enterprises and critical infrastructure.

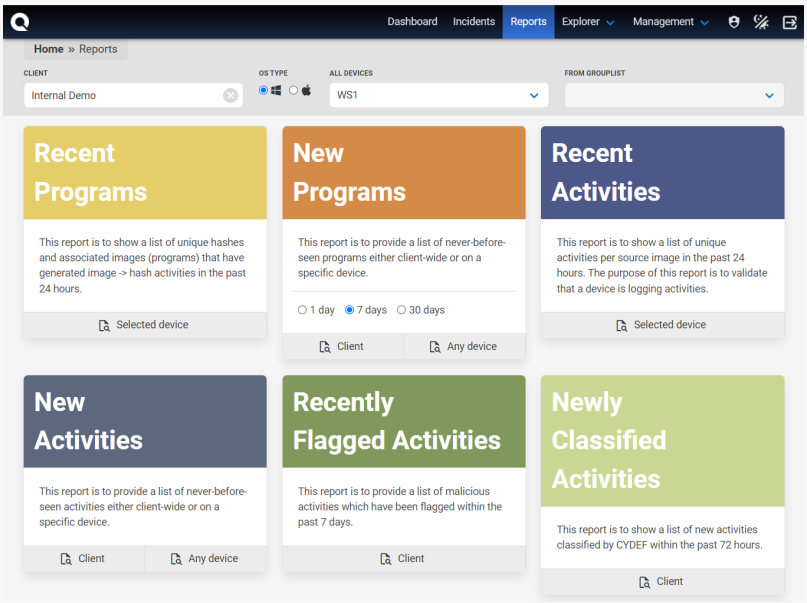
CYDEF's founders were frustrated with the inability of existing solutions to prevent cyber attacks from succeeding. They felt too much trust had been put on artificial intelligence (AI) and automation.

"We didn't want to create something only to be marginally better," said Tiago de Jesus, co-founder and Chief Innovation Officer at CYDEF. "We genuinely wanted to find a better way to keep businesses safe."

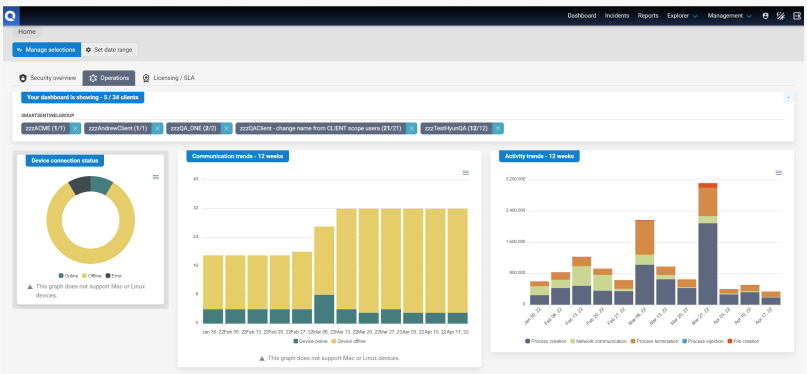
Our founders recognized the industry was lacking in the area of threat hunting.

Threat hunting is a human-led, proactive approach to identifying unknown threats (new attacks that haven't been seen before). According to IBM, automated cybersecurity solutions stop approximately 80% of threats. For more sophisticated attacks, they say, threat hunting is required.

"One of the main problems we needed to solve was how to make threat hunting faster and more efficient – and therefore, more affordable – without sacrificing quality," said de Jesus. "The solution was beautiful in its simplicity."



Cyber threat detection reports dashboard - CYDEF SMART-Monitor



Cyber threat detection dashboard - CYDEF SMART-Monitor

"We realized we needed to look at the data differently. Instead of searching for what might be malicious, we decided to focus on classifying acceptable behaviors. Once you eliminate what is acceptable, or 'good', everything left over is a potential threat and must be investigated."

CYDEF's machine learning technology maintains an allow list of behaviors that are acceptable in a business environment. For example, when a user clicks a PDF file, Adobe Reader opens that PDF document – that's expected. CYDEF isn't reading the document, but rather, monitoring the processes running in the background.

This list of 'good' activities (or, application and process behavioral analytics) is much shorter and easier to maintain than the infinite list of potential malicious activities and vulnerabilities.

"As our baseline matures, anomalous activity stands out more," said Michael Noory, Senior Threat Hunter at CYDEF. "Using this process-driven method, we're not only finding things like ransomware precursors, living-off-the-land attacks, and corporate espionage, but also PUPs and policy violations such as video games. The more we find, the more our customers improve their cybersecurity posture. Everybody wins."

This combination of people, process, and technology ensures that 100% of telemetry is reviewed

by humans – an unprecedented accomplishment in the cybersecurity world.

The solution is so effective, that after only three years in operation, one CYDEF threat hunter can perform approximately five times the work of a traditional SOC analyst. And that number is getting bigger.

“It took just over a year to develop the technology and then another year or so of beta testing before we officially launched. Product updates are now all about the user experience for customers and staff,” explained Mark Levine, CYDEF’s Chief Product Officer and Technology Officer. “We’ve stopped doing major releases and have moved to a bi-weekly continuous improvement cycle. The product works and it scales extremely well.”

“The global IT staffing shortage impactours us less because our tech is specifically built to make a threat hunter’s job easier and more efficient. The process is repeatable and teachable, which is even more impactful for our partners looking to boost their local economies rather than outsourcing tech jobs,” said Elana Graham, CYDEF’s Chief Operating Officer and co-founder. “And unlike our competitors, as we scale, our threat hunting solution becomes more efficient, not less. One day, we expect our analysts to perform the work of 10 or 20 traditional SOC analysts.”

“We enable IT companies to break into the cybersecurity market,” said Ameen Sait, Chief Revenue Officer at CYDEF. “Partners can move away from a break/fix model to a subscription-based model, without any up-front costs or additional resources. We now have partners, including three distributors, selling our solution in ten countries on five continents.”

CYDEF addresses yet another major problem: Reverse engineering of security software.

A common method criminals use to bypass cybersecurity software involves signing up for product demos, downloading the security software to an isolated computer, then disconnecting the internet while they figure out how to bypass it. Once they succeed, they launch an attack – often working together in cyber crime rings to maximize the damage.

CYDEF’s solution differs because the software installed on endpoints (computers, desktops, and laptops) serves only to collect the data. Processing is done in the cloud. If a device is offline for any period, the telemetry is collected and held in a queue. Once a device re-connects, the telemetry is shipped to our Azure servers and gets investigated as usual.

“There is a serious lack of transparency in cyber,” said Steve Rainville, Chief Executive Officer at CYDEF. “We’ve heard for years that cybersecurity companies are ‘selling smoke and mirrors.’ But providers can’t compete if they share too much about their proprietary technology, which would also expose them to further attacks. They keep closely guarded secrets to stay in business. Cyber criminals don’t have that problem, so they work together, joining forces and sharing critical information among themselves.”

“When I learned about CYDEF’s approach, I knew I wanted to be involved. This patent is one more stamp of approval, confirming what we already know,” added Rainville. “It’s a game-changer.”

About CYDEF
CYDEF revolutionized cybersecurity with a “threat hunting first” approach to detection and response. The result is a managed, zero trust solution that’s simple, transparent, affordable, and scalable – it gets more efficient as we grow.

Proudly Canadian and dedicated providing clarity into cyber health because everyone should feel safe to do business online. Visit us at https://cydef.ca/.

Elana Graham, COO
CYDEF
info@cydef.ca
Visit us on social media:
LinkedIn
