EINPRESSWIRE

CYDEF Revolutionizes Threat Detection with AI-Powered 'Known Good' Intelligence

Ottawa-based cybersecurity pioneer's patented technology investigates 100% of anomalous activity, ensuring no threats slip through EDR/SIEM systems.

CYDEF Logo

OTTAWA, ON, CANADA, July 28, 2025 /EINPresswire.com/ -- CYDEF, a leading Canadian cybersecurity innovator, today announced how its groundbreaking Behavioral Threat Detection and Response (BTDR) platform is transforming enterprise security by directly addressing the industry's most critical blind spot: false negatives. While traditional security solutions focus on identifying "bad" behavior, CYDEF's patented approach leverages artificial intelligence to establish comprehensive baselines of "known good" activity, ensuring that every unclassified action receives human-verified investigation.

> Our technology ensures that nothing slips through the cracks by investigating every single anomaly that doesn't match our AI-built baseline of known good behavior.”
>
> *Martin Shepherd, CEO of CYDEF*

The False Negative Crisis
While the cybersecurity industry has long focused on reducing false positives—the 95% of alerts that waste analyst time—the more dangerous challenge lies in false negatives: the real threats that go undetected. These missed detections can result in extended dwell times, lateral movement, and catastrophic breaches that traditional EDR and SIEM solutions simply cannot catch.

"The industry has been solving the wrong problem," said Martin Shepherd, CEO of CYDEF, who brings 20 years of executive cybersecurity leadership to the company. "While everyone focuses on alert fatigue from false positives, the real danger is what you're not seeing. Our technology ensures that nothing slips through the cracks by investigating every single anomaly that doesn't match our AI-built baseline of known good behavior."

Revolutionary "Known Good" Intelligence
CYDEF's proprietary Stack View technology, protected by three U.S. patents with additional patents pending, fundamentally reimagines threat detection:

* AI-Powered Baseline Creation: Machine learning algorithms continuously build and refine comprehensive profiles of legitimate user and system behavior
* 100% Anomaly Investigation: Every activity that falls outside the "known good" baseline receives human-verified analysis
* Zero Trust Validation: Systematic review of all endpoint activities ensures no malicious behavior is overlooked
* Deterministic Detection: Explainable results without black-box AI uncertainty

This approach enables CYDEF to maintain over 51 million threat classifications while allowing a single threat hunter to monitor more than 15,000 endpoints simultaneously—a scale impossible with traditional detection methods.

Validation for Existing Security Infrastructure

Beyond primary threat detection, CYDEF serves as a critical validation layer for existing security investments. The platform can:
* Confirm EDR/SIEM Effectiveness: Verify whether current security tools are properly tuned and functioning as intended
* Identify Coverage Gaps: Reveal blind spots in existing security architectures
* Provide Incident Verification: Offer independent confirmation of security events and responses
* Support Forensic Analysis: Deliver detailed behavioral context for post-incident investigation

Proven Enterprise Performance

CYDEF's approach delivers measurable results across diverse industries including banking, healthcare, insurance, manufacturing, retail, and education:
* Mean Time to Detect (MTTD) <8 Hours: Rapid identification and response to genuine threats
* 98% Customer Retention Rate: Sustained value delivery across client base
* 99% Customer Satisfaction: High-quality service and results
* SOC 2 Type 2 Attestation: Enterprise-grade security and compliance standards

Canadian Innovation, Global Impact

As a proudly Canadian technology company, CYDEF exemplifies the nation's growing prominence in cybersecurity innovation. Operating across 10 countries and five continents, the Ottawa-headquartered company combines Canadian ingenuity with global expertise, backed by a leadership team including former Royal Canadian Navy Combat Systems Engineering Officer Elana Graham (COO) and technology innovation expert Mark Levine (Chief Product and Technology Officer).

"CYDEF represents the best of Canadian technology innovation," said Graham. "We're solving global cybersecurity challenges with distinctly Canadian values: thoroughness, reliability, and an unwavering commitment to protecting our clients' digital assets."

Addressing Modern Threat Landscapes

As cyber attackers increasingly leverage legitimate tools like PowerShell and WinRAR to evade traditional detection methods, CYDEF's behavioral analysis becomes even more critical. The platform's ability to identify subtle deviations from normal behavior patterns enables detection of advanced persistent threats, zero-day exploits, and sophisticated lateral movement that conventional signature-based and scoring-model systems routinely miss.

About CYDEF
Founded in Ottawa, Canada, CYDEF is revolutionizing endpoint security through its innovative Behavioral Threat Detection and Response platform. The company's patented Stack View technology eliminates traditional threat scoring models in favor of comprehensive human-verified threat classification, creating a continuously learning, adaptive security ecosystem. With active operations in 10 countries across five continents, CYDEF serves enterprises across banking, healthcare, insurance, manufacturing, retail, and education sectors.

For more information about CYDEF's breakthrough cybersecurity solutions, visit cydef.io.

CYDEF Media Relations
CYDEF
+ +13439445098
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
