CYBER THREAT INTELLIGENCE (CTI) + THREAT HUNTING:

TURBO-CHARGING INNOVATION AND SETTING A NEW STANDARD FOR INTELLIGENCE-DRIVEN SECURITY

Combined solution disrupts the market, fuses together critical capabilities, and delivers unmatched value

Our customers have grown to rely upon Intel 471's expertise to unlock the power of cyber threat intelligence (CTI). Our recent acquisition of Cyborg Security (now Intel 471 Threat Hunt Intelligence) turbo-charges our customers' ability to operationalize CTI using advanced behavioral threat hunting packages to proactively hunt for stealthy threats within their environment — threats that often go undetected by traditional security tools, but can be identified and removed before greater damage is done. Customers can benefit from expertly crafted behavioral threat hunt packages available on the 471HUNTER Platform to improve their hunt team's efficiency, stay ahead of advanced threats, and continually improve security posture.

BENEFITS:

The Intel 471 solution fuses "best-in-class" threat hunting with industry-leading cyber threat intelligence (CTI) to help your organization stay ahead of threats, reduce cyber risk, and to:

- **Operationalize CTI with intelligence-driven behavioral threat hunting**
- **Map emerging threats to your attack surface**
- **Streamline hunt processes, and improve hunt efficiency and accuracy**
- **Close gaps in telemetry and logging to improve visibility and security posture**
- **Use proper threat hunt metrics to measure success**
- **Identify advanced threats that go undetected by IoC-based detection.**

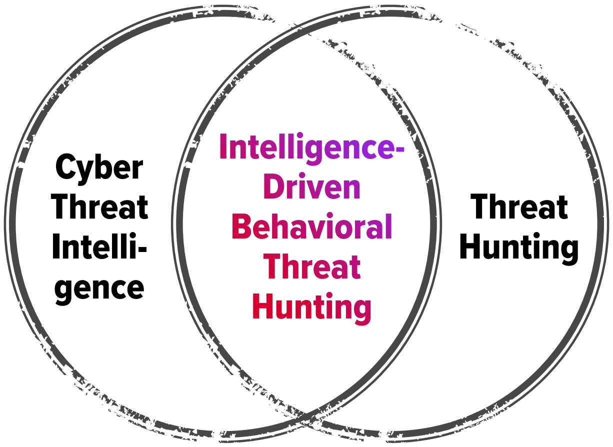
How CTI-driven threat hunting changes the game

In recent years, forward-thinking organizations have strategically aligned the goals of CTI programs and threat hunting operations. CTI helps organizations map the threat landscape to their organization's assets and continuously monitor emerging threats, active malware campaigns, and exposures that matter to them, such as compromised credentials and weaponized vulnerabilities. Threat hunting can then focus on identifying threats in their environment in a more informed manner based on CTI data. CTI-driven threat hunting enhances the relevance and accuracy of hunts, and when combined with adversarial emulations, helps Security Operations be more proactive.

With our leadership in human-led CTI, Intel 471 is now uniquely equipped to help customers adopt a behavioral approach to threat hunting underpinned by adversary behaviors and their evolving tools, and tactics, techniques, and procedures (TTPs). The Intel 471 Threat Hunt Intelligence team helped pioneer behavioral threat hunt queries to uncover stealthy, malicious activity in security log data. This is one reason why Intel 471 sets the standard for intelligence-driven threat hunting, which helps organizations to adopt complementary use cases with integrated CTI and threat hunting practices. Intel 471 Threat Hunt Intelligence and the 471HUNTER platform help customers perform more accurate and efficient hunts and provide proper operational success metrics that demonstrate ROI on a threat hunt program.

The threat landscape is vast but intelligence-driven threat hunting can narrow the internal search. Intel 471's unmatched CTI data contextualization and analysis of adversary TTPs and behaviors help threat hunters to narrow the search for artifacts and behaviors of malicious activity within an organization. Why is this important? Threat actors invest significant time and energy into developing TTPs that cannot be easily changed once discovered, unlike indicators of compromise (IoCs) relied on by traditional security systems. To find how to supercharge your security with best-in-class, intelligence-driven behavioral threat hunting, check out our new white paper.

How does Intel 471 CTI and Threat Hunt Intelligence improve your security?


Cyber Threat Intelligence
Intelligence-Driven Behavioral Threat Hunting
Threat Hunting

Intel 471 brings its human-driven, machine-enhanced approach to the creation of advanced, intelligence-based behavioral threat hunting packages. Unlike solutions from other vendors, 471HUNTER threat hunt packages are built on the CTI data that Intel 471's renowned global team of cyber intelligence experts collect, contextualize, and process into operational insights.

The 471HUNTER platform provides operational success metrics that demonstrate the

ROI on a threat hunt program. Intel 471's CTI also empowers threat hunters with insights into the mindset of a ransomware operator, and their tools and procedures, which can help determine the actor's primary objectives, such as gaining persistent access or laterally moving through an environment.

For customers, this means having up-to-date queries customized for their security tools, including over a dozen different SIEM and EDR platforms supported by Intel 471. This capability goes far beyond IoC monitoring to detect specific threat actor TTPs in a single platform. It also enables threat hunters to launch hunts across many platforms within hours, not weeks or months.

471HUNTER uniquely provides emulation and validation packages that customers can download and safely detonate inside their environment to see the effects of the attack immediately and validate that their security tools are properly configured. This helps security teams reduce their attack surface by closing visibility gaps in security logging and telemetry, and continuously improve security posture. Additionally, and unlike competitors, our hunt content is based on exhibited advanced adversary behaviors and TTPs, not a specific threat. This methodology offers significant benefits, allowing hunt teams to run queries to detect behaviors and TTPs adopted by multiple adversaries, supported by detailed tagging to help in threat actor attribution. This is true advanced behavioral threat hunting.

Customers also leverage Intel 471's strategic, operational, and tactical CTI to support the different cyber risk management objectives of key stakeholders, including senior management, security operations, incident response, forensics, and legal and risk management. The 471HUNTER platform provides this contextual stakeholder-focused reporting that demonstrates how each hunt package and associated hunts help reduce organizational risk.

The Difference: Intelligence-Driven Security Solutions to Reduce Cyber Risk

Intel 471's CTI and intelligence-driven security solutions help organizations reduce cyber risk. Intel 471's market leading intelligence-driven security solutions are powered by our unmatched human-led intelligence capabilities spanning the whole digital threat environment, including cybercrime, state-based threats, hacktivism, and geopolitical events that impact the threat landscape.

Our key intelligence domains include:

- Adversary Intelligence
- Threat Hunt Intelligence
- Malware Intelligence
- Vulnerability Intelligence
- Attack Surface Intelligence
- Identity Intelligence
- Cyber Geopolitical Intelligence
- Fraud & Abuse Intelligence

In the CTI competitive landscape, our "boots on the ground" model with native-language cyber intelligence operators in regions where adversaries operate provides unmatched access to the cyber underground, where we have established long-standing and active presences in highly-guarded, exclusive channels where adversaries communicate, collaborate, and plan. Our human-driven research and intelligence operations are enhanced with automated intelligence collection and unparalleled analytics on adversaries and their tooling and malware. Intel 471 develops General Intelligence Requirements (GIRs) to classify malicious activity, adversary behaviors, and TTPs. This provides a framework for collection efforts and informs behavioral threat hunt content packs developed by Intel 471 Threat Hunt Intelligence.

FROST & SULLIVAN

> *Intel 471 enables organizations to rapidly deploy intelligence-driven threat hunting and detection, furthering its customers' ability to operationalize CTI using advanced behavioral threat hunting packages to proactively hunt for stealthy threats within their environment — threats that go undetected by traditional tools but can be identified and removed before greater damage is done.*
>
> *— Enabling Technology Leadership Award, 2024*

About Intel 471

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using the real-time insights about adversaries, their relationships, threat patterns, and imminent attacks relevant to their businesses. The company's platform collects, interprets, structures, and validates human-led, automation-enhanced intelligence, which fuels our external attack surface and advanced behavioral threat hunting solutions. Customers utilize this operationalized intelligence to drive a proactive response to neutralize threats and mitigate risk. Organizations across the globe leverage Intel 471's world-class intelligence, our trusted practitioner engagement and enablement, and globally-dispersed ground expertise as their frontline guardian against the ever-evolving landscape of cyber threats to fight the adversary — and win. Learn more at www.intel471.com.

Our customers' eyes and ears outside the wire.