



HUNTER471 OVERVIEW

Hunt faster. Stop cyber threats in their tracks.

Empowering Intelligence-Driven Threat Hunting Across Your Security Platforms

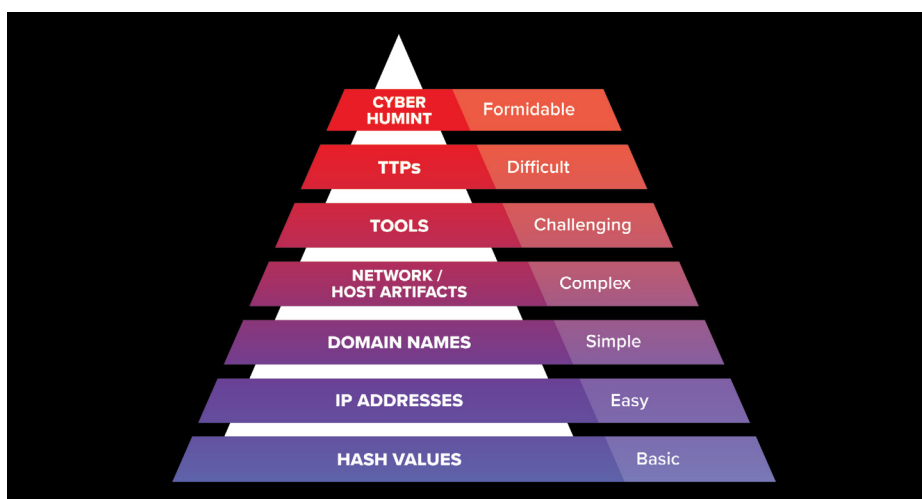
In a world where new threats can be weaponized and deployed within hours, it's vital that threat hunters have the right tools and content to rapidly investigate, identify, and remove stealthy threats before they manifest into a more serious incident.

The HUNTER471 platform hosts nearly 700 (continually updated) Hunt Packages with pre-validated queries that help your teams launch expert behavioral hunts within minutes across 13 fully supported EDR, XDR, NDR, and SIEM platforms, with more being added on a near-weekly basis.

All HUNTER471 queries written by Intel 471's world-class Threat Hunt Intelligence team focus on adversary tactics, techniques, and procedures (TTPs) to help your security teams expertly scale the Pyramid of Pain (see next page) and identify methods known to beat detections for Indicators of Compromise (IoCs). The content is based on identifiable behaviors that are verified to be used in attacks that bypass detections.

Intel 471's unique strength in cyber human intelligence (HUMINT) collection helps your teams reach even higher in the Pyramid of Pain, enabling earlier and deeper insights into adversary tradecraft that are not available with OSINT and generic CTI feeds. Cyber HUMINT depends on relationships, often nurtured over years, with well-placed human sources who can provide exclusive and novel insights about adversary motives, plans, tactics, and tools.

Intel 471's cyber analyst-validated automated collection fuels HUNTER471 Hunt Packages and are mapped to the MITRE ATT&CK framework, enabling intelligence-driven threat hunting with greater speed, precision, and frequency to reduce risk.



Behaviors and TTPs are the hardest for adversaries to change

HUNTER471 Validation Packages

HUNTER471 validation packages help security teams test what techniques each package finds or does not find using the lightweight open-source Atomic Red Team format. Validation packages allow teams to “trust but verify” our pre-validated packages in their environment. With them teams can:

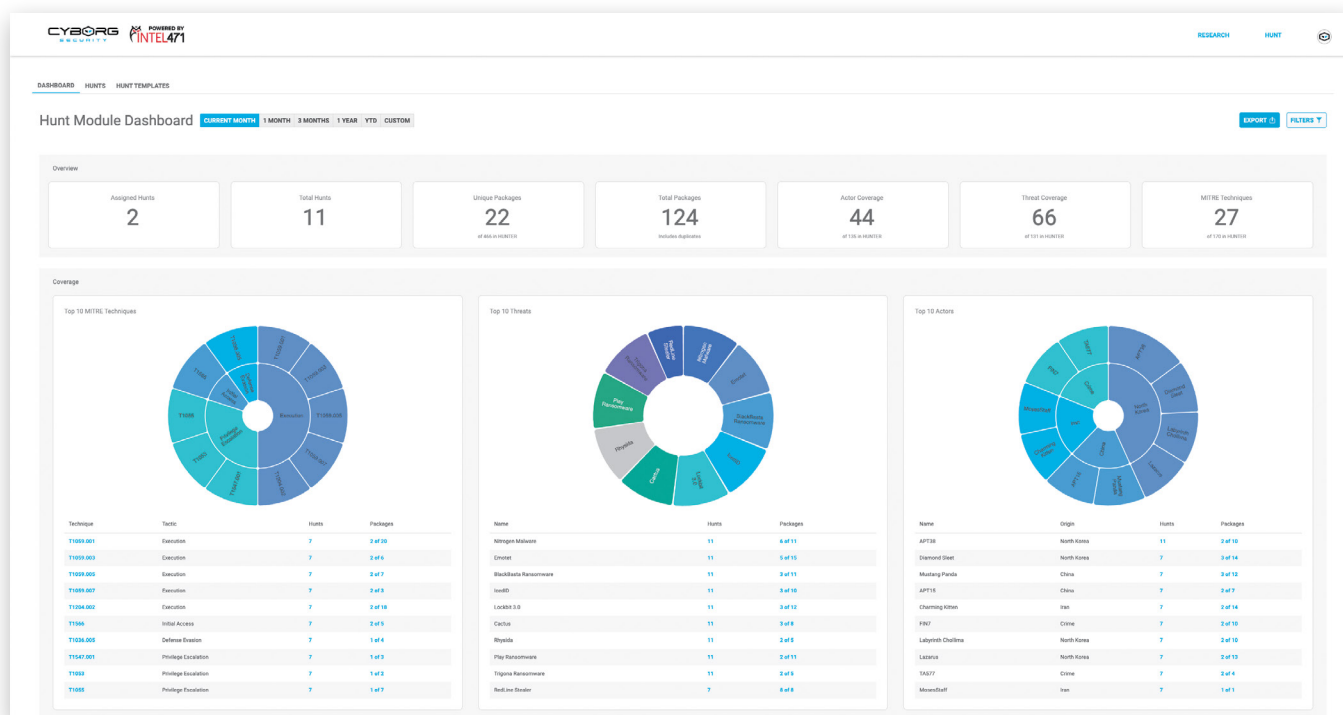
- Validate queries against production logging configurations and environments;
- Test the logging configuration and identify visibility gaps;
- Compare the results of HUNTER471 queries against the execution of each validation package;
- Emulate Analyst Runbooks and Mitigation Recommendations within the associated hunt package.

HUNTER471 content meets the growing need for risk-driven threat hunting sought by converged threat hunting and CTI practices. The platform helps organizations use CTI to initiate new investigations, guide hunts, and transform threat hunting results into enriched CTI that improve proactive defense and risk-based remediation.

HUNTER471 Hunt Management Module for Collaborative Hunting

Customers deploy the HUNTER471 Hunt Management Module to enable collaborative hunting across security teams, scale the platform as organizations build CTI and threat hunt maturity, and demonstrate each hunt’s return on investment (ROI).

- Hunt performance metrics dashboard tracks success in identifying threat actor behaviors by MITRE ATT&CK tactic, malware family name, and threat actor name.
- Assign, schedule, track, and manage hunts, monitor individual hunt progress, and coordinate ongoing threat hunting activities between purple and blue teams.
- Manage key findings, evidence, and remediations, supported by customizable spaces for storing and managing hunt content and custom queries.
- Produce tactical, operational, and strategic threat hunt reports for security operations, governance, and risk teams.



HUNTER471 Hunt Management Module Performance Dashboard

The HUNTER471 Advantage

The HUNTER471 platform and Hunt Packages offer quantifiable benefits that amplify the capabilities of organizations' security operations:

- Operationalize hunt data:** The platform delivers prioritized threat intelligence from Intel 471 sources, coupled with actionable hunt data, resulting in significant reduction in analyst effort and up-to-the-minute Hunt Packages.
- Increase hunt frequency by up to 500%:** With access to a vast library of human-built and curated threat hunting content, the HUNTER471 platform ensures organizations can address both novel and commonly occurring threats more efficiently. The ability to increase the volume of hunts conducted monthly by up to five times highlights the effectiveness of the platform.
- Use CTI to drive hunt investigations:** HUNTER471 offers tactical, operational, and strategic threat intelligence to guide the hunt. With MITRE ATT&CK tactics and techniques documented in each pack, hunters can pivot between related TTPs and explore new hunting activities. Tactical hunt reporting demonstrates the value of threat hunting as it relates to the context and coverage of hunt packages.
- Hunt with pre-built contextualization:** The platform eliminates the need for teams to spend extra effort on research and contextualization of threat hunt packages, resulting in increased efficiency.

Here's what Frost & Sullivan says about Intel 471's approach to CTI:

"While many CTI vendors rely on third-party and open-source data, Intel 471 stands out for its human-intelligence-centered approach and timely, actionable reports. Leveraging a global team of skilled analysts, Intel 471 extracts insights directly from threat actors and conducts tailored research upon request, ensuring its intelligence's relevance, timeliness, and exclusivity."

— Martin Naydenov, Frost & Sullivan Sr. Industry Analyst

5. **Follow expert runbooks:** Comprehensive content documentation, including detailed deployment, runbooks, and remediation guides allow threat hunters to channel their efforts more towards hunting.
6. **Deploy hunt content faster:** The platform offers deployment steps and documentation in a standardized manner, enabling engineering teams to deploy content faster and more efficiently.
7. **Safely test and validate hunt queries:** Emulation and validation tools accompanying each threat hunt package enable non-destructive emulation of adversary tactics, techniques, and procedures (TTPs), without needing extra engineering resources.
8. **Reduce pre- and post-hunt decision making:** Threat hunt packages come with threat intelligence, attack documentation, and detailed remediation guides to reduce effort throughout the pre-hunt process. Detailed remediation guidance ensures expedited and consistent mitigation of threats across infections.
9. **Know the next steps:** The platform provides comprehensive guidance and next steps for each threat hunt package, including detailed analyst runbooks to reduce the effort during the hunt process and mitigation recommendations that can be leveraged in an incident response process. The detailed response actions included in the packages can be incorporated into organization-specific documentation.
10. **Easier detection engineering:** Threat hunt packages include detection content logic to reduce the overall effort in developing and engineering detection content.

About Intel 471

Intel 471 empowers enterprises, government agencies, and other organizations to win the cyber-security 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 intel471.com.

Our customers' eyes and ears outside the wire.