INTEL471

HUNTER OVERVIEW

Hunt faster.
Stop cyber threats in their tracks.

Empowering Intelligence-Driven Threat Hunting Across Your Security Platforms

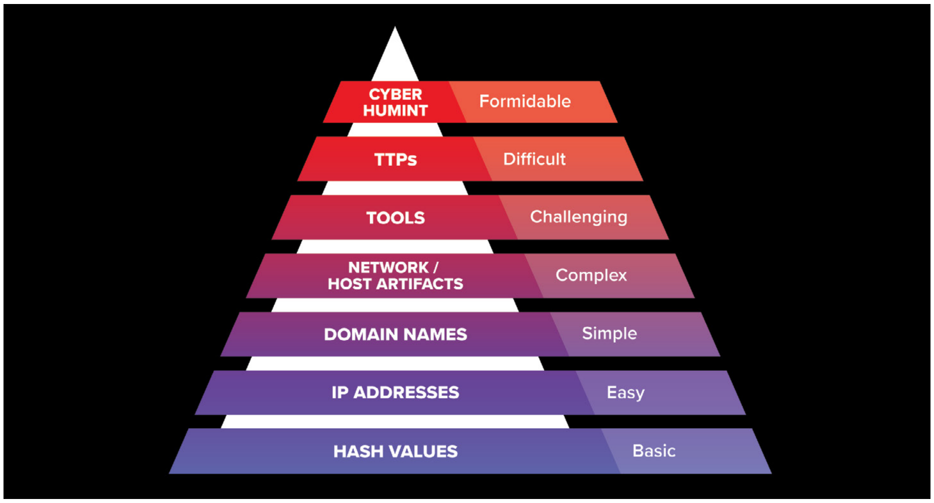
In a world where new threats can be weaponized and deployed within hours, it's vital that threat hunters have the right tools and content to rapidly investigate, identify, and remove stealthy threats before they manifest into a more serious incident.

The HUNTER 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 HUNTER 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. Our 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

HUNTER Validation Packages

HUNTER 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:

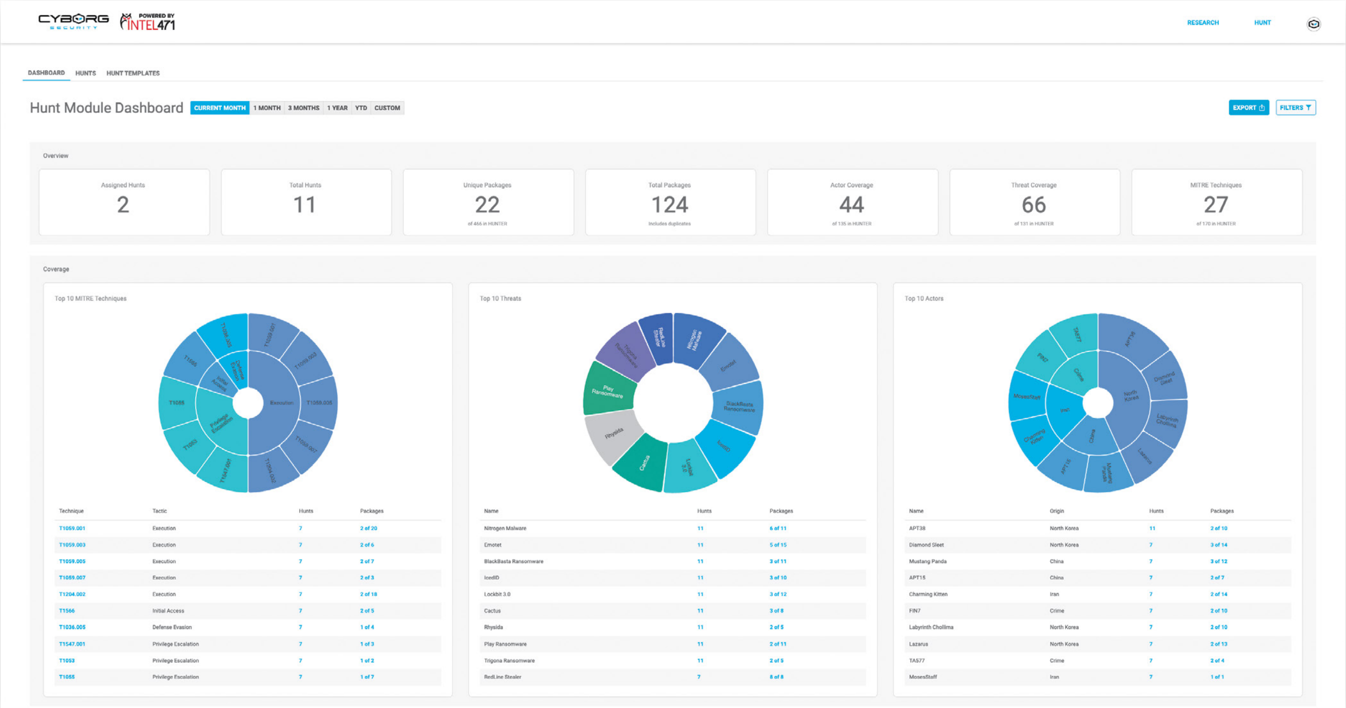
- Validate queries against production logging configurations and environments;
- Test the logging configuration and identify visibility gaps;
- Compare the results of HUNTER queries against the execution of each validation package;
- Emulate Analyst Runbooks and Mitigation Recommendations within the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

HUNTER 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.

The Hunt Management Module for Collaborative Hunting

Customers deploy the 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.



Hunt Module Dashboard

Overview

Assigned Hunts	Total Hunts	Unique Packages	Total Packages	Actor Coverage	Threat Coverage	MITRE Techniques
2	11	22	124	44	66	27
		of 466 in HUNTER	Includes duplicates	of 135 in HUNTER	of 131 in HUNTER	of 170 in HUNTER

Coverage

Top 10 MITRE Techniques

Technique	Tactic	Hunts	Packages
T1059.001	Execution	7	2 of 20
T1059.003	Execution	7	2 of 6
T1059.005	Execution	7	2 of 7
T1059.007	Execution	7	2 of 3
T1204.002	Execution	7	2 of 18
T1566	Initial Access	7	2 of 5
T1036.005	Defense Evasion	7	1 of 4
T1547.001	Privilege Escalation	7	1 of 3
T1053	Privilege Escalation	7	1 of 2
T1055	Privilege Escalation	7	1 of 7

Top 10 Threats

Name	Hunts	Packages
Nitrogen Malware	11	6 of 11
Emotet	11	5 of 15
BlackBasta Ransomware	11	3 of 11
IcedID	11	3 of 10
Lockbit 3.0	11	3 of 12
Cactus	11	3 of 8
Rhysida	11	2 of 5
Play Ransomware	11	2 of 11
Trigona Ransomware	11	2 of 5
RedLine Stealer	7	8 of 8

Top 10 Actors

Name	Origin	Hunts	Packages
APT38	North Korea	11	2 of 10
Diamond Sleet	North Korea	7	3 of 14
Mustang Panda	China	7	3 of 12
APT15	China	7	2 of 7
Charming Kitten	Iran	7	2 of 14
FIN7	Crime	7	2 of 10
Labyrinth Chollima	North Korea	7	2 of 10
Lazarus	North Korea	7	2 of 13
TA577	Crime	7	2 of 4
MosesStaff	Iran	7	1 of 1

HUNTER471 Hunt Management Module Performance Dashboard

The HUNTER Advantage

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

1. **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.

2. **Increase hunt frequency by up to 500%:** With access to a vast library of human-built and curated threat hunting content, the HUNTER 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.

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

3. **Use CTI to drive hunt investigations:** HUNTER 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.

4. **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.

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