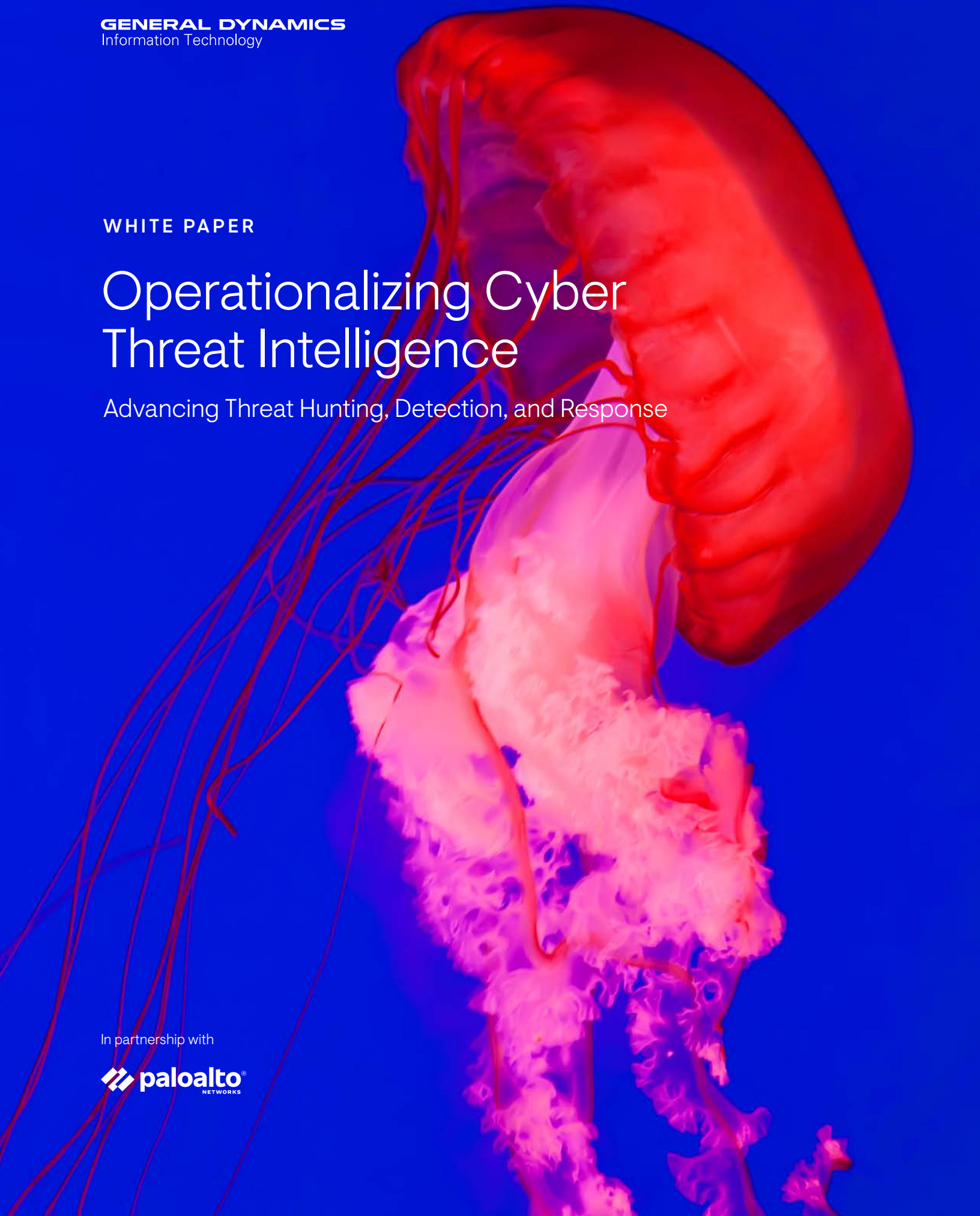
GENERAL DYNAMICS
Information Technology



WHITE PAPER

Operationalizing Cyber Threat Intelligence

Advancing Threat Hunting, Detection, and Response

In partnership with

paloalto NETWORKS

“The threat is not theoretical.”

JEN EASTERLY
Director, Cybersecurity and Infrastructure Security Agency

Executive Summary

The current geopolitical environment presents immense challenges as cyber threat activity becomes increasingly prevalent, serving as a core strategy for nation-states in conflict. The frequency of vulnerability and exploitation notifications is on the rise, and government officials regularly address concerns over cyber threats. The rapid evolution of artificial intelligence (AI) is transforming the threat landscape; offensive cyber actors have long utilized AI as a force multiplier, necessitating that cyber defenders swiftly adapt. By harnessing the power of cyber threat intelligence (CTI), organizations can continue to operate effectively amidst these growing threats. CTI is essential for guiding daily operations, informing cybersecurity priorities, and directing strategic investments. However, challenges such as intelligence sharing, data analysis, automation, and prioritization of actions can complicate its implementation. This white paper, the first in a three-part series, aims to educate on the significance of CTI, facilitate self-evaluation and maturity, and provide guidance on developing an effective CTI strategy and technology suite.

1

CTI POWERS A PROACTIVE DEFENSE

Integrating CTI across strategic, operational, and tactical levels enables organizations to transition from reacting to threats to anticipating and mitigating them proactively. This approach ensures that cybersecurity resources are focused where they’re most needed, enhancing the ability to protect critical assets effectively.

2

AUTOMATE AND LEVERAGE AI

Automating the detection of indicators of compromise and employing AI for threat analysis allows for faster, more efficient threat response and lets cybersecurity teams concentrate on high-level strategic planning.

3

AMPLIFY CTI WITH COLLABORATIVE SHARING

Sharing threat intelligence among organizations enhances the overall effectiveness of CTI. A collaborative approach to information sharing expands the data pool, offering broader insights into cyber threats and enabling more robust detection and defense strategies.

4

INVEST CONTINUOUSLY TO ADAPT

The dynamic nature of cyber threats necessitates ongoing investment in CTI capabilities. Staying ahead of adversaries requires not only investing in the latest technologies but also in training and retaining skilled professionals who can translate CTI into actionable defense strategies.

Current Cyber Threat Landscape

U.S. government agencies are confronted with an incredibly challenging cyber threat environment.

Ransomware continues to pose a significant threat to daily operations and data security. We are observing tactics, techniques, and procedures from cybercriminals that, just a few short years ago, we would have expected only from advanced persistent threat (APT) level actors. The landscape of vulnerabilities is expanding both in volume and criticality, and AI will only further shorten the path from proof of concept (POC) to exploitation.

Although AI has not yet introduced entirely new threat vectors, it has significantly accelerated the trends mentioned above, a fact that holds true across the existing range of cyber threat vectors. We have observed threat actors quickly leveraging AI – WormGPT is a prime example – while defenders have been somewhat slower in assessing how best to utilize AI for cyber defenses. CTI offers valuable use cases as we seek to harness AI to protect IT assets and information.

GDIT is monitoring these trends across the cyber threat landscape. Our clients often face similar challenges in this environment, including data overload, uncertainty about how best to use cyber threat data to support their missions, difficulties in vetting and assessing CTI data, and barriers to sharing and receiving information, among others. Looking forward, we anticipate the environment of vulnerabilities will become increasingly challenging. Moreover, as global geopolitical events continue to unfold, we can expect the cyber components of these conflicts to have worldwide repercussions. Finally, as U.S. officials implement sanctions to address cyber activities or comment on threats posed by adversarial nations, follow-on cyber activities are likely.

BEDROCK DEFENSES

In GDIT's recent research study, respondents identified CTI as the top capability for proactive defensive cyber operations within federal agencies.

GET THE FULL REPORT AT
gdit.com/perspectives/bedrock-defenses/

Cyber Threat Intelligence

Threat intelligence encompasses information about cyber threat activities, taking various forms, including indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), adversary collection priorities, adversary intent, triggers for action, finished intelligence products, and early warnings. These categories of CTI can be applied across tactical, operational, and strategic levels. The collection and dissemination of CTI typically adhere to an intelligence production cycle, which may vary between organizations but is essential for effective threat intelligence management.

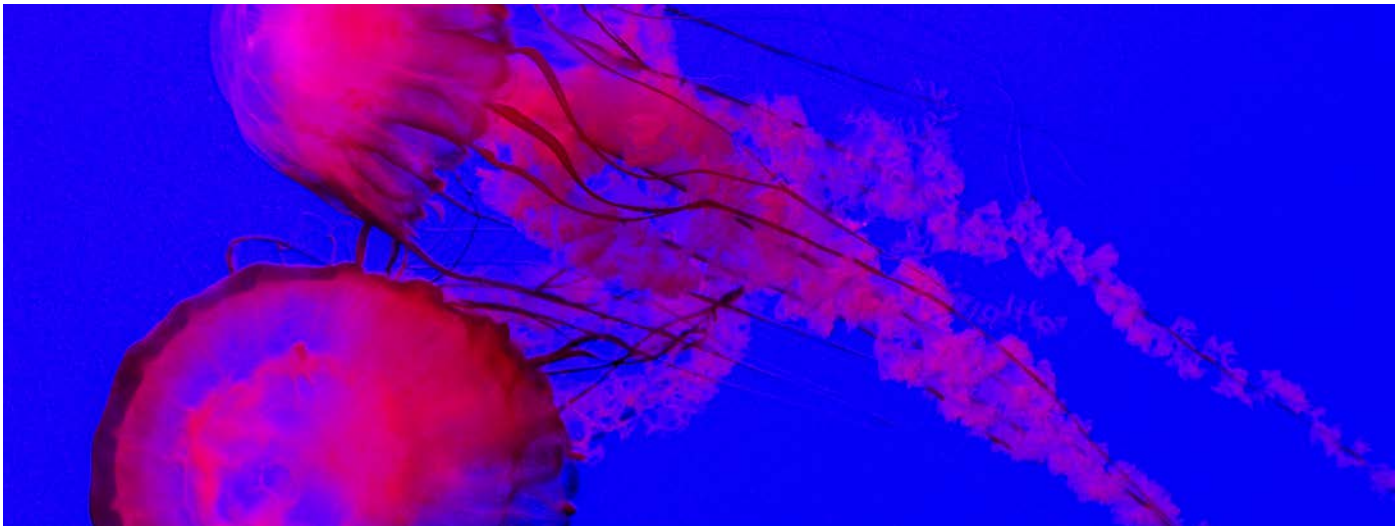
- **Adversary intent to target:** Different adversaries exhibit varying levels of intent to target organizations, influenced by factors such as diplomatic relationships, international alliances, and geopolitical events. For instance, cyber network

defenders and executive decision-makers would be more concerned about a moderately sophisticated actor with high intent to target their organization than a highly sophisticated adversary with low intent. Intent can encompass desires for intelligence collection, destruction (e.g., targeting critical infrastructure), establishing persistence, and preparing for future disruption or distraction.

- **Adversary intelligence collection priorities:** These priorities indicate the type of information an adversary is tasked with collecting. Cybercriminals may target personally identifiable information (PII) or protected health information (PHI) for fraudulent purposes, whereas nation-state actors may focus on specific information types to support their government or employers, such as U.S. government policy insights.
- **Adversary capabilities:** Assessing adversaries' cyber threat capabilities based on raw CTI can lead to classifications such as highly or moderately sophisticated. This assessment encompasses technical skills, resources, infrastructure, and personnel, informing the risk they present to an organization.
- **Adversary triggers:** Insight into a threat actor's collection priorities and past targeting can indicate which geopolitical and other events might trigger offensive cyber threat activity. Although secondary to intent, this understanding aids network defenders in focusing their attention and enhancing awareness during critical times.
- **Indicators of compromise (IOCs):** These are technical data points used to detect potential malicious activity on computers or other assets, indicating a breach. This information is invaluable for network defenders as they scour their networks for signs of compromise.
- **Tactics, techniques, and procedures (TTPs):** CTI collects and analyzes tactics, techniques, and procedures to describe the operational behavior of cyber threat actors. TTPs offer a broader perspective than IOCs, detailing an actor's modus operandi, including targeting, exploitation, lateral movement, and information harvesting strategies.
- **Finished intelligence assessments:** Relying on both raw and processed intelligence, finished intelligence assessments utilize analytic methods to evaluate information and produce judgments on issues like adversary collection priorities, intent, capabilities, likelihood of future attacks, and potential success. This analysis can include predictive and early warning elements, supported by various federal and commercial sources, and is crucial for organizations seeking to tailor intelligence to their specific operational environments.

THE CONVERGENCE OF APT AND CYBERCRIME TACTICS

Organizations often track activity from APT separately from cybercriminals and ransomware activities. However, in recent years, GDIT has observed a significant increase in the sophistication of ransomware actors, noting an overlap between the infrastructure and tactics, techniques, and procedures of APTs and cybercrime actors. To keep pace with these shifts in sophistication and potential impact, organizations need to invest in cybercrime intelligence. This is a critical component of CTI on the strategic front to ensure the right investments are made. Operationally, it aids in training and deploying resources effectively. Tactically, it enables the rapid deployment and action on indicators of compromise (IOCs).



Why CTI Matters

Threat should be the engine that drives cybersecurity efforts, acting as the North Star that directs cyber operations at both the working level and in executive decision-making and investments. CTI enables organizations to prioritize defenses based on risk, ensuring that resources are proactively allocated where they will have the greatest impact and deliver the highest return.

SPEED

CTI enables a quicker response to cyber threats and improves decision-making processes. It allows front-line analysts to prioritize alerts and respond more swiftly to the most critical threats, thereby providing a data-driven approach to managing data overload and alert fatigue.

In the midst of an active incident, understanding an adversary's collection priorities and TTPs can forecast their next moves and likely targets for lateral movement. This insight increases a defender's ability to keep pace with an attacker and potentially prevent further data breaches or data exfiltration.

SHIFT FROM REACTIVE TO PROACTIVE

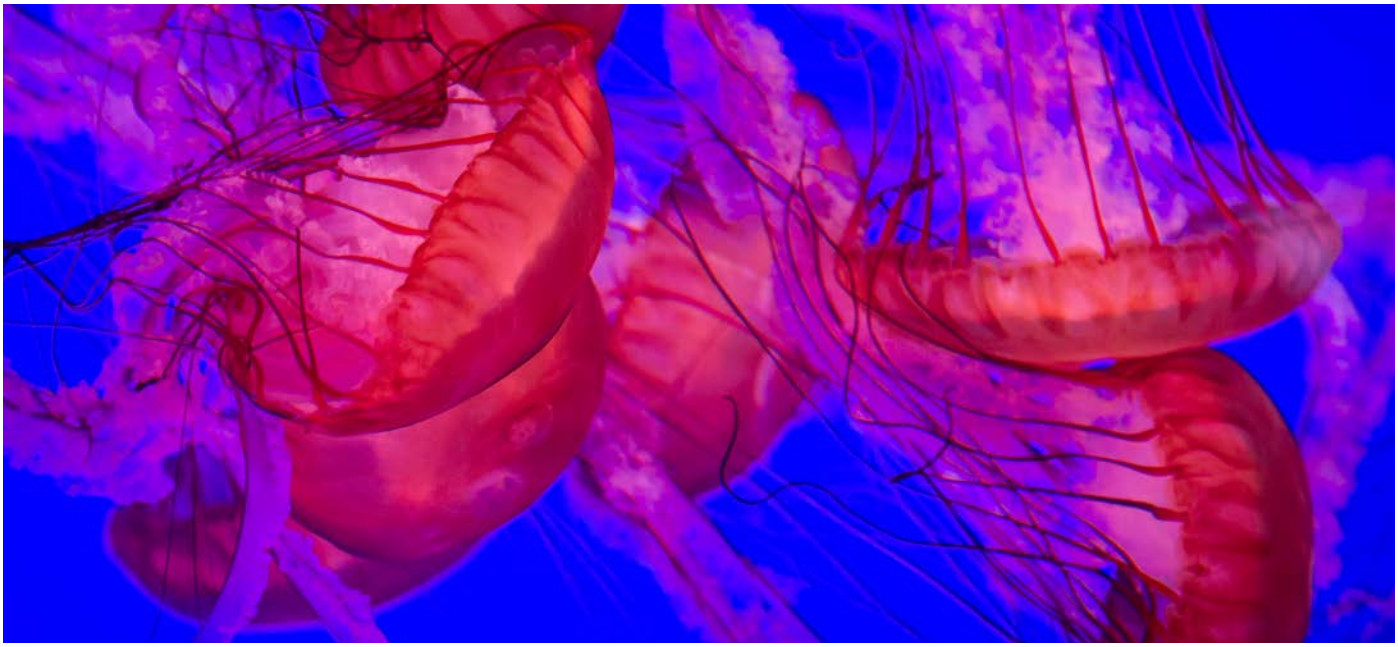
Integrating CTI across cyber organizations fosters a preventative and flexible approach rather than a reactive response to compromises. While this shift takes time, organizations can see a rapid return on investment through better decision-making, faster detection, and a significant reduction in the time and resources spent on incident response containment.

For instance, knowledge of an adversary's collection priorities can inform assessments of high-value assets (HVA) and help prioritize enhanced monitoring for certain data sets or users, supporting early detection efforts.

Understanding the current threat landscape, including which actors are likely to target your organization and their preferred TTPs, drives investments in tools, personnel, and training. This ensures that limited resources are utilized most effectively to achieve the best possible cybersecurity outcomes.

THE INTELLIGENCE CYCLE

An effective CTI program follows an intelligence production cycle, typically encompassing five stages, though the terminology may vary. Initially, intelligence analysts require direction to understand the information needs of their stakeholders, also known as intelligence collection priorities. These priorities drive the organization's data collection efforts. Upon collecting information—be it raw or processed—intelligence analysts then process this data, a step that can involve translation, relevance assessment, and source credibility evaluation. Analysts then analyze the processed data using various methods, potentially including machine learning or AI, to produce CTI that is disseminated to stakeholders in formats like briefings, white papers, or technical data sharing. A feedback loop allowing stakeholders to verify whether the intelligence meets their needs is crucial, fostering organizational growth and maturity over time.



Best Practices for Applying CTI in Your Organization

CTI is an invaluable tool for executive decision-making and resource allocation; it reduces guesswork and enables data-driven decisions. Understanding your organization's threat landscape allows for better resource allocation and should inform the prioritization of daily tasks as well as long-term projects. The current labor market for cybersecurity professionals is highly competitive, with more jobs available than qualified personnel. A data-driven approach is necessary to focus our workers' attention on our most vulnerable and likely targeted assets and threat vectors. Cybersecurity professionals face challenges with data overload and alert fatigue; using CTI to prioritize where our analysts focus their time means we can achieve more with our current resources, which cannot examine every data feed simultaneously and need to selectively focus on certain alerts.

UTILIZE IOCS TO IDENTIFY THREATS AND BREACHES

IOCs are primarily useful tactically, and hunting for them can be automated to enhance detection and support rapid incident response.

Automating the correlation of IOCs against an organization's internal infrastructure streamlines detection and supports rapid incident response by freeing up cybersecurity personnel to concentrate on behavior-based and other advanced forms of threat hunting.

ASSESS ADVERSARY INTENT

Understanding adversary collection priorities should inform high-value asset (HVA) identification, continuous monitoring, and data protections. Tripwires, honeypots, or other deceptive technologies can be effectively employed to detect and deter activity targeting HVAs.

ANALYZE TTPS TO UNDERSTAND ADVERSARY TACTICS

TTPs are useful for cybersecurity operations and can serve as a detection mechanism. TTPs are also useful in attributing cyber threat activity to a particular actor, which can assist in assessing collection priorities, likely next steps, and informing effective remediation actions.

The MITRE ATT&CK framework has been effectively used during incident response to determine attribution, then to forecast adversary actions and likely collection priorities, allowing for more bespoke and effective incident response, monitoring, hunting, and remediation actions. MITRE provides matrices for Enterprise, Mobile, and Industrial Control Systems (ICS) covering tactics and techniques across stages of threat activity such as reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defensive evasion, credential access, discovery, etc.

ALIGN DEFENSES WITH ADVERSARY CAPABILITIES

These CTI assessments should inform day-to-day security operations as well as executive decision-making around resources and investments. Every frontline security operations center (SOC) operator should have a working understanding of the key cyber threat actors who have and are likely to target their organization, as well as how capable those actors are and what sort of threat vectors and TTPs to be on the lookout for when events dictate.

SHARE AND COLLABORATE ON CTI

A mature CTI program should regularly share CTI insights—not only IOCs and TTPs but also assessments and predictions—with frontline defenders to help focus their threat hunting and incident response actions. Heightened monitoring of certain assets and personnel, responsive to geopolitical events, exemplifies a proactive strategy. For instance, the conflict between Ukraine and Russia shifted Russian cyber threat actors' targeting in predictable ways. Using this information to inform cyber threat defenses, such as heightened monitoring around assets and personnel of particular interest to Russian threat actors, is a strategy we have successfully used in support of federal agencies to keep them ahead of the threat.

BOOST SKILLS WITH CONTINUOUS CYBER TRAINING

Personnel who work in cybersecurity want to feel that they are growing professionally and making an impact on their organization. Training in CTI and how to effectively use it both empowers them and elevates their skills.

Next Steps

Whether you're exploring CTI for the first time or looking to enhance an existing program, now is the moment to invest. Mature organizations should integrate both internal feeds and multiple, vetted external feeds—across various classification levels, if applicable—to effectively assess their infrastructure and rapidly detect malicious activity. CTI must not only feed into automation but also prioritize our analysts' time. AI and machine learning can be leveraged to support threat detection and data analysis. We must embrace AI for defensive purposes just as our adversaries utilize its power to enhance and accelerate their offensive operations.

We invite you to contact us to assess your current use of CTI and to explore your specific threat landscape. With GDIT's Digital Accelerators, including Eclipse Defensive Cyber Operations and Everest Zero Trust architectures, we are dedicated to supporting digital transformations, driving modernization, and enhancing cybersecurity postures.

GDIT

About GDIT Digital Consulting

General Dynamics Information Technology (GDIT) stands at the nexus of digital consulting and mission-centric innovation in the public sector. As the pace of technology changes and as mission demands accelerate, GDIT's Digital Consulting Practice supports agencies navigating intricate landscapes and harnessing the transformative potential of AI, cybersecurity, and cloud solutions. Partnering with visionary leaders across the public domain, we craft strategies that catalyze digital evolution, drive sustainable modernization, and position our clients at the forefront of excellence.

About GDIT

GDIT is a global technology and professional services company that delivers consulting, technology and mission services to every major agency across the U.S. government, defense and intelligence community. Our 30,000 experts and consultants extract the power of technology to create immediate value and deliver solutions at the edge of innovation. We operate across 30 countries worldwide, offering leading capabilities in digital modernization, AI/ML, cloud, cyber and application development. Together with our clients, we strive to create a safer, smarter world by harnessing the power of deep expertise and advanced technology. More information about GDIT is available at www.gdit.com.

paloalto NETWORKS

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats so organizations can confidently embrace technology. We provide next-gen cybersecurity to thousands of customers globally across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the zero trust enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice. For more information, please visit www.paloaltonetworks.com.

Contact

GENERAL INQUIRIES

Christopher Aiello
Senior Marketing Manager
GDIT
Email: christopher.aiello@gdit.com

MEDIA INQUIRIES

Jay Srinivasan
Senior Public Relations Manager
GDIT
Email: jayendran.srinivasan@gdit.com

Author

Dr. Mischa Beckett
Director of Cyber Threat Intelligence, Federal and Civilian, GDIT

Dr. Mischa Beckett is a cybersecurity expert specializing in analytic frameworks and threat intelligence analysis. She has extensive experience supporting federal clients in cyber threat intelligence and cybersecurity operations.

Contributors

Dr. Matthew McFadden
Vice President, Cyber & Distinguished Technologist, GDIT

Michael Paluzsay
Chief Information Security Officer, Federal and Civilian, GDIT

Angelique Napoleon
Deputy Chief Information Security Officer, Intelligence and Homeland Security, GDIT