COLUMBIA UNIVERSITY SCHOOL OF INTERNATIONAL AND PUBLIC AFFAIRS

CYBER THREAT HUNTING IN THE U.S. DEFENSE INDUSTRIAL BASE

A THIRD-PARTY SERVICE MODEL APPROACH & POLICY RECOMMENDATIONS

APRIL 2021 // ASHLEY FOX, LOUIS JARVERS, YUELIN LI, KEVIN MAGUIRE, ANDREW NGUYEN, YUNZHEN WANG, ZHENRONG WU, YOUYOU WU

Executive Summary

The "US Cyberspace Solarium Commission and the Defense Industrial Base" is a Columbia University capstone project conducted in association with PricewaterhouseCoopers (PwC). The project seeks to assess the viability of a recommendation from the US Cyberspace Solarium Commission's (CSC) 2020 for a mandated cyber threat hunting (CTH) program across the Defense Industrial Base (DIB). The project sought three objectives: market potential of CTH as a service across the DIB, criteria for establishing a "DoD-approved third party" that could undertake these services, and how CTH should be prioritized across the DIB.

CTH is a proactive solution to digital vulnerabilities facing modern organizations. It is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. For the DIB, a group of companies that enable the DoD's warfighting capabilities, the size and scope of the organization matters as to whether CTH services make the most sense.

There are many other issues with establishing a mandated DIB CTH program. Firstly, organizations must already have common cyber security practices in place. The Cybersecurity Maturity Model Certification (CMMC), a cyber certification process, regulates this for DIB members. CMMC standards have had significant issues to include a lack of policy delineation leading to third-party compliance saturation and accreditation issues. Secondly, mandated intelligence sharing policies, necessary for effective CTH, have not been implemented. Thirdly, CTH as a service (CTHaaS) is cost prohibitive for many DIB members, especially mid and small-size DIB companies. Ultimately, PwC's success depends largely on how CTH policy is shaped in the near future. The FY 2021 National Defense Authorization Act (NDAA) calls for the creation of DIB CTH program following an initial study, after which the Secretary of Defense can take factors such as maturity, operational role and others into account when proposing a mandated CTH program. Requirements, DoD mechanisms, incentives, and program participation levels are all part of these considerations, while also providing the Secretary of Defense the authority to waive prohibitions due to non-compliance where needed. Given that the study is being undertaken during other urgent policy crises such as SolarWinds, PwC can help shape the conversation.

We recommend three general policy guidelines when pursuing this conversation. First, the policy should avoid "one-size-fits-all" requirements and scale requirements based on risk and maturity. Second, the policy should reshape a com-

pliance-only mentality that balances punitive actions with incentives for companies to meet CTH compliance. Third, in order for CTH to work, the establishment of a mandated cyber-intelligence sharing program for the DIB must be resolved. With these policies in place, PwC can move forward with pursuing a DIB CTH service model.

The service model must take into account the size and capability of the DIB member. Large organizations such as Boeing or Lockheed-Martin will find CTH easy with extensive resources and personnel, while small- and medium-size companies will struggle to implement CTH. CTHaaS will only apply to organizations of CMMC Level 3 or higher, have financial capability, and do not have in-house services. CMMC accreditation is a factor, and PwC may want to apply as for CMMC accreditation. Actual CTHaaS services will follow a standard CTH cycle, with higher and more expensive service provisions allowing for more complex hunts. Event-based services (a response to major cyber events like SolarWinds or the Microsoft Exchange attacks) can also be included. Pricing should reflect the differing levels of sophistication, expertise brought, and hours for the CTH project.

Acknowledgements

The SIPA-PricewaterhouseCoopers capstone team would like to extend special thanks to PwC Senior Director for Cybersecurity, Privacy and Forensics Shawn Lonergan, for conceptualizing the project and providing feedback throughout the process. We would also like to highlight the dedication and assistance of our capstone project advisors, Neal Pollard and Elizabeth Cartier, for their mentorship, expertise, and assistance over the last three months.

Furthermore, over the course of the project, the team solicited advice and interviews with 25 individuals with expertise related to cyber threat hunting and/or the U.S. defense industrial base. The authors would like to acknowledge the following individuals for their contributions and assistance over the last few months:

Michael Gibbons, Chris Hendricks, Triet Bach, Erica Borghard, Rob Morgus, John Costello, Michael O'Hanlon, Mark Montgomery, David Christie, Haris Shawl, April Lenhard, Dan Madden, Cristina Martinez, Jason Healey, Greg Rattray, Jim Keffer, JD Work, Jenny Jun, Scott Shepard, Katie Arrington, Mark Klenko, Corbin Evans, and others.

Table of Contents

Executive Summary ii
Acknowledgements iii
Introduction 2
Background 2
Problem Summary 4
Research Findings 5
Policy Findings 5
Market Findings 6
Recommendations 7
Policy Recommendations 7
Service Model Recommendations 11
Conclusion 13
Appendices 14
Appendix A: Definitions and Relevant Stakeholders 15
Appendix B: Details for a third-party service model 17
Appendix C: Proposed legislative language for a mandated CTH program 21

Introduction

The U.S. Cyberspace Solarium Commission (CSC) Report recommends a mandated program for cyber threat hunting (CTH) across the networks of defense industrial base (DIB) companies. The recommendation and associated legislative proposal note CTH could be conducted by the network owners, Department of Defense (DoD) entities, and/or approved third parties. This project seeks to address the following objectives:

- The potential market and scalability of CTH as a service across the DIB.
- Criteria to be considered in the establishment of a "DoD approved third party."
- The ideal use case of how these activities should be prioritized across the DIB with respect to the risk environment and the maturity of the organization.

The data in this report is aggregated through research of existing archives and field interviews with industry experts, policy makers, and DIB representatives. The project's objectives will be addressed through an analysis of two primary scopes: market potential and policy prospects.

This project includes a brief primer on CTH and the DIB, to include discussion of cybersecurity needs across federally contracted firms. We also discuss our research findings to include pertinent policy recommendations and market viability. Finally, we will recommend an operating model PwC should pursue and describe the challenges of providing CTH services within the framework of a mandated program.

Background

As companies increasingly pivot toward digital business models, exponentially more data is generated and shared among organizations, partners and customers. This digital information has become the lifeblood of the interconnected business ecosystem and is increasingly valuable to organizations—and to skilled threat actors. It also means companies are exposed to new digital vulnerabilities, making an effective approach to cybersecurity, privacy, and forensics more important than ever.

CTH refers to the process of proactively and iteratively searching through networks to detect and counter tactics, techniques, and procedures of advanced attackers that evade existing security solutions.[1] CTH is an analyst-centric process

[11] Gunter, D. (2021). *A Practical Model for Conducting Cyber Threat Hunting*. SANS Institute. https://www.sans.org/reading-room/whitepapers/threathunting/practical-model-conducting-cyber-threat-hunting-38710.

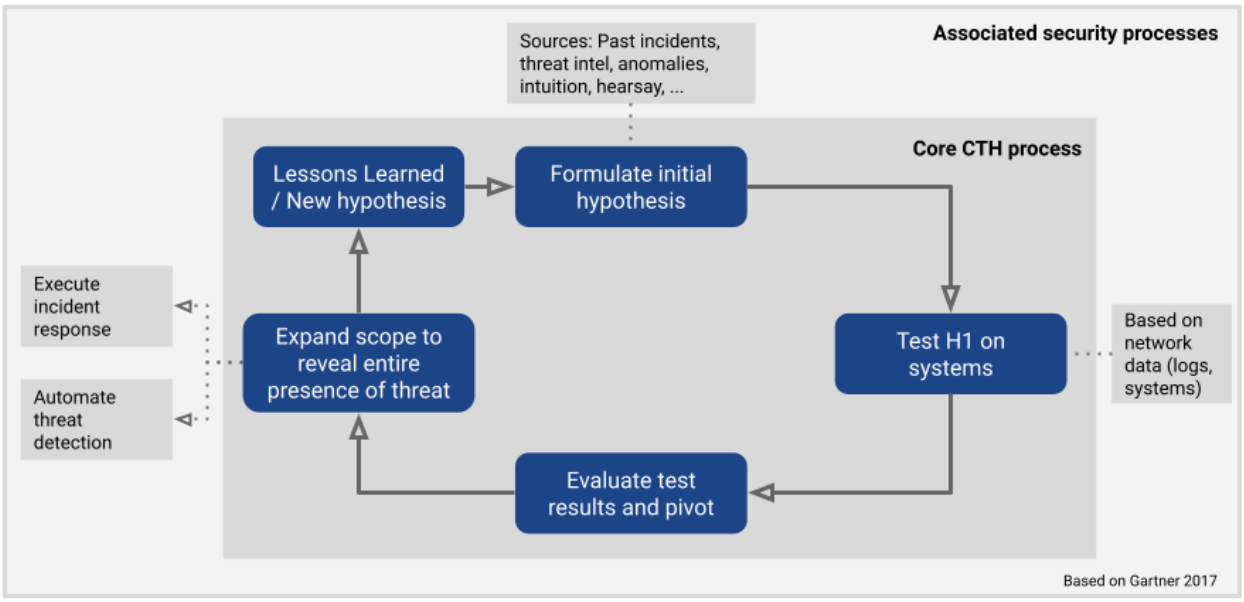


Figure 1: Cyclical model of a cyber threat hunting process

that enables organizations to uncover hidden advanced threats missed by automated preventative and detective controls. CTH represents an advanced security practice suitable for organizations facing persistent threats. Being different from traditional threat management measures that typically involve investigating evidence-based data after a potential threat, CTH is a more proactive approach to cyber threats. CTH usually follows a cyclical process that starts with a hypothesis of a potential intrusion and what to hunt for, then collects and assesses network data to prove or reject the hypothesis, before taking respective follow-up measures (e.g., intrusion responses, updates to Intrusion Detection Systems). Feedback is collected and discussed to improve future hunts.[2]

The DIB is a wide-ranging and complex group of companies that produce products and services that enable the DoD's warfighting capabilities. The size and scale of DIB entities varies and include both domestic and international DIB entities. Domestic DIB entities include public-sector (government owned and operated) facilities, academic institutions, and private-sector companies located in the United States. The global DIB includes foreign-owned companies and commodities sourced from countries with which the United States may or may not maintain formal defense cooperation partnerships. The domestic DIB and portions of the global DIB form the National Technology

[2] Chuvakin, A. (2017). How to Hunt for Security Threats. *Gartner Report*. https://www.gartner.com/smarterwithgartner/how-to-hunt-for-security-threats/.

Industrial Base (NTIB) as codified in 10 U.S.C. §2500.[3]

Regulations, incentive, and disincentive structures differ for the private and public sectors. DIB companies vary in size, cyber threat level, capabilities, and needs for CTH services will vary. We considered CTH for different-sized companies to better determine the scope of DIB. In our interviews, much of the difficulty with cyber threat hunting as a service (CTHaaS) has come from determining the size of companies that require this service. DIB entities are classified as prime contractors and subcontractors in terms of how they differentiate and compound the problem of broadness in providing CTH services.

PROBLEM SUMMARY

Enacting a mandated CTH program faces significant challenges. The nature of CTH requires a firm to have a prior level of risk awareness; it is not worthwhile if other common cyber security practices are not set. There are government frameworks for cybersecurity that have been recently adopted such as the Cybersecurity Maturity Model Certification (CMMC), a cyber certification process required for DIB members. The CMMC model offers a case study in how a DIB CTH program could be implemented, as well as challenges such a CTH program will face. While large DIB entities can likely afford CTH services, smaller firms with less internal resources have no ability or no need for robust threat hunting depending on the nature of their role within the supply chain. Therefore, CTHaaS aimed at all firms in the DIB supply chain would not be an efficient strategy for PwC.

In addition, the current legislative landscape is not clearly defined. Previous National Institution of Standards and Technology (NIST) standards and even CMMC have seen irregular adherence throughout the DIB. These oversights are not due to a lack of effort but more often than not, due to confusion or controversy regarding federal regulations.[4] Cybersecurity is presently a significant topic of discussion, but specifics beyond broad frameworks for regulation are often ambiguous or in flux. Many of our interviews highlighted the confusion created by a lack of policy delineation which has also led to an oversaturation of third-party cybersecurity firms with questionable efficacy. Current operating procedures are already seen as cumber-

[3] Peters, H. (2021). *Defense Primer: U.S. Defense Industrial Base*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF10548/10

[4] Barnett, J. (2021, March 30). CMMC is under an internal DOD review. *FedScoop*. https://www.fedscoop.com/dod-cmmc-review-new-administration/

some and DIB firms will be resistant to additional regulatory burdens as well as third-party vendors who may be seen as dubious cybersecurity peddlers.[5]

CTH is an advanced service that comes after there is a strong foundation to support it. While it will likely be a requirement for critical DIB firms in the future, implementing such a mandate will not be without growing pains in the interim.

Research Findings

POLICY FINDINGS

Any discussion of a mandated CTH program is inherently acquisition reform. Currently the Defense Federal Acquisition System (DFARS) governs private-sector compliance in obtaining federal contracts. The most pertinent clause that will affect cybersecurity is DFARS 252.204-7012 which requires contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted over the contractor's internal networks.[6] "Adequate security" is defined as adherence to the NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (NIST 800-171).[7] NIST 800-171 provides recommended requirements for the threshold of cybersecurity a contractor and any subcontractors must comply with when fulfilling a federal defense contract.

The CMMC, introduced in 2020, sets standards that tiers a DIB firm's cyber defenses along five levels of ascending controls.[8] CMMC is a de-facto auditor of how adequately NIST standards are incorporated across DIB firms. Federal defense contracts require DIB firms meet CMMC requirements. The CSC 6.2.2 recommendation for a mandated CTH program across DIB firms will likely operate within CMMC. However, such a mandated program faces significant challenges and will require further definition of related legislation before any third-party vendor can confidently gauge profitability.

---

[5] Corbin Evans. Principal Director, Strategic Programs. National Defense Industry Association. Interview 4/6/2021.

[6] Assad, S. (2017). *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*. Office of the Undersecretary of Defense, Acquisition, Technology, and Logistics. https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

[7] Spencer, T. (2019, October 8). *What Is the NIST SP 800-171 and Who Needs to Follow It?* [National Institute of Standards and Technology]. https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0.

[8] Office of Under Secretary of Defense for Acquisition & Sustainment CMMC. https://www.acq.osd.mil/cmmc/faq.html

The greatest challenge to mandated CTH will be unsettled policy or legislation. The definitions of "adequate security" are ambiguous and fluid as CMMC is still being implemented unevenly across the DIB. DIB firms are saturated by CTH providers that are not necessarily approved by the CMMC-Accreditation Body (CMMC-AB).[9] DIB firms as well as any approved third-party vendor face uncertainty regarding what standards will be defined.

Scoping the DIB is another added challenge to implementing a mandated CTH program. From a prime contractor to subcontractors, all have to adhere to CMMC standards but not all have the resources or even necessity to adhere. Achieving parity along the entire supply chain requires precision or tailored legislation that is not yet existent. NIST standards have been around since 2016; however, adherence across the DIB has been inconsistent.

The CSC's recommendation for a CTH program may be premature considering that it's 6.2.1 recommendation for mandated cyber intelligence sharing across the DIB has yet to be implemented. As CTH necessitates a prior foundation of knowledge for implementation, intelligence aggregation as a basic fundamental is not yet robust enough across the DIB supply chain for CTH to be effective. CTH will be necessary for mature organizations in the future (CMMC Level 3 and above), however conditions for a mandated CTH program remain challenging.

MARKET FINDINGS

The market size and pricing of CTH services is very dependent on which firms are serviced. A one-size-fits-all pricing is not feasible because DIB organizations are at different levels of CMMC maturity. Therefore, the market size and pricing for CTH services will depend on an individual firm's capabilities. Firms with robust in-house cybersecurity resources will have more knowledge of their risk environment and may even already be conducting CTH internally. Smaller firms may not warrant CTH services or may not be risk aware enough to optimize a hunt.

The market will most likely grow because of increasing levels of digitization, the scale of the industry, and the iterative requirement for CTH through government regulation. Third-party vendors will likely be necessary and in demand as CMMC standards become requirements in the next 5 years.[10] There is no existing criteria to be an approved third-party vendor

[9] Corbin Evans. Principal Director, Strategic Programs. National Defense Industry Association. Interview 4/6/2021.

[10] Katie Arrington. Chief Information Security Officer to the Assistant Secretary of Defense for Acquisition. Interview 4/14/2021.

which has led to a rise of questionable service providers. PwC should expect stricter standards and criteria for what an approved third-party vendor will be. This criterion will likely come from CMMC-AB or a related entity. As an additional consideration, the current costs of CTHaaS, however, is often above what many organizations are willing or able to pay. Firms that third-party vendors want to target for CTHaaS occupy a very specific niche. Our research has shown that third-party vendors should target middle-maturity DIB firms that are risk-aware but do not have the resources to proactively address those risks.

Recommendations

POLICY RECOMMENDATIONS

PwC's success with the recommended service operating model will depend significantly on the legislative and regulatory framework within which it operates. There is currently no existing government-mandated CTH program across any United States critical infrastructure sector. However, our research indicates that the DIB is a prime candidate for a CTH program.

Language introduced in a draft version of H.R.6395 - National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) (See Appendix B) calls for the creation of a "defense industrial base cybersecurity threat hunting and sensing, discovery, and mitigation" program following an initial threat hunting study.[11] Upon a positive determination from the study that a CTH program is feasible, the bill's language called for the establishment of a tiered program by the Secretary of Defense that takes the maturity, operational role, level of information classification, and level of access to covered defense information of each covered entity into account. The proposed parameters for the subsequent mandated CTH program were as follows:

A. Include requirements for mitigating any vulnerabilities identified pursuant to the Program;

B. Provide a mechanism for the Department of Defense to share with entities in the DIB malicious code, indicators of compromise, and insights on the evolving threat landscape;

C. Provide incentives for entities in the DIB to share with the Department of Defense, including National Security Agency's Cybersecurity Directorate, threat and vulnerability information

[11] Adam Smith, "National Defense Authorization Act for Fiscal Year 2021," Pub. L. No. H.R. 6395, § 1634 (2020), https://www.congress.gov/bill/116th-congress/house-bill/6395/text/rh#toc-HA575E6541EC14C5494AE22AFEE8AAE49.

collected pursuant to threat monitoring and hunt activities; and

D. Mandate a minimum level of program participation for any entity that is part of the advanced DIB.

Lastly, the NDAA proposed language further provided authority for the Secretary of Defense to waive a prohibition from procuring any item, equipment, system, or service from "any entity in the defense industrial base that is not in compliance with the requirements of the Program" if the Secretary determines that "the requirement to participate in the Program is unnecessary to protect the interests of the United States," or that "at the request of such an entity … there is a compelling justification for such a waiver."[12]

This specific CTH program proposal was ultimately removed from the final version of the NDAA but included the preliminary mandated assessment for the feasibility and suitability of a DIB CTH program. While the programmatic regulation language was removed, the inclusion of the mandatory preliminary assessment lays a solid foundation for the potential of a government-mandated CTH program across the DIB in the near future. Given the publicity and urgency surrounding the SolarWinds and Microsoft Exchange incidents, field experts we interviewed indicated a government-mandated CTH program is becoming more likely than ever. Specifically, the CSC is already requesting that the Biden administration bring a threat hunting program to fruition.[13]

As the nature of such a program is currently in flux, PwC has an opportunity to help shape the discussion on what a CTH program might look like for service providers and covered entities alike. To that end, our team recommends the following policy provisions to supplement the original proposed language for a government mandated CTH program from the FY21 NDAA:

Avoid "one-size-fits-all" by scaling program requirements based on entity risk and maturity

Given the sheer size of the DIB and the variance in maturity, capability, and risk of its members, it will be crucial for the Department of Defense to distinguish between covered entities whose current security

[12] National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, United States Congress, 116th (2020). https://www.congress.gov/bill/116th-congress/house-bill/6395/text/rh#toc-HA575E6541EC14C5494AE22AFEE8AAE49.

[13] Mariam Baksh, "CISA Shares Specs for Threat-Hunting Solution," Nextgov.com, January 25, 2021, https://www.nextgov.com/cybersecurity/2021/01/cisa-shares-specs-threat-hunting-solution/171612/.

Risk-based Criticality Assessment	Low Risk	Medium Risk	High Risk
Risk-Ignorant	Medium	High	High
Risk-Aware	Low	Medium	High
Risk-Managed	Low	Low	Medium

Figure 2: Risk-based criticality matrix for DIB members

posture poses a significant or critical risk to national security and those who do not. As referenced in the service model recommendations, risk-based criticality of DIB members can be assessed with a matrix model outlining threat levels and the risk awareness of a company (see Figure 2).

Any government mandated program should first endeavor to work with the most at-risk and least mature entities to bring them to a comparable level of security to their more mature and capable counterparts. At the same time, those covered entities with the existing capability and maturity to implement CTH activities must be held accountable from a compliance and due diligence standpoint. A one-size-fits-all approach would not adequately address the variance in capabilities and maturity of the various covered entities and attempting to provide a blanket policy could further exacerbate existing security issues in the sector.

By categorizing covered entities by risk, maturity, and capability, the government could better distribute its resources by implementing the program at an initial high-priority threshold and scaling it to other groups of DIB members accordingly over time. For example, Congress could mandate that all covered entities with a staff of at least 50 but no more than 200 people that have active contracts with the Department of Defense and deal with sensitive classified information, and do not currently have any CTH services, must submit to an initial assessment of organizational capacity for a CTH program within 180 days of the legislation passing. After the initial assessment, if proven to have the organizational capacity, these DIB members must then work in-house or with an approved third-party vendor to establish a baseline program within one year of the initial assessment. For prime contractors that already have in-house CTH programs or resources to implement, a CMMC audit in the same timeframe would be sufficient.

After a given period for pilot implementation, e.g., 2 years, the program could be expanded to include smaller covered enti-

ties, covered entities that are low-risk, covered entities that are medium-to-high risk that do not have foundational capacity to support CTH services, etc.

Reshape the punitive compliance-only mentality by providing a carrot and stick approach

Field experts from the government, private sector, and academia have indicated that the punitive approach to compliance in the sector is a prominent barrier to successfully implementing a government-mandated CTH program. Imposing high costs on smaller DIB members entities that lack capability will not suddenly make them more capable, nor will it necessarily deter larger covered entities that can afford to pay the costs without significant effect on business operations. While punitive action will certainly remain an important component of compliance, especially for mid-sized organizations, we recommend a balanced approach that provides incentives. Our research found a number of ways in which the government can create a carrot-and-sticks approach to a mandated CTH program. This program could implement components such as sliding scale fee rates for covered entities that do not meet implementation requirements, withholding government contracts after prolonged risk-exposure, grading standards awarded by CMMC, tax incentives, and subsidies.

Incentivize information sharing as a complementary component to threat hunting

A final policy recommendation to support a mandated threat hunting program is to first incentivize information sharing as a complementary component. The CSC 6.2.1 recommendation calls for establishing a mandatory cyber-intelligence sharing program across the DIB. Participation in current intelligence-sharing programs has been voluntary and asymmetric. As a result, there is not enough reliable information on threats DIB firms face to efficiently utilize a hunt. CTH requires prior knowledge of the risk environment to optimally hunt for potential attacks. Establishing an intelligence platform first would facilitate the creation of a threat hunting program later. A mandated intel-sharing program would directly complement a threat hunting program's robustness.

SERVICE MODEL RECOMMENDATIONS

Regardless of the status of a government-mandated program, any CTH service model for a third-party provider like PwC must be adaptable to the specific requirements of the DIB. Most relevant is accounting for the various sizes and cyber capabilities across DIB members. Director for Cyber at Lockheed Martin Government Affairs MG(R) Jim Keffer states that while companies like Lockheed, Boeing, or Raytheon (the so-called "primes") can leverage extensive resources for internal cybersecurity teams, cooperate with one another and are doing well in protecting their networks, small- and medium-sized companies struggle to find a similar ability.

A lack of human capital and knowledge of advanced cybersecurity measures like CTH is also critical. Dr. Erica Borghard and DIB CERT engineers clarified that CTHaaS applies only to DIB members that are mature enough to conduct advanced cybersecurity methods (CMMC level 3 and higher), are financially capable to pay for labor-intensive CTH consulting and services, and do not (yet) have in-house capacities to conduct CTH. An exception applies to highly-capable companies where third-party providers can design niche services that fill service gaps, consult current processes with an outside perspective, or work in an auditing role that signals credibility and sophistication of cybersecurity processes. The CMMC-AB is the only entity that approves third-party vendors as auditors of CMMC compliance. PwC may seek to apply as an accredited organization to further complement legitimacy as well as contribute to future standards.

Limits	CTH-as-a-Service	Reason for (in)applicability	Type of company
Upper limit	Only for special consulting services (niche, outside role, auditing)	Conducting in-house threat hunting themselves	Primes (e.g., Raytheon, Lockheed Martin, Boeing)
Target range	Applicable	Financially capable and sufficient cyber maturity	Mid-sized companies
Lower limit	Not applicable	Lack of cybersecurity maturity or financial resources	Start-ups, small subcontractors

Figure 3: Delimiting Lower and Upper Scope of a Cyber Threat Hunting-as-a-Service Model for the DIB

Here, a third-party service model can begin: aligned with the risk-based criticality assessment that establishes a matrix model between threat level against a DIB member and its respective risk awareness, a service model can offer a range of services along the risk levels and the company-specific requirements.

At the lower end, a third-party provider can focus on advancing regular activities and operations within a Security Operations Center (SOC) and establish the groundwork for a cyber hunt process. In the middle, external providers set up a hunting process via a framework, recommending participants, and ensuring quality standards. Oriented on a standardized hunting cycle (see Appendix A), the third-party can consult the hypothesis building in workshop formats and best practices references, guide data collection and evaluation, and iteratively improve hunts through structured feedback sessions. At the highest level of service provision, a third party can "go deep"; bringing technical experts to the hunt team and addressing sophisticated threats. Ranging from company or time-specific attacks with extensive cyber threat intelligence collection to malware-specific technical support, these advanced services require extensive external expertise from the third-party provider, but can be attractive even for mature DIB members.

In addition to a standard service model, a third-party provider can offer event-based services that focus on high-risk events in the DIB such as company mergers, new contracts, or attack patterns regarding DIB-specific companies. In particular if a policy design includes event-based CTH requirements, the third-party provider can provide specific services to mitigate disruption from these events.

The different levels of sophistication of the services offered reflect in the pricing for CTHaaS that can be calculated as a combination of the anticipated hours for the project, the respective expertise of the team members and/or the size of the client and its network. Possibly in competition with public CTH services, it is recommended to seek competitive pricing in particular when addressing new clients. Appendix B provides further details on a proposed service model to include prerequisites for the third-party team, client-side participants, ideas for CTH services along a standardized hunting cycle, and outlines of service value propositions.

Conclusion

Should PwC seek to shape the future of a mandated CTH program across the DIB, our suggested third-party service model is a conservative example to follow that would allow PwC to hedge against overinvestment as well as gain insights as the DIB adjusts to new regulations. Any future mandated program is sure to raise the threshold of risk awareness across the DIB; we recommend PwC prepare for that eventuality by catering to mid-tier firms now. Critically, third-party vendors such as PwC should anchor expectations to CMMC and obtain formal accreditation once guidelines are more defined.

In summary, a mandated CTH program across the DIB faces significant challenges. Ambiguity is the greatest challenge when determining what CTH services should be offered. Immediate profitability of PwC's investment in providing these services is not guaranteed as the market is largely dependent on legislation still in development. Policy remains fluid due to the sheer scope of DIB firms—prime and subcontractors. Drafting regulations that fully insure against security risks while maintaining flexibility to avoid needless burdens for resource-scarce DIB firms is difficult.

A cost-resistant industry and a tightening of cybersecurity regulations has led to an oversaturation of CTH providers. This compounds the problem of defining adequate standards that will inhibit policy and profitability of PwC-provided CTH services. Until further legislation is defined, forecasting market potential would not be prudent. The only conclusion that can be drawn currently is that the market for CTH will certainly exist in the future as the government rolls out CMMC standards.

Appendices

Appendix A: Definitions and relevant stakeholders

Appendix B: Details for a third-party service model

Appendix C: Proposed legislative language for a mandated CTH program

APPENDIX A: DEFINITIONS AND RELEVANT STAKEHOLDERS

CERT | Computer Emergency Response Team, a group of IT and cyber professionals who respond to cyber incidents within an organization.

Covered Entity | Any entity in the defense industrial base that performs research and development, designs, produces, delivers, and maintains military weapon systems, subsystems, components, or parts to meet military requirements and currently holds a Department of Defense contract that requires a cybersecurity maturity model certification.

CMMC-Accreditation Body (CMMC-AB) | Entities that approve third-party vendors as auditors for CMMC compliance.

Cyber Threat Hunting | The process of proactively and iteratively searching through networks to detect and counter tactics, techniques, and procedures of advanced attackers that evade existing security solutions.

Cybersecurity Maturity Model Certification (CMMC) | A cyber security certification process required for DIB members. Audits firms according to 5 levels of ascending controls.

Cyberspace Solarium Commission (CSC) | A bipartisan commission established by Congress to develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences.[14]

Cyberspace Solarium Commission Recommendation 6.2.2 | CSC recommendation to require cyber threat hunting on Defense Industrial Base networks.

Cyberspace Solarium Commission Recommendation 6.2.1 | Recommends a requirement for DoD to establish a DIB cyber threat information sharing program.

Cyber Threat Hunting as a Service (CTHaaS) | Cyber Threat Hunting sold as a service by third-party providers.

Defense Industrial Base | A wide-ranging and complex group of companies that produce products and services that enable the DoD's warfighting capabilities.

Defense Federal Acquisition System (DFARS) | System that governs private-sector compliance in obtaining federal contracts.

The National Defense Authorization Act (NDAA) of 2021 | Annual act specifying budget and appropriations for the DoD. The 2021 NDAA includes provisions for DoD to research feasibility of CSC recommendation 6.2.2.

National Institution of Standards and Technology (NIST) | A non-regulatory agency of the United States Department of Commerce.

National Technology Industrial Base (NTIB) | Entities within the domestic DIB and some global DIB members who provide technology services to the U.S. national security enterprise.

[14] H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 https://www.congress.gov/bill/115th-congress/house-bill/5515/text

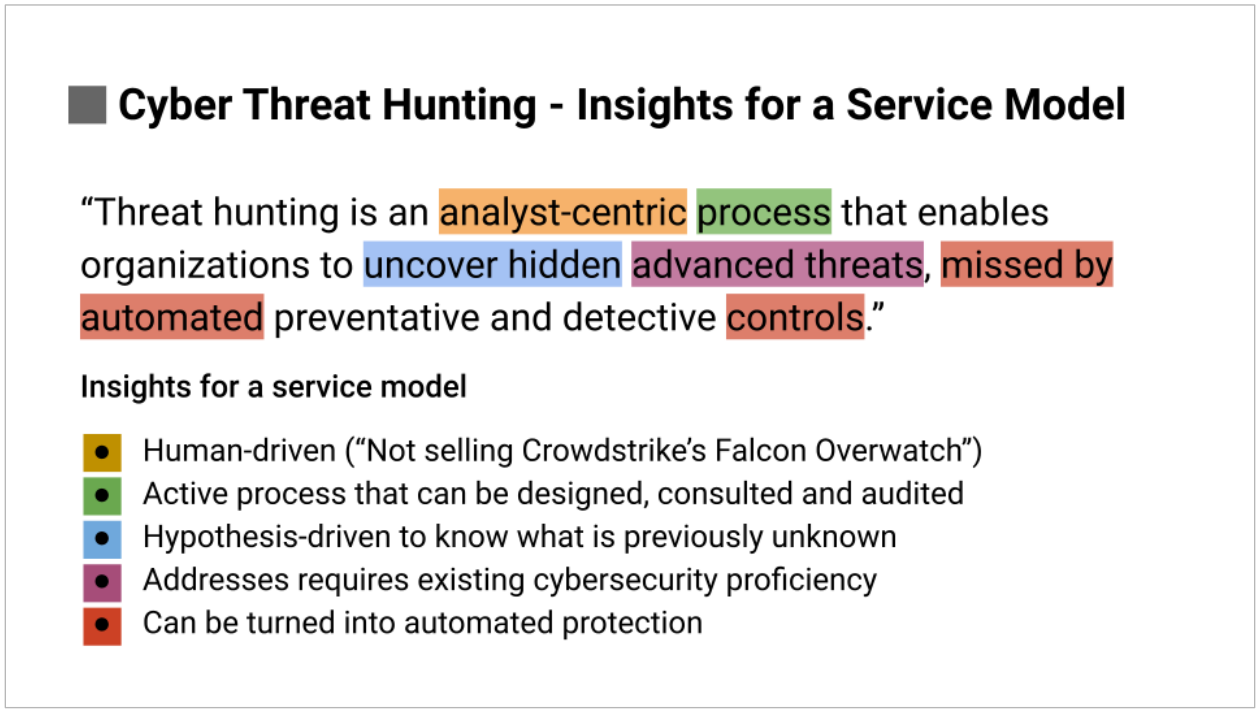
NIST 800-171 | Recommended requirements for the threshold of cybersecurity a contractor and any subcontractors must comply with when fulfilling a federal defense contract.

Service Provider | Third-party vendors with the capabilities to provide cybersecurity services.

Security Operations Center (SOC) | A facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis.

APPENDIX B: DETAILS FOR A THIRD-PARTY SERVICE MODEL

This section provides details on a third-party service model that were derived from the conducted interviews and existing consulting approaches and reports. It focuses on the team composition on provider and client side, consulting services along the hunting cycle and value propositions.



Human-driven Approach: The Right Team

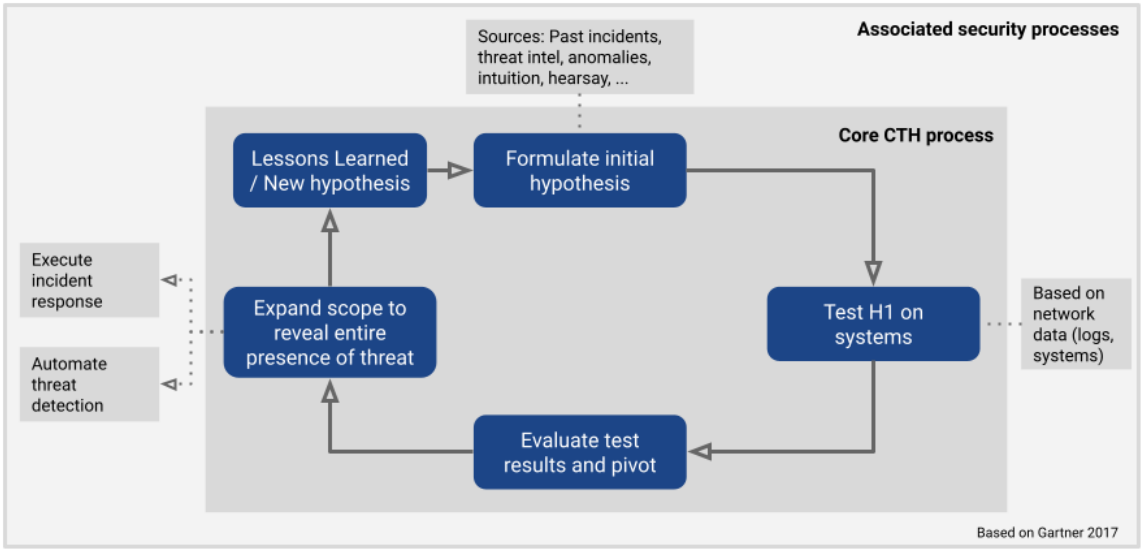
Client team:

- Interdisciplinary teams
- Minimum representation of
  - CERT
  - SOC
  - CTI (?)
  - Log/IDS expert
- Mixture of tech and non-tech
- Ideally: Mixture of experienced hunters and newbies

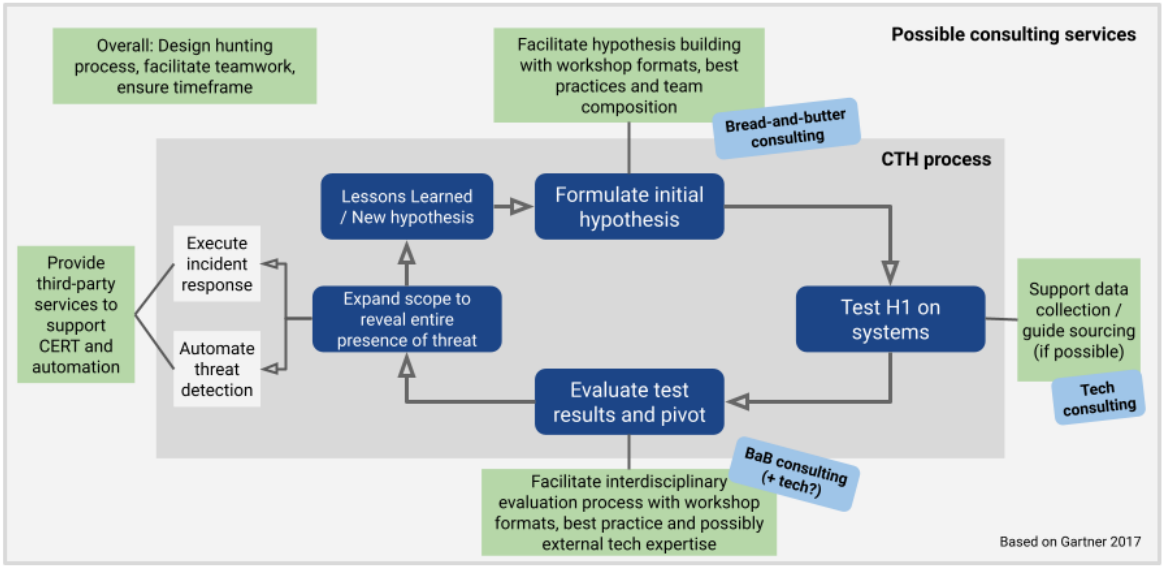
Consulting team:

- Process moderation
- Network expert
- Maybe: Data Scientist (explore log/sensor data)
- Additionally: CERT people

A Standardized Cyber Threat Hunting Process



Consulting the Hunting Process



Designing, Consulting, Auditing | Service Overview

- Workshop development:
  - Hypothesis workshops & methods ("What are we afraid of?")
  - Update workshops ("What going on in CTI?")
  - Evaluation workshops & methods ("Is this normal?")
- Timing & Coordination: Weekly, bi-weekly, monthly hunts with X iterations
- Team composition: Big hunt (interdisciplinary) vs small hunt (specialists), tech v. non-tech interaction, outside expert input
- Feedback process:
  - Content-driven for new hunts
  - Process-driven for what can be improved next time
- Training services:
  - CTH expert training
  - Current CTI
  - Incident Response handling
- Audit the hunt / Certification of hunts or hunting teams

Potential Clients

- Need to fulfill a minimum cybersecurity standards
  - CERT/SOC team
  - CTI routines, even if only via information exchange
  - Log and sensor analysis
- Must face an advanced threat of intrusions
- Must have capacity handle results of a hunt

→ Majority of DIB members fulfills requirements

More Services

- Data science: Collect, process and evaluate logs and sensor data
- Provide IDS, SIEM, EDR system and/or update routines with new threat detection (e.g., in cooperation with CS/FE)
- Provide CERT support in case of intrusion
- Extension of the other currently provided consulting services (management / technical)

Service Value Propositions as CTHaaS Provider

1. Design, implement and consult hunting process OR audit and consult current process
2. Provide insights from CTH at other companies
3. Increase accountability through external role and standardization

APPENDIX C: PROPOSED LEGISLATIVE LANGUAGE FOR A MANDATED CTH PROGRAM

HR 6395 National Defense Authorization Act for Fiscal Year 2021

SEC. 1634. DEFENSE INDUSTRIAL BASE CYBERSECURITY THREAT HUNTING AND SENSING, DISCOVERY, AND MITIGATION.

(a) Definition.—In this section:

(1) DEFENSE INDUSTRIAL BASE.—The term "defense industrial base" means the worldwide industrial complex with capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

(2) ADVANCED DEFENSE INDUSTRIAL BASE.—The term "advanced defense industrial base" means any entity in the defense industrial base holding a Department of Defense contract that requires a cybersecurity maturity model certification of level 4 or higher.

(b) Defense Industrial Base Cybersecurity Threat Hunting Study.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a study of the feasibility and resourcing required to establish the Defense Industrial Base Cybersecurity Threat Hunting Program (in this section referred to as the "Program") described in subsection (c).

(2) ELEMENTS.—The study required under paragraph (1) shall—

(A) establish the resources necessary, governance structures, and responsibility for execution of the Program, as well as any other relevant considerations determined by the Secretary;

(B) include a conclusive determination of the Department of Defense's capacity to establish the Program by the end of fiscal year 2021; and

(C) identify any barriers that would prevent such establishment.

(c) Defense Industrial Base Cybersecurity Threat Hunting Program.—

(1) IN GENERAL.—Upon a positive determination of the Program's feasibility pursuant to the study required under subsection (b), the Secretary of Defense shall establish the Program to actively identify cybersecurity threats and vulnerabilities within the information systems, including covered defense networks containing controlled unclassified information, of entities in the defense industrial base.

(2) PROGRAM LEVELS.—In establishing the Program in accordance with paragraph (1), the Secretary of Defense shall develop a tiered program that takes into account the following:

(A) The cybersecurity maturity of entities in the defense industrial base.

(B) The role of such entities.

(C) Whether each such entity possesses controlled unclassified information and covered defense networks.

(D) The covered defense information to which such an entity has access as a result of contracts with the Department of Defense.

(3) PROGRAM REQUIREMENTS.—The Program shall—

(A) include requirements for mitigating any vulnerabilities identified pursuant to the Program;

(B) provide a mechanism for the Department of Defense to share with entities in the defense industrial base malicious code, indicators of compromise, and insights on the evolving threat landscape;

(C) provide incentives for entities in the defense industrial base to share with the Department of Defense, including the National Security Agency's Cybersecurity Directorate, threat and vulnerability information collected pursuant to threat monitoring and hunt activities; and

(D) mandate a minimum level of program participation for any entity that is part of the advanced defense industrial base.

(d) Threat Identification Program Participation.—

(1) PROHIBITION ON PROCUREMENT.—If the Program is established pursuant to subsection (c), beginning on the date that is one year after the date of the enactment of this Act, the Secretary of Defense may not procure or obtain, or extend or renew a contract to procure or obtain, any item, equipment, system, or service from any entity in the defense industrial base that is not in compliance with the requirements of the Program.

(2) IMPLEMENTATION.—In implementing the prohibition under paragraph (1), the Secretary of Defense shall prioritize available funding and technical support to assist affected entities in the defense industrial base as is reasonably necessary for such affected entities to commence participation in the Program and satisfy Program requirements.

(3) WAIVER AUTHORITY.—

(A) WAIVER.—The Secretary of Defense may waive the prohibition under paragraph (1)—

(i) with respect to an entity or class of entities in the defense industrial base, if the Secretary determines that the requirement to participate in the Program is unnecessary to protect the interests of the United States; or

(ii) at the request of such an entity, if the Secretary determines there is a compelling justification for such waiver.

(B) PERIODIC REEVALUATION.—The Secretary of Defense shall periodically reevaluate any waiver issued pursuant to subparagraph (A) and revoke any such waiver the Secretary determines is no longer warranted.

(e) Use Of Personnel And Third-Party Threat Hunting And Sensing Capabilities.—In carrying out the Program, the Secretary of Defense may—

(1) utilize Department of Defense personnel to hunt for threats and vulnerabilities within the information systems of entities in the defense industrial base that have an active contract with Department of Defense;

(2) certify third-party providers to hunt for threats and vulnerabilities on behalf of the Department of Defense;

(3) require the deployment of network sensing technologies capable of identifying and filtering malicious network traffic; or

(4) employ a combination of Department of Defense personnel and third-party providers and tools, as the Secretary determines necessary and appropriate, for the entity described in paragraph (1).

(f) Regulations.—

(1) RULEMAKING AUTHORITY.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall promulgate such rules and regulations as are necessary to carry out this section.

(2) CMMC HARMONIZATION.—In promulgating rules and regulations pursuant to paragraph (1), the Secretary of Defense shall consider how best to integrate the requirements of this section with the Department of Defense Cybersecurity Maturity Model Certification program.