Final Cyber Threat Intelligence Proposal

John McGovern

CSOL580 - Cyber Intelligence

February 28th, 2022 - Spring 2022

Professor Biedermann

Cyber Threat Intelligence Plan

Prepared for the Processor Design Corporation

Prepared by John McGovern

February 2022

Table of Contents

Executive Summary

Cyber Threat Intelligence (CTI) is the cybersecurity function of learning as much as possible about the threats, threat actors, and techniques these groups use to better prepare and protect the organization against threats. By following the intelligence lifecycle of planning, collecting intelligence, analyzing the collected intelligence, putting this information into action in production, and reviewing outcomes, the Processor Design Group (PDC) can engage in a continuous improvement model. This model aims to allow the organization to be proactive in their cybersecurity efforts rather than just being reactive to circumstances and attacks as they occur. A Cyber Threat Intelligence Program allows the PDC cybersecurity team and leadership to make better-informed decisions when addressing cyber threats inside the organization. Further, it allows PDC leadership to strategically apply resources to the areas needed to offer the organization the best opportunity to thwart emergent threats and threat actors.

This report addresses multiple breaches, threats, threat actors, and delivery methods as examples of the kind of information an organizational CTI capability would provide. The breaches discussed are the Maersk NotPetya breach, JBS Foods ransomware attack, and the Kaseya software supply chain compromise. Each of these breaches is evaluated using the industry-standard Lockheed Martin Cyber Kill Chain® (CKC) methodology. The CKC provides a de-facto standard vocabulary for discussion attacks using a seven-step model. The seven steps are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives (CrowdStrike, 2021). Using this model, attacks can be classified and compared, and measures can be implemented along each step of the chain to make a successful breach more difficult and costly for the adversary.

This report proposes funding a cyber threat intelligence program using a threat intelligence management (TIM) system. A threat intelligence management system acts as the centerpiece of the CTI practice and is the database of record for CTI analysts. The TIM aggregates digital indicators of compromise (IoCs) from sources such as commercial and open-source threat intelligence feeds. IoCs include suspicious Internet Protocol (IP) addresses, web domain names, and file fingerprints (digital hashes). When an IoC is received from a trusted source, it can be blocked across all PDC systems, such as next-generation firewalls and endpoint protection software. The goal of this system is that an attack can only be attempted once. A single threat feed can make many organizations aware of the issue to immediately block future attempts using the same indicators.

After careful evaluation, the Recorded Future TIM solution has been chosen for the organization. Its module architecture will allow PDC to expand with the solution in the future as needed. Over the PDC standard three-year product lifecycle, the total cost of ownership is $816,500. The solution is expected to save $1,013,500 in costs avoided leading to a 2.24x return on investment over the same three-year lifecycle, using industry-standard breach cost metrics.

Launching a cyber threat intelligence program centered around a threat intelligence management solution with dedicated personnel represents a specific solution to improve the PDC cybersecurity practice. Outcomes will be measured based on positive matches on the system as a proxy for system efficacy. Given that the system is deployed as a cloud-hosted service, the project is achievable and realistic based on what similar-sized organizations have accomplished. It fills a timely need for the organization. Cyber threat intelligence is the ideal initiative for the cybersecurity group to pursue at this stage in the group’s maturity and capability level.

1 Introduction to Cyber Threat Intelligence

Given the ubiquity of computers systems and digital devices used to process and store information critical to the operations of a business, cybercrime crime and cybercriminals are an ongoing concern for most modern organizations. These organizations spend a significant and growing amount of time and resources implementing security controls. Professionals do their best to mitigate threats through improvements to cybersecurity standards, systems, and knowledge throughout the organization. However, a more proactive approach is required in a world of limited time and resources to devote to address security challenges. Cyber Threat Intelligence (CTI) helps organizations make better decisions concerning prioritizing these resources against the wide variety of threats and threat actors who would seek to do them harm in the digital domain.

Due to its large repository of intellectual property (IP), extensive digital presence, and valuable stores of customer and employee information, the Processor Design Corporation (PDC) is a prime target for a wide variety of entities who would seek to benefit from the theft and destruction of corporate digital assets. Rather than respond defensively after attacks inevitably occur, the PDC cybersecurity group aims to take a forward-thinking approach to understand, prioritize resources against, and mitigate threats proactively.

The following Cyber Threat Intelligence Plan (CTIP) exists to outline the helpful role that cyber threat intelligence serves in the organization. Provided examples of CTI information include a previous breach case study and two post-mortem analyses of attacks on other companies. This type of information demonstrates the type of collateral PDC leadership can receive through the expanded operation of the CTI program and execution of the provided plan. Finally, this plan recommends S.M.A.R.T. steps (specific, measurable, achievable, realistic, and

timely) for the organization to expand CTI program efficacy and return value in the form of attack surface reduction and proactive threat mitigation.

2 Cyber Threat Intelligence Plan

2.1 Cyber Threat Intelligence Plan: Purpose & Goals

A Cyber Threat Intelligence Plan is critical to organizations that operate at scale and choose to leverage knowledge of their cyber adversaries to improve cyber security resiliency and decision making. Therefore, the PDC has chosen to adopt such a plan to guide the adoption and use of cyber threat intelligence. The document and the accompanying presentation explain the purpose and goals of the CTIP and CTI program in general and then outline the CTIP cyclical model used to operationalize threat intelligence within the organization.

PDC's greatest asset is its intellectual property (IP). Adversaries worldwide are unfortunately interested in gaining access to that IP and make attempts to do so daily. In addition, PDC possesses significant repositories of valuable operational, human resources, and financial data. Any cyberattack or data leakage caused by an external threat group could result in a major loss to PDC. Rather than simply standby and wait for attacks in hopes that existing cybersecurity controls will be enough to detect and prevent them, the PDC CTIP takes a proactive approach to understanding threats, threat groups, and adversary tactics under the conviction that this information will allow the PDC cybersecurity team to better prioritize resources and block most low-level and repetitive attacks automatically.

Various types of threat actors (adversaries in the cybersecurity domain) exist worldwide. These can be broadly divided into three categories: hobbyists, criminal organizations, and state-sponsored entities. Hobbyists, while annoying, present the lowest level of threat to the organization. Their aims are often reputational or low-level financial gain. Cybercriminal threat

actors attack networks for profit by using extortion and ransom. They often want to be discovered. On the other hand, Nation-state groups are often the most sophisticated and well-funded. They may be joined to a nation-state military organization. Rather than draw attention to themselves, they may simply seek concealment while they siphon up intellectual property data for months or years (Grimes, 2020).

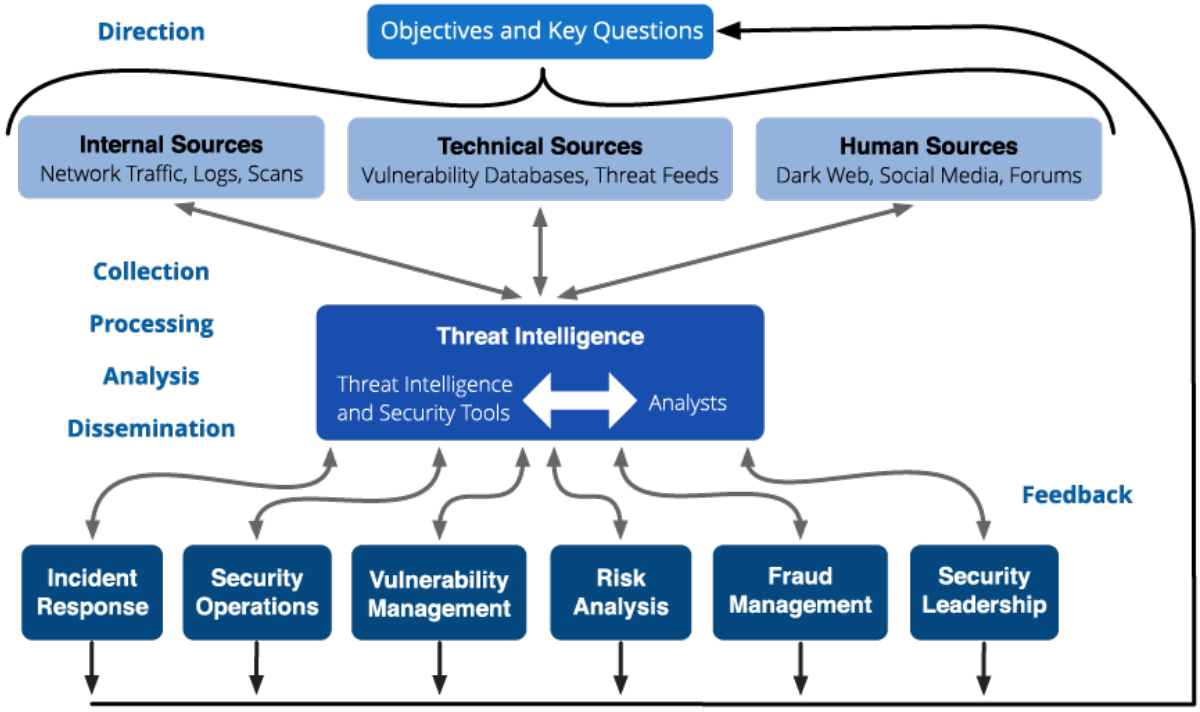
Much like legitimate corporations, various threat actors have their own sets of "intellectual property" in the form of tactics, techniques, and procedures (TTPs) that they use against other organizations (Daszczyszak et al., 2020). They may use specific malware packages, programming languages, concealment methods, and infrastructures to operate their criminal organization. APT29 is one such group that specifically targets technology companies amongst others and is nation-state sponsored. This group uses many of the same tools such as dynamic DNS entries, Visual Basic and Python coding, PowerShell scripting, HTTP exfiltration, and various obfuscation methods to execute attacks (MITRE, n.d.). This threat actor is one of many the CTIP proposes to study but is a model group for the program.

Indicators of compromise (IoCs) and the database-like systems that manage them, such as threat intelligence management (TIM) software, are in many ways the core language of the cyber threat intelligence effort. Each digital connection, whether malicious or not, leaves various pieces of data behind, such as Internet Protocol (IP) addresses, domain names, and file names/hashes, as well as various keys and text strings (Trend Micro, n.d.). While many of these pieces of data are harmless, some indicate something has gone wrong. By searching corporate systems for these indicators and blocking them using automated systems, PDC can work to ensure that a given attack is only viable once. IoCs can be sourced internally as well as from open-source and commercial threat intelligence feeds.

2.2 Cyber Threat Intelligence Plan: Lifecycle

This plan proposes a cyclical process that is used within the CTIP to continuously improve intelligence program accuracy and effectiveness. The planning phase of the program initially identifies what types of intelligence are collected and for what purpose. Focus is initially limited to a few prioritized efforts. The collection phase takes the intelligence targets from planning and begins to build a database of potential IoCs. Collection is performed by a variety of systems such as next-generation firewalls (NGFWs), endpoint monitoring software, intrusion detection systems, honeypots, and others, depending on the type of intelligence required. In the analysis phase, the cybersecurity groups use manual and automated techniques to comb through the collected data and mark certain indicators as malicious. IoCs may be scored and prioritized based on their relevance to PDC. In the production use (operationalization) phase, automation is used to block known indicators of malicious activity based on the analyst's work. Automation reduces time to contain a given identified threat and saves analyst effort, resources, and burnout. After a defined observation period, the results of the initial cycle are reviewed in the reporting phase. Lessons learned are gathered based on efficacy data and the impact of the CTIP implementation is highlighted where appropriate. Finally, the group returns to the planning phase to start the cycle again. However, each subsequent cycle, they are armed with more information about what types and sources of intelligence are most effective for the organization and how the next cycle can be more impactful to business objectives (Recorded Future, 2020).

Figure 1: Recorded Future Threat Intelligence Lifecycle Diagram



(Recorded Future, 2020)

3 Threats, Threat Actors, & Methods of Delivery

The Processor Design Corporation faces threats from a wide variety of external threat actors and groups with a variety of motivations, levels of sophistication, and capabilities at their disposal. Understanding these facets of various threats, threat groups, and methods of delivery available to the attacker is foundational to a CTI program. When the organization understands the nature of possible attacker motivations, methods, and behaviors, it can better align decisions and resources to mitigate threats to the business.

The following sections use the Lockheed Martin Cyber Kill Chain® (CKC) framework to help describe the lifecycle of an attack against an organization using industry-standard terms in a stepped framework. Three examples are included to demonstrate the types of proactive

intelligence that can be gathered from attacks against other organizations in a variety of verticals and market segments. The PDC CTI program can collect, analyze, and integrate information such as that highlighted in the following sections. In addition, the CTIP calls for the collection of intelligence on competitive companies (adversarial assessments) to better understand organizations with similar and overlapping technologies and market positioning. The collection of competitive intelligence must be done ethically using open-source data available publicly. This collection methodology is discussed more below.

3.1 Introduction: Lockheed Martin Cyber Kill Chain® Framework

The Cyber Kill Chain® (CKC) is a model developed in 2011 by the Lockheed Martin Corporation. It describes the steps or stages that an attacker would need to pass through to execute a successful attack on a given organizational target. These steps are provided sequentially, but some attacks may skip or bypass steps in modern attacks. The Kill Chain framework is a helpful reference for organizational cyber defenders to align products, controls, and mitigations. By mapping the entity to a step or steps, the analyst can better understand where the product fits into defending against attack executions. If the organization can thwart the attacker at any one of the steps, they can reduce the harm to the organization or, in early cases, completely mitigate against it (CrowdStrike, 2021). The Kill Chain model was built specifically to defend against a category of attack known as an advanced persistent threat (APT). This threat type and threat actor is focused on long-term strategic attacks that persist for months or years at the hands of dedicated adversaries (Lockheed Martin, n.d.)

Figure 2: Lockheed Martin Cyber Kill Chain® Diagram

(Lockheed Martin, n.d)

3.2 Case Study: Maersk NotPetya Attack

The case study below provides an in-depth review of the NotPetya malware that caused the Maersk organization and many other companies hundreds of millions of dollars in damage. Given the notable success of this campaign in causing damage to companies worldwide, it is worth understanding and implementing countermeasures against similar attacks. Of particular

interest are the geopolitical nature of the threat actor and particularly insidious delivery methods used to conduct the attack.

3.2.1 Maersk - Overview

Maersk is a large container shipping and logistics corporation that employs approximately 95,000 people and US$61 billion in total revenue in 2021 (Yahoo, 2022). On June 27th, 2017, the corporation was hit with a then-unknown cyberattack that propagated rapidly throughout the network, rendering devices unusable (Greenberg, 2018). Upon reboot, devices would display a message stating that important files had been encrypted and demanding a ransom (Sood & Hurley, 2017). The worm known as NotPetya was not ordinary ransomware, however. It was, in actuality, a sophisticated cyberweapon created by Russian threat actors targeting Ukrainian corporations, many of which use the M.E.Doc tax preparation software (similar to TurboTax in the Unites States) (Greenberg, 2018). All told, the NotPetya cyberweapon is thought to have caused at least US$10 billion in damages to corporations around the world (not just those in Ukraine).

3.2.2 Maersk - Kill Chain Alignment

The Lockheed Martin Cyber Kill Chain (CKC) comprises seven steps ordered sequentially to map to the proposed attack lifecycle. These steps are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. In the initial reconnaissance phase, the Russian Cozy Bear and Sandworm groups identified that the M.E.Doc Ukrainian tax software was vulnerable and commonly used by their targets. Therefore, it represented a potential software supply chain attack vector to execute additional CKC steps (Greenberg, 2018).

In the weaponization step, a modified version of the M.E.Doc software was produced to include the various software packages and tools used by the malware. These included code to exploit various Windows vulnerabilities and to replicate to other systems (Nzeata, n.d.).

The delivery step involved the NotPetya malware being uploaded to the M.E.Doc software update servers that were normally used to automatically push valid software updates to various customers. However, the new update appeared to be from a trusted system, and as such, delivery of malicious software was not suspected (Nzeata, n.d.).

In the exploitation phase, NotPetya was executed on the victim system. In some ways, this execution phase was unusually pernicious as it did not require the initial exploitation of a vulnerability in the system to run. The delivery phase had bypasses many traditional defenses, and the software is thought to be the valid M.E.Doc product (Greenberg, 2018).

In the installation phase, NotPetya goes to work leveraging the EnternalBlue vulnerability and the Mimikatz toolkit to infect other systems on the same network as the original victim computer. It is important to note that only one system was thought to be running the M.E.Doc software within Maertz (Greenberg, 2018). The software could find systems vulnerable to the U.S. National Security Administration (NSA) developed EternalBlue storage exploit and infect other systems using these additional exploits. On each infected system, an attempt was made, using Mimikatz, to dump valid Windows credentials from computer memory. This allowed NotPetya to infect even systems that were not vulnerable to EternalBlue, significantly broadening the attack's ability to damage Windows devices and servers (Hypr, n.d.).

The command-and-control phase is largely not applicable to the NotPetya worm as it was built to replicate indiscriminately, do as much damage as possible, and erase its tracks and the tracks of the authors. This may have been to cover up previous exploits. Although NotPetya

masqueraded as ransomware (which would have required a command-and-control channel), it, in reality, was generating random strings which could be used to decrypt data in question (Hypr, n.d.).

Finally, in the action on objectives phase, the worm irrecoverably encrypted the master file table that stores required metadata about storage on the impacted device. The device could not operate without this information, and data would be largely useless. The install and erase process would continue for all systems that could be accessed through the EnternalBlue exploit or the Mimikatz password dumping methodology (Nzeata, n.d.). As companies often use directory services such as Microsoft Active Directory to allow the same user to login to multiple systems, widespread damage occurred to many organizations, including Maersk.

3.2.3 Maersk - Summary

At least two months had gone from the first Maersk system exploitation to full recovery (Pownall, 2021). It is certainly plausible that the NotPetya cyberweapon had taken years before that to develop and deploy. The restoration efforts against it involved hundreds of Maersk employees and contractors. Damages to the corporation were stated to be US$300 million, although this certainly could be a low estimate (Greenberg, n.d.). Proper patching and security controls such as disabling legacy storage services and segmenting networks could have prevented much of the damage caused by NotPetya for the prepared organization. Even if a few systems were infected, the worm would not have caused as much damage.

By looking through this and other attacks using the Cyber Kill Chain lens, PDC and other organizations can learn from the history of the world's worst cyberweapons and prepare, at each step, to mitigate the same and similar APT patterns. While not all attacks map neatly against the

Kill Chain, many do, and the shared vocabulary used within is of value to the cybersecurity team within the organization.

3.3 Post-Mortem: JBS Foods Breach

JBS Foods Group is the world's largest meat processing corporation and has locations worldwide (NPR 2021; JBS Foods, n.d.). In 2021, JBS was the victim of a ransomware campaign against its facilities in Brazil and Australia (Sherstobitoff, 2021). The U.S. Government, through the Federal Bureau of Investigation (FBI), has attributed the ransomware attack to the REvil threat actor. The REvil group is a Russian-speaking actor known for conducting several high-profile campaigns against domestic and global companies (NPR, 2021).

As with many prominent attacks against large organizations, some of the details as to the nature of the campaign are unknown. This is understandable as the organization seeks to protect information about its vulnerabilities and security posture.

The initial attack against JBS is thought to have been a targeted attack specifically against the Brazilian portion of the company for geopolitical motivations based on captured intelligence. Reconnaissance would have been conducted accordingly against the organization to find any weaknesses or points of entry. Although not confirmed by JBS, a compromised set of user credentials to a device on the JBS network was thought to be the initial point of entry. The ransomware involved in this specific attack is thought to be the Sodinokibi ransomware package that the REvil group has used in the past (Sherstobitoff, 2021). The capabilities of the ransomware/malware used are of specific interest in the exploitation and installation CKC phases in which the hacker uses their specific set of tactics, techniques, and procedures (TTPs) to gain persistent access to the target. This package is typically used to establish a CKC command and control channel, encrypt assets on one or more systems and notify the victim how to pay the

ransom in question. An attempted attack can be thwarted in the delivery, exploitation, installation, or command and control phases. However, responding to the breach is simpler the sooner the attack can be interdicted.

Actions on objectives is the last step the attacker needs to accomplish their goals. Often, and specifically in the JBS Foods case, the action is positioning themselves to receive payment. In the end, JBS paid the ransomware group $11 million (USD) to "mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated (JBS Foods, 2021)." Some sources indicate that data was indeed exfiltrated, which may have laid the foundation for a double extortion scenario. Double extortion schemes occur when an attacker charges for both the delivery of encryption keys to decrypt data and for promises that exfiltrated sensitive data will be deleted permanently (Agcaoili et al., 2021). It is plausible that the threat of releasing sensitive data caused JBS to provide payment to the threat group.

3.4 Post-Mortem: Kaseya Breach

The July 2nd, 2021 Kaseya breach differs from the JBS breach in that it was an attack on the software supply chain of a company whose primary business is to provide information technology systems management software to its customers. These customers are often Managed Services Providers (MSPs) that, in turn, handle the management of 3rd party systems for a fee. Given the business model, a breach in the Kaseya VSA (virtual system administrator) software has implications well beyond a single company. However, both breaches share an interesting common thread in that the REvil ransomware threat group is thought to be behind both 2021 attacks.

It is unclear how REvil discovered the initial vulnerability in the Kaseya software, but it is plausible to assume it was during their own reconnaissance efforts. The Kaseya software is

now known to have been vulnerable to attack since at least April 2nd, 2021, when a Common Vulnerabilities and Exposures (CVE) entry was initially filed in the industry-standard CVE database. In addition, another CVE entry dated back to July 2015 detailed an issue with the Kaseya portal in which data could be extracted through a common “directory traversal” issue (Krebs, 2021). These vulnerability disclosures may have helped the threat group target their attack.

Once the vulnerability was discovered, REvil used capabilities built into the Kayesa VSA software to expedite the attack's delivery, exploitation, and installation phases. The VSA agent operated with administrative privileges on each system it was deployed on to perform tasks such as managing user accounts and deploying software. As such, the threat actor deployed a variant of its Sodinokibi ransomware toolkit using means that a normal administrator would have used to deploy software patches (Sason, 2021). Therefore, no direct system exploitation was required, and installation occurred through standard methods. This is why supply chain attacks against systems administration software are so pernicious and difficult to detect. Command and control (C2) and action on objective were typical of this threat group. In both cases, they use C2 traffic to communicate compromised target information and decryption keys back to the attacker's system. Action on objectives occurred when the affected MSP customers received notification that they were compromised. Given the zero-day nature of the vulnerability (it had not been publicly disclosed), vulnerable MSPs and customer organizations were in a race to turn off on-premises Kaseya management servers. Kaseya hosted many of these systems in their software-as-a-service offering and also brought the systems offline to prevent them from being used to install malware (Osborne, 2021).

Although the command and control and actions on objective CKC phases were similar in both the JBS Foods and Kayesa ransomware attacks, the means of delivery, exploitation, and installation were customized by REvil to impact each target. Having a toolkit at the ready such as REvil's Sodinokibi means that the attacker can progress quickly through the weaponization phase when reconnaissance discovered delivery and exploitation opportunities present themselves.

3.5 Post-Mortem: Lessons Learned

Both breach post-mortems present ample learning opportunities for the PDC cybersecurity team. It is helpful to walk through the lifecycle of both attacks to identify solutions to interdict the attackers in as many ways as possible. While no solution is perfect, a defense-in-depth approach is always preferred. If the attackers can be stopped at any given security control point, significant damage to the organization can be prevented.

The Center for Internet Security publishes a helpful list of their top 18 recommended security controls that should be applied to help secure the enterprise. Account management and access control management are listed as CIS Control 5 and 6, respectively (CIS, n.d.). Both REvil attacks serve as reminders of the importance of these control in managing credentials and access. In both cases, monitoring for unusual usage of privileges and ensuring that all accounts used secure multi-factor authentication (MFA) may have helped prevent the attacker from delivering an exploit to the corporations in the first place.

CIS Control 7 is Continuous Vulnerability Management (CIS, n.d.). In the case of the Kaseya attack, multiple vulnerabilities had been discovered and reported through the CVE process. Once a vulnerability is discovered and reported, it is reasonable to assume an attacker has already or will soon make the same discovery. The time taken by the Kaseya team to patch

vulnerabilities in their software and systems (more than two months) was unacceptable given the nature of the software the company produced and the threat of a successful compromise to the organization. An organization must have a program to continuously find and mitigate vulnerabilities in their systems in order of their severity.

One of the unknowns in both cases was the extent to which JBS and Kaseya had employed log management and analytics. CIS Control 8 is Audit Log Management (CIS, n.d.). Active log monitoring and analytics with detections to prevent common threats is a best practice and can significantly improve the mean time to discover and respond to a security threat. For example, a monitoring system should alert a team of analysts if an account is accessed from an abnormal location or Internet Protocol (IP) address. Similarly, a system asking to run new software as an administrator or disable system security protections should immediately generate alerts.

CIS Control 10 is to implement Malware Defenses (CIS, n.d.). In a perfect world, these defenses would serve only as a last stop-gap measure and should not be needed. However, sophisticated endpoint protection software (for employee devices and servers) is a requirement, given the current threat landscape. This software acts as a last line of defense in preventing the types of behavior commonly seen in ransomware attacks, such as executed using REvil's Sodinokibi software. Preventing malicious execution and immediately alerting the team can mean the difference between a close call and a full-blown breach leading to millions of dollars in remediation costs. Endpoint protection software alerts can shorten the time to detect issues and help ensure other enterprise systems have not fallen victim to similar attacks.

Finally, CIS Control 17 highlights Incident Response (IR) Management as a key step (CIS, n.d.). JBS and Kaseya both seem to have responded adequately regarding their specific

incidents. Both involved government entities and 3rd party investigators (JBS Foods, 2021; Osborne, 2021). If a cybersecurity incident occurs (which is inevitable given time), having a plan of action upfront on responding to a breach is of major value. Having an IR plan with runbooks, contact lists, procedures, and other key pieces of data will influence how fast a team can respond to, contain, and address an attack. Skillsets not possessed by the company's cybersecurity team can be outsourced and available remotely when needed. In many cases, IR activities done right can help a team contain the threat of a patient zero before an attack becomes company-wide. Good planning speeds execution when it matters.

3.6 Adversarial Assessment

3.6.1 Assessment Overview

The Nvidia Corporation (often stylized as NVIDIA) is a large publicly traded technology company based in Santa Clara, California. It currently employs more than 18,000 individuals worldwide at more than 50 offices (Yahoo, n.d.; Nvidia, n.d.-c). Nvidia trades on the NASDAQ stock exchange under the ticker symbol $NVDA. At the time of this update (after close of business on February 25th, 2022), the company enjoys a market capitalization of slightly over US$602 billion. It produced approximately $16.6 billion in annual revenue as of January 31st, 2021. Referencing data compiled in 2020, Nvidia was ranked as the 9th largest semiconductor manufacturer globally, behind Intel, Samsung, Taiwan Semiconductor Manufacturing Co. (TSMC), and others (Flynn, 2021).

Nvidia was co-founded by Jen-Hsun "Jensen" Huang, Chris Malachowsky, and Curtis Priem. Of the three founders, two remain on with the company (Tilley, 2016). Huang is the current president and CEO and has been in these roles since he started the company in 1993 at the age of 30. Malachowsky is an Nvidia Fellow and member of the executive staff. Colette

Kress serves as the Executive Vice President (EVP) and Chief Financial Officer (CFO). Jay Puri serves as the EVP, Worldwide Field Operations. Debora Shoquist serves as the EVP, Operations. Tim Teter serves as the EVP, General Counsel, and Secretary (Nvidia, n.d.-b). Michael Kagan serves as the Chief Technology Officer (CTO) (Crunchbase, n.d.). Sonu Nayyar serves as the Chief Information Officer (CIO) (The Org, n.d.). Mark Vorzimmer serves as the Senior Director, Global Security (RocketReach, n.d.).

Nvidia has branched out into a wide range of revenue sources and product types centered around its core semiconductor and graphics processing unit business. These product areas include the core graphics processing unit (GPU) business which provides high-end technologies such as Ray Tracing through its RTX product line. (Nvidia, 2021). In addition, Nvidia has developed Deep Learning Super Sampling (DLSS) technology that uses machine learning and dedicated processing cores onboard RTX series GPUs to increase framerates with minimal additional load on the GPU.

Nvidia has proven that GPUs are not only for graphics processing and has innovated in several key areas where parallel processing power is important. For example, Nvidia uses its semiconductor design prowess to support computer vision workloads for smart cities, robotics, autonomous driving, and vehicle fleet command. Nvidia also produces processors for high-performance computing (HPC) workloads. In addition, Nvidia provides many software and cloud-native products to help manage GPUs and provide vGPU (virtual GPU) offerings to customers (Nvidia, 2021). Finally, specialized Nvidia CMP chips are used extensively for mining cryptographic currencies such as Ethereum (Leswing, 2021).

3.6.2 Competitive Landscape

Nvidia does present a significant competitive threat to PDC based on several key factors. First, Nvidia's product portfolio is extensive. They have entered into several strategic and potentially lucrative markets and product areas such as artificial intelligence, computer vision, computer graphics, and cryptocurrency. Additionally, Nvidia has produced software tools for devices and cloud computing to extend the functionality of their GPUs. The PDC is primarily a custom semiconductor design firm and has therefore focused its efforts up until this point on hardware design and building custom system on a chip (SoC) products that integrate general purpose and specialized graphics processing functions into custom silicon. This silicon is sourced as original equipment manufacturer (OEM) parts for a range of devices that benefit from high processing performance in a low power package (AnySilicon, n.d.). Nvidia produces similar chips for 3rd parties such as Nintendo in the case of the Nintendo Switch (Byford, 2021). The risk to PDC is that customers who use and license SoC and processor designs will increasingly turn to an organization that provides a stronger vertical integration story in that it can provide services and products, including software add-ons and developer resources, in multiple adjacent areas.

Rather than compete directly with Nvidia in the same market segments and industries, it is recommended that PDC pursue a more targeted strategy, playing to the strengths of its various partnerships. This tact is partially a factor of smaller overall company size (one-quarter the size based on revenue and headcount comparisons with Nvidia). As PDC can fabricate its own silicon, the company can aim to drive new lower power, higher performance processes to embed into customers' next-generation applications such as Internet of Things (IoT) and wearables. In addition, a renewed focus on underlying software and developer tools might allow PDC to serve additional customers in the cryptocurrency and graphics processing unit markets. Technologies

such as Ray Tracing and DLSS represent a serious competitive threat and have been marketed extensively by Nvidia to consumers (Nvidia, 2021, Nvidia, n.d.-a). As such, PDC should pursue similar capabilities and developer tools in its product suite to ensure future competitiveness. Due to its vertical integration in manufacturing and distribution, PDC can realize higher product margins to meet price points attractive to value-conscious gamers, embedded applications developers, and cryptocurrency miners.

3.6.3 Collection Methodology

All data collection was performed using open-source intelligence sources, as documented in the References section of this report. At no point were illegal or unethical means of collecting or analyzing competitive intelligence data used. Off-limits collection mechanisms include any form of hacking or computer system intrusion, dumpster diving, 3rd party employee impersonation, trespassing, or other related corporate espionage activities. Data collection in the report was published by Nvidia, posted by 3rd party analysts, or sourced from publicly available financial data. PDC employees and contractors are held to a high legal and ethical standard. As such, competitive intelligence is limited to methods that are not illegal, harmful, or unethical in dealing with other corporations. Information concerning PDC's corporate priorities and posture related to future competitive plans were supplied as confidential corporate strategy documents and through interviews with key product and engineering personnel.

4 Risk Reduction Plan

4.1 Risk Reduction Plan: Gap Analysis

The PDC cybersecurity team has identified several critical gaps in organizational cybersecurity posture and has prioritized their remediation as part of a continuous improvement project cycle. To understand the problem space, it is helpful to briefly review the concepts of

cyber threat intelligence (CTI) and threat intelligence platforms (TIP). Gartner, a leading information technology analysis firm, provides the following helpful definition: “Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject’s response to that menace or hazard (McMillan, 2013).” Without CTI, the organization must sit and wait for threats to arrive and hope that defensive measures are good enough to mitigate attacks. By employing CTI, the organization can take a proactive stance in understanding the nature of current threats and act to stop them proactively when seen on a PDC network or device. TIP is an umbrella term for various products and solution sets that allow an organization to collect, analyze, and act upon CTI information from various sources (Palo Alto, n.d.).

As PDC does not use a TIP, there are several gaps in coverage of cyber threats. First, PDC visibility into threats and indicators of compromise (IoCs) is limited to the single-vendor perspective that existing tools such as an intrusion prevention system or firewall provide. Some tools are essential in their function (such as virtual private network and endpoint monitoring software) but have no native or built-in CTI capability. This gap makes it hard to determine which connections or data points indicate malicious activity. In addition, PDC cannot integrate with threat intelligence feeds from multiple external entities (governmental and commercial) such as CISA’s threat intelligence feed and various open-source feeds provided at no cost (CISA, n.d.; Banerd, 2019).

4.2 Risk Reduction Plan: System TCO & ROI

The total cost of ownership (TCO) and return on investment (ROI) are key evaluation criteria weighted equally with technical considerations. For a system to be selected, it must be

economical to operate and more than pay for itself over the given lifecycle. The total cost of ownership of the CTI product is calculated based on a three-year product lifecycle. PDC certainly can and does extend past the three years, but a three-year cost model has proven effective for other solutions and gives visibility into ongoing cost structures.

The Recorded Future Threat Intelligence module has been chosen for this analysis. Many software vendors are moving to a software-as-a-service (SaaS) model. Recorded Future offerings follow this pattern which saves on traditional costs such as hardware purchases, operating system costs, maintenance, and server virtualization costs. PDC responsibility is limited to the high-level configuration and use of the system. Subscription fees have been provided through the Amazon Web Services (AWS) Marketplace, of which PDC is a current customer (AWS, n.d.).

At this time, PDC is interested in the base Threat User license ($50,000), purchased with the SecOps User license ($10,000), and the 3rd Party Intel License ($45,000). These three licenses are included to address all gaps found in the gap analysis phase. In total, the SaaS subscription cost for the solution is $105,000 per year. In addition, it is estimated that one full-time equivalent (FTE) is required to manage the system. This will represent two employees' half-time positions to ensure redundancy exists in the required knowledge and skillset. The PDC fully encumbered employee cost for one cybersecurity analyst is $140,000 per year. Taxes are calculated at 10% of the price of the software subscription. In addition, a one-time $50,000 charge is included for professional service and training required upon installation of the solution. The three-year cost projection is shown in Table 1 below.

Table 1: CTI Solution TCO (3-year projection)

Item	Cost
Subscription	$105,000

FTE Cost (2x 50% FTE)	$140,000
Tax	$10,500
Professional Services / Training (First year only)	$50,000
First Year Total	$305,500
Three Year Total	$816,500

The same three-year lifecycle is used to calculate both the ROI and TCO data. As shown in Table 1, $816,500 will be used to represent the three-year TCO, encompassing subscription costs, labor, taxes/fees, and services.

The PDC estimates breach costs using industry-standard data provided by the Ponemon Institute, as reported by SecureWorld (Todd, 2021). Given the most recent 2021 data, a breach for an organization in the technology sector averages $4.88 million. This project aims to prevent one major data breach per year. However, it is not reasonable to assume that any single investment has a complete or 100% role in the given mitigation. Therefore, this ROI model credits the installation of the TIP software with a 12.5% role in mitigation, and cost savings are assigned accordingly.

Table 2: CTI Solution ROI (3-year projection)

Item	Cost
3-year breach expenses	$14,640,000
TIP impact %	12.5%
TIP-credited savings	$1,830,000
TIP 3-year TCO	$816,500

3-year cost avoidance	$1,013,500
Return on Investment	2.24x

As shown in Table 2, PDC estimates a $1,013,500 cost savings and looks forward to a 2.24x return on the initial investment when considering the TCO of the solution and industry-standard breach cost data. This ROI metric was competitive with or superior to other vendors with similar capabilities.

4.3 Risk Reduction Plan: System Selection & Recommendations

Although the TCO/ROI figures are compelling, the technical advantage and gap mitigation are considered equally. The Recorded Future system was chosen for several reasons. First is that Recorded Future is exceptionally well regarded in Gartner analyst reports and peer reviews. It enjoys a generally excellent reputation in the industry and among PDC analysts (Gartner, 2022). Second, it provides a modular architecture that allows PDC to use more system components as needed in the future. These modules include integrations with security information and event management (SIEM) software, brand intelligence to monitor for domain abuse and data leakage cases, and vulnerability intelligence to highlight system vulnerabilities as they are discovered (Recorded Future, n.d.). These capabilities were lacking in several of the other vendors considered. Finally, the software can consume desired threat feeds such as those provided by governments, commercial entities, and open-source entities, as well as the information provided natively in the software.

PDC has selected the Recorded Future solution to meet gaps identified in the organization's ability to proactively identify and mitigate threats before they impact PDC business operations. Based on equally weighted TCO/ROI and technical selection components,

Recorded Future is the best option for the organization. The use of this system to collect, analyze, and act on CTI data and proactively prevent attacks will serve the organization well for the standard three-year purchase lifecycle and, hopefully, well beyond.

5 Conclusion

The Processor Design Corporation has an important opportunity to launch a Cyber Threat Intelligence Program, as discussed in this planning document. Having a CTI capability at the center of the cybersecurity group allows this team to be proactive rather than reactive in identifying and applying mitigations against threats and threat actors in the wild. As discussed in this report, having compiling intelligence on key actors and attacks can help PDC prioritize the expenditure of limited corporate cybersecurity time and resources. Through the implementation of the Recorded Future system, PDC security analysts can collect, analyze, share, and act upon various forms of collected intelligence. Integrations with the SIEM and other security control points such as next-generation firewalls and endpoint protection software ensure that indicators of compromise are blocked in an automation fashion before they can be used in the PDC environment. The ultimate goal of such a capability is that a known attack, when seen by any of the threat feeds used by PDC, will fail. For the threat actor, this dramatically raises the cost of a successful attack. This capability also filters out the noise of known threats for the cybersecurity team and allows analysts to spend more of their time hunting for novel attack patterns. Ultimately the investment in this capability is merited due to low implementation overhead (equivalent to one FTE) and a more than double in return on investment over the three-year lifecycle of the project. Capitalizing on the power of cyber threat intelligence will allow PDC to operate a more efficient and effective cybersecurity organization now and into the future.

References

Agcaoili, J., Ang, M., Earnshaw, E., Gelera, B., & Tamaña, N. (2021, June 15). *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

AnySilicon. (n.d.). *What is a System on Chip (SoC)?* https://anysilicon.com/what-is-a-system-on-chip-soc/

AWS. (n.d.). *AWS Marketplace: Recorded Future Security Intelligence*. AWS Marketplace. https://aws.amazon.com/marketplace/pp/prodview-vffbkdmopipia

Banerd, W. (2019, March 30). *10 of the Best Open Source Threat Intelligence Feeds*. D3 Security. https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/

Byford, S. (2021, March 23). *OLED Nintendo Switch reportedly uses new Nvidia chip with DLSS support*. The Verge. https://www.theverge.com/2021/3/23/22346041/oled-nintendo-switch-dlss-nvidia-chip-report

CIS. (n.d.). *The 18 CIS Controls*. Center for Internet Security. https://www.cisecurity.org/controls/cis-controls-list

CISA. (n.d.). *Automated Indicator Sharing*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/ais

CrowdStrike. (2021, April 22). *What is the Cyber Kill Chain? Introduction Guide*. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/

Crunchbase. (n.d.). *Michael Kagan - Chief Technology Officer @ NVIDIA*. https://www.crunchbase.com/person/michael-kagan

Daszczyszak, R., II, Ellis, D., Luke, S., & Whitley, S. (2020, July). *TTP-Based Hunting*. The MITRE Corporation. https://www.mitre.org/publications/technical-papers/ttp-based-hunting

Gartner. (2022). *Recorded Future Intelligence Services Reviews, Ratings, and Features*. https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendor/recorded-future/product/recorded-future-intelligence-services

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Grimes, R. A. (2020, September 11). *11 types of hackers and how they will harm you*. CSO Online. https://www.csoonline.com/article/3573780/11-types-of-hackers-and-how-they-will-harm-you.html

Hypr. (n.d.). *What is NotPetya? 5 Fast Facts*. https://www.hypr.com/notpetya/

JBS Foods. (2021, July 9). *JBS USA Cyberattack Media Statement*. JBS Foods. https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9

Krebs, B. (2021, July 8). *Kaseya Left Customer Portal Vulnerable to 2015 Flaw in its Own Software*. Krebs on Security. https://krebsonsecurity.com/2021/07/kaseya-left-customer-portal-vulnerable-to-2015-flaw-in-its-own-software/

Leswing, K. (2021, November 17). *Nvidia crypto mining chip sales fell off a cliff this quarter*. CNBC. https://www.cnbc.com/2021/11/17/nvidia-crypto-mining-chip-sales-dropped-60percent-sequentially-in-q3.html

Lockheed Martin. (n.d.). *Cyber Kill Chain®*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

McMillan, R. (2013, May 16). *Definition: Threat Intelligence*. Gartner. https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

MITRE. (n.d.). *APT29, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, Group G0016*. MITRE ATT&CK. https://attack.mitre.org/groups/G0016/

NPR. (2021, June 3). *REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says*. https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says

Nvidia. (2021). *Nvidia Who We Are*. https://images.nvidia.com/nvimages/aem-dam/Solutions/about-us/documents/NVIDIA.pdf

Nvidia. (n.d.-a). *Deep Learning Super Sampling (DLSS) Technology*. Nvidia GeForce. https://www.nvidia.com/nl-nl/geforce/technologies/dlss/

Nvidia. (n.d.-b). *Executive Bios*. NVIDIA Newsroom. https://nvidianews.nvidia.com/bios/

Nvidia. (n.d.-c). *NVIDIA Locations & Regional Offices*. https://www.nvidia.com/en-us/contact/

Nzeata, V. (n.d.). *The Cyber Kill Chain in Practice - Cyber Brain Academy*. Cyber Brain Academy. https://www.cyberbrainacademy.com/the-cyber-kill-chain-in-practice/

Osborne, C. (2021, July 23). *Updated Kaseya ransomware attack FAQ: What we know now*. ZDNet. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

Palo Alto. (n.d.). *What is a Threat Intelligence Platform*. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform

Pownall, C. (2021, January 11). *Maersk NotPetya cyberattack response timeline*. Charlie Pownall. https://charliepownall.com/maersk-notpetya-cyberattack-timeline/

Recorded Future. (2020, January 15). *What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team*. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

Recorded Future. (n.d.). *License Options*. https://www.recordedfuture.com/license-options/

RocketReach. (n.d.). *RocketReach - Mark Vorzimmer's Email & Phone Number*. https://rocketreach.co/mark-vorzimmer-email_121870473

Sason, D. (2021, July 6). *REvil Ransomware Attack on Kaseya VSA: What You Need to Know*. Varonis. https://www.varonis.com/blog/revil-msp-supply-chain-attack

Sherstobitoff, R. (2021, June 8). *JBS Ransomware Attack Started in March*. SecurityScorecard. https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march

Sood, K., & Hurley, S. (2017, June 29). *NotPetya Ransomware Attack [Technical Analysis]*. CrowdStrike. https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

The Org. (n.d.). *Sonu Nayyar - SVP & CIO at Nvidia*. https://theorg.com/org/nvidia/org-chart/sonu-nayyar

Tilley, A. (2016, November 30). *The New Intel: How Nvidia Went From Powering Video Games To Revolutionizing Artificial Intelligence*. Forbes. https://www.forbes.com/sites/aarontilley/2016/11/30/nvidia-deep-learning-ai-intel/

Todd, D. (2021, September 1). *Ponemon Institute: Cost of Data Breach Hits Record High*. SecureWorld. https://www.secureworld.io/industry-news/cost-of-a-data-breach

Trend Micro. (n.d.). *Indicators of compromise*. https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise

Yahoo. (2022). *A.P. Møller - Mærsk A/S (AMKBY)*. Yahoo Finance. https://finance.yahoo.com/quote/AMKBY/profile?p=AMKBY