CYBER THREAT INTELLIGENCE_

SOLUTIONS GUIDE & BEST PRACTICES

digital shadows_

CTI: DEFINITIONS AND USE CASES

Cyber threat intelligence (CTI) improves the resilience of your business against emerging cyber threats. The best CTI program informs preventative and proactive security actions and is intimately tied to business concerns and effective reduction of risk.

This guide serves to navigate you through the jargon surrounding cyber threat intelligence (of which there is plenty!), to outline some of the best practices for cyber threat intelligence, and to point you towards some excellent resources to leverage when developing or improving your organization's cyber threat intelligence capabilities.

FORRESTER DEFINITION

"Assessing the intent, capabilities, and opportunities of threat actors in response to stakeholder requirements."

GARTNER DEFINITION

"Evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets."

POPULAR CTI USE CASES

In the past, CTI was viewed in terms of a tactical response to block Indicators of Compromise (IoCs). This approach saw CTI as providing security teams with feeds of IP addresses, file hashes and domains (among other observables) that threat actors use. By blocking these, security teams look to reduce the risk that they will also be targeted.

While these tactical applications are still relevant, nowadays attackers have increased in technical sophistication and abilities. They can swiftly change their infrastructure or tactics rendering many IOC feeds out-of-date. That's why more mature threat intelligence capabilities focus on operational and strategic intelligence above the tactical.

TACTICAL	OPERATIONAL	STRATEGIC
IOC feeds of observables to block	Understand the tactics and techniques employed by actors	Threat research and thematic trend reports

Threat intelligence can also be considered synonymous with other use cases, such as brand protection, data leakage detection, and attack surface monitoring. This guide will focus on CTI in its most classic applications— *information about threats and threat actors that provides sufficient understanding to mitigate a potentially harmful event in the cyber domain.*

THE INTELLIGENCE CYCLE

The purpose of intelligence is to 'reduce ignorance in decision-making' or simply aid understanding of the confusion and complexity of outside factors from an organization. The intelligence cycle is a great model to help us produce that.

Let's be clear: the intelligence cycle we outline in this guide is one of many. Some cycles have five stages. Some have six stages. Some even have seven. However, they are all different versions of the same cycle. The defining factor of a good threat intelligence cycle is iteration. A Cyber Threat Intelligence capability is not something you set up, configure, turn on, and then let run. For this approach to work, it must be an iterative process that requires continuous feedback at every stage of the cycle.

THE INTELLIGENCE PROCESS

PLANNING AND DIRECTION

Cyber Threat Intelligence is effective when it's answering the correct questions, and these "correct questions" are commonly referred to as "Priority Intelligence Requirements" within the CTI community. The number of organizations reporting a formal process for gathering such requirements increased 13% from last year to almost 44% (SANS 2020).

To effectively gather requirements, it's worth considering these three stages:

1. **IDENTIFY CRITICAL ASSETS**
2. **IDENTIFY STAKEHOLDERS**
3. **CAPTURE REQUIREMENTS**

IDENTIFY CRITICAL ASSETS

Before considering stakeholders and requirements, it's essential to identify the business' critical assets through threat modeling. Although a few threat actors are indiscriminate in their targets, the vast majority of these attackers target companies based on the assets they hold. Common examples of critical business assets are databases holding customer data, payment processing systems, employee access systems, trading platforms or exchanges, or Enterprise Resource Planning (ERP) applications.

Threat modeling is a way of structuring thinking around what critical assets an organization has and the likely threats to that organization. A company's measure of criticality may not match the thought process of an attacker, which means that it can be tricky to understand what constitutes a "critical asset." Companies may not consider their social media accounts a critical asset to the business, but attackers routinely target them for social engineering schemes, phishing, impersonations, and more.

With critical assets defined, it's then important to understand how these assets may be targeted. The threat actor FIN7, for example, went after payment card data and non-public information. The Russian military intelligence group GRU sought emails, analytics and internal documents. The Syrian Electronic Army (SEA) targeted social media accounts.

OWASP

Threat Modeling: "works to identify, communicate, and understand threats and mitigations within the context of protecting something of value".

IDENTIFY KEY STAKEHOLDERS

CTI professionals must understand who their key stakeholders are–and there are plenty of options. The reality is that the more stakeholders you can serve, the easier it will be to demonstrate the value of the CTI program. Below are eight top internal stakeholders and example actions.

Customers, in particular, are often overlooked as CTI stakeholders. Businesses thrive on customer relationships. Understanding and mitigating threats to customers is critical to the brand relationship with that customer. An active conversation about how trust is established that is informed by real threats helps strengthen the trust between company and it's customer.

1. INCIDENT RESPONSE
Understand TTPs of threat actors and their motivations.

2. VULNERABILITY MANAGEMENT TEAM
Understand what vulnerabilities to prioritize based on threat activity.

3. SECURITY OPERATIONS
Enrich observables with threat intelligence; Identify insider threats.

4. MARKETING/BRAND TEAM
Understand attackers using social media and brand presence to launch targeted attacks.

5. GENERAL
Receive security awareness training tailored to the threat landscape.

6. CISO AND LEADERSHIP
Understand the threat landscape and changing risk profile

7. RISK PROFESSIONALS
Better Understand threat as a component of overall risk.

8. CUSTOMERS
Intelligence failures can impact the trust customers have in a company.

CAPTURE SPECIFIC REQUIREMENTS

Once you have understood what assets need protecting and who the stakeholders are, you can begin to capture different requirements.

At this stage, specificity is key. For example, if your high-level requirement is "what's the threat to us from ransomware", the following sub questions should be those you attempt to answer:

- **What ransomware variants are focused on targeting organizations in financial services?**
- **What ransomware variants are the most likely to impact financial services organizations?**
- **What are the top exploits used by ransomware variants?**
- **What tactics are ransomware variants using for initial access?**
- **What ransomware variants are being discussed in criminal locations?**
- **What ransomware variants are focused on targeting organizations in my geography?**

COLLECTION

After identifying the questions you want to answer, you can start to collect the relevant data. There are three main buckets: internal data, sharing communities, and external sources. The most mature threat intelligence capabilities create a collections plan to ensure no sources skipped at this stage.

INTERNAL DATA

It's best practice to make use of as much internal data as possible, and most companies are unaware of the rich reserves of data they possess. Internal data can be generated from proxy, mail, and NDS logs, and general security incident data. Historical events of cyber threats, although they do not provide the full picture, can give a compelling dataset to understand current and ongoing threats. The challenge then for stretched security teams is balancing collection of internal data with moderation of the noise these alerts can generate.

SHARING COMMUNITIES

In addition to internal data, more mature Cyber Threat Intelligence capabilities leverage sharing communities. These can include:

1. **INDUSTRY ISACS**
   Such as FS ISAC, Health ISAC, IT-ISAC
2. **GOVERNMENT ADVISORIES**
   Such as those from CISA and FBI
3. **OPEN-SOURCE SHARING COMMUNITIES**
   Such as MISP
4. **PRIVATE GROUPS**
   Such as on Slack and other channels

EXTERNAL SOURCES

For a comprehensive collection program, internal data and sharing community data combine with data from external sources, of which there are free and paid options. According to SANS, these open source or public CTI feeds (DNS, MalwareDomainList.com) are used by 74.3% of CTI Pros. A longer list of free feeds can be found in the final "Resources" section of this guide.

These public feeds are then combined with more premium external feeds, often providing data from more exclusive sources. Many organizations lack the ability or bandwidth to collect from criminal forums, dark web markets, and messaging apps and turn to external providers such as Digital Shadows to provide that visibility. Beyond the "dark web" sources, companies should consider pulling from other sources including social media, code repositories, file stores, mobile app stores, and other open sources. Whatever the source, the vast majority of mentions online are largely irrelevant and finding the relevant information is akin to finding a needle in a haystack.

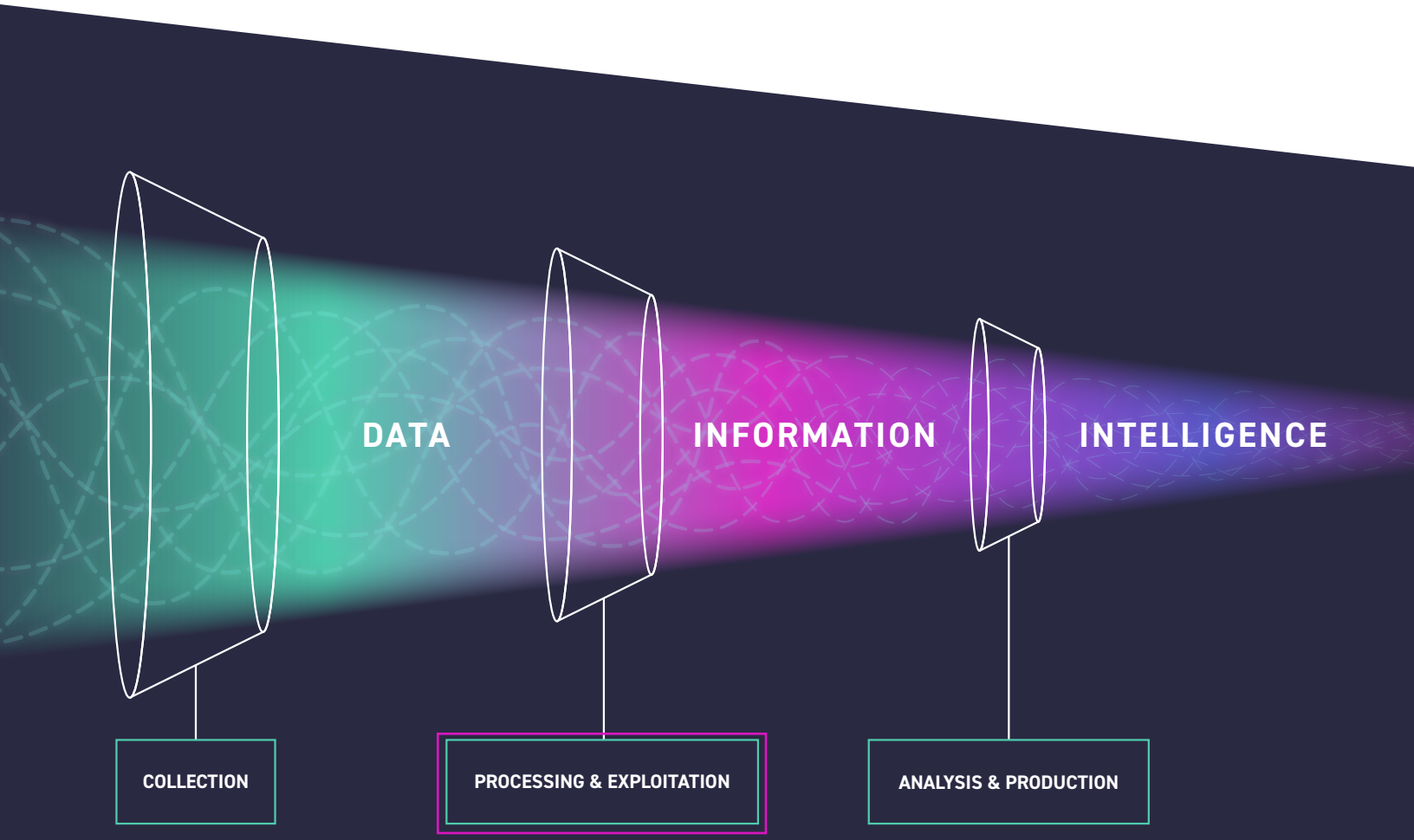
300K

AVERAGE ANNUAL DARK WEB MENTIONS OF A COMPANY

PROCESSING AND EXPLOITATION

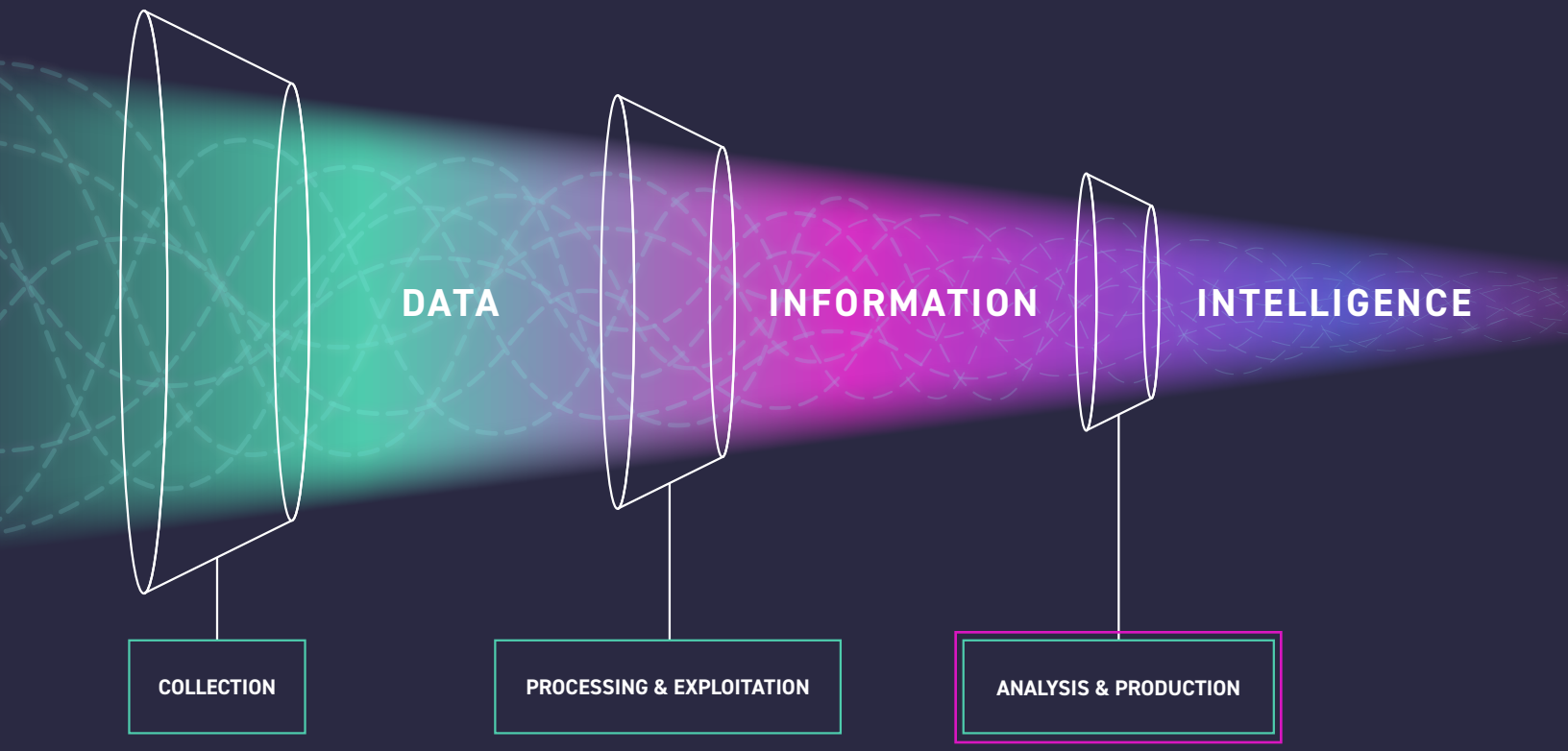
Collection data may come in many different forms—including technical data, documents (including metadata), images, tweets, and much more. All these types of data must be stored, processed, and normalized. This is where Threat Intelligence Platforms, such as Anomali, ThreatConnect, TruStar, EclecticIQ, and ThreatQuotient can add value.

After it is normalized, the data must be turned into information. This can be done by humans, computers or a combination of the two. Software can remove a majority of false positives and duplications. The human element is additionally critical as it is a key factor in removing as much irrelevant data as possible at this stage. SearchLight removes 99.5% of raw data so that resource-constrained teams can focus on only the most pertinent information.



ANALYSIS AND PRODUCTION

At this stage, the processed information is transformed into intelligence, or information useful to taking action. In the process of taking information and rendering it into actionable threat intelligence, it's critical to avoid traps such as biases and assumptions. This section outlines some commonly used cognitive biases and heuristics in CTI to look out for and techniques to mitigate them.



COGNITIVE BIASES

One of the biggest hurdles to good analysis is cognitive biases, or "a mistake in reasoning, evaluating, remembering, or other cognitive processes, often occurring as a result of holding onto one's preferences and beliefs regardless of contrary information." While there are a large number of cognitive biases, the most frequently occurring ones are:

CONFIRMATION BIAS
Focusing on information that confirms pre-existing assumptions

ANCHORING EFFECT
Relying too much on the initial information

BANDWAGON EFFECT
Believing in something because an established majority do

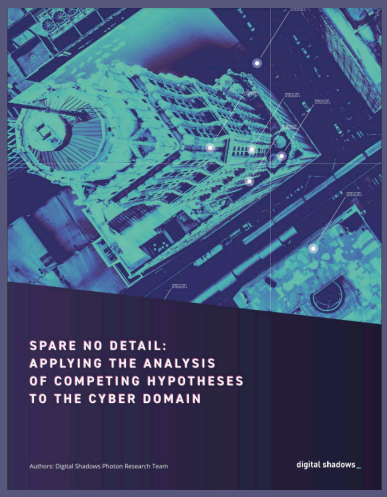
STRUCTURED ANALYTICAL TECHNIQUES

Structure Analytical Techniques (SATs) are methods that intelligence analysts employ to overcome cognitive biases. Richards Heuer, widely regarded to be the father of intelligence analysis, published many of these techniques in his 1999 paper, Psychology of Intelligence Analysis.

TI pros often immediately look for the sophisticated SATs. However, in truth, there's plenty that can be done with simpler methods. For example, Devil's Advocate and a SWOT analysis (techniques within the reach of all of us), can help to sharpen our analysis.

For analysts with more time, techniques such as Analysis of Competing Hypotheses (ACH), a methodology developed by Richards Heuer himself, and the Cone of Plausibility can be extremely useful for forming threat hypotheses and forecasting threats.

ANALYSIS OF COMPETING HYPOTHESES



APPLYING THE ANALYSIS OF COMPETING HYPOTHESES TO THE CYBER DOMAIN

CONSISTENCY OF LANGUAGE

We recommend using consistent language so that stakeholders can easily make sense of the analysis. Doing so enables CTI analysts to explicitly express what they know, what they don't know, and what they think.

Language of Uncertainty (LoU), also known as Words of Estimative Probability (WEP), exists so threat intelligence analysts and security practitioners can express confidence in a probabilistic judgment and provide parameters for each level of confidence.

QUALITATIVE STATEMENT	ASSOCIATED PROBABILITY RANGE
REMOTE OF HIGHLY UNLIKELY	<10%
IMPROBABLE OR UNLIKELY	15-20%
REALISTIC POSSIBILITY	25-50%
PROBABLE OR LIKELY	55-70%
HIGHLY / VERY PROBABLE / LIKELY	75-85%
ALMOST CERTAIN	>90%

DISSEMINATION AND INTEGRATION

The final step for finished threat intelligence is to deliver it to the right people in the correct format.

There are several delivery formats, including reports, briefings, SOC alerts, and enriching lookups. However, most often, it's as simple as an email to the right stakeholder. In fact, according to SANS, email and documents are still the most common forms of disseminating intelligence (66.3%).

Here are six considerations for effective dissemination of intelligence:

USE THEIR TERMINOLOGY, NOT YOURS.

Those of us from both the intelligence and cybersecurity communities tend to use our abbreviations and jargon. Unless your intelligence consumer is within your organization, they won't understand what you are trying to communicate. Use their own lexicon and analogies to help convey your message.

FOCUS ON WHAT THEY CARE ABOUT.

If you are creating products for a technical audience, Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs) are fine to use, but they are not acceptable language for executive-level products. Business risk, assets, liabilities, profit, and loss are terms executives are interested in. This has been said for many years, yet the problem persists.

BUILD BRIEFING DOSSIERS ON YOUR INTELLIGENCE CONSUMERS.

You build dossiers on your adversaries. Why not make them for your intelligence consumers. What are their trigger words? What are they passionate about? Understanding and documenting what to say and what not to say is vital for effective communication with a challenging consumer. Capturing this information is key; you need to learn from your successes and failures. Given the rate of turnover within organizations, capturing this knowledge is essential for continuity of production.

YOU MAY HAVE TO ALTER YOUR EXISTING PRACTICES.

Just because you have historically done something doesn't mean the approach can automatically apply to a new intelligence consumer. When it comes to intelligence products, one size does not fit all. You will have to tailor your intelligence product's format and timetable to the audience.

ENGAGE WITH THEM OUTSIDE OF OFFICIAL WORK CHANNELS.

Look for ways to interact with your intelligence consumers outside of official forums and meetings. Would they be willing to mentor you? Could you take them out for lunch or coffee? This should resonate with people from our space; develop a benign social engineering strategy to establish trust that will be the foundation of an ongoing relationship.

OPERATIONALIZING CYBER THREAT INTELLIGENCE

Effective dissemination will give you the best chance of answering stakeholder requirements and effectively operationalizing your threat intelligence. This stage will have a significant bearing on the success of your overall CTI program. To learn more about some of the topic metrics, listen to this presentation "How to Get Promoted: Developing Metrics to Show How Threat Intel Works" from Marika Chauvin and Toni Gidwani.

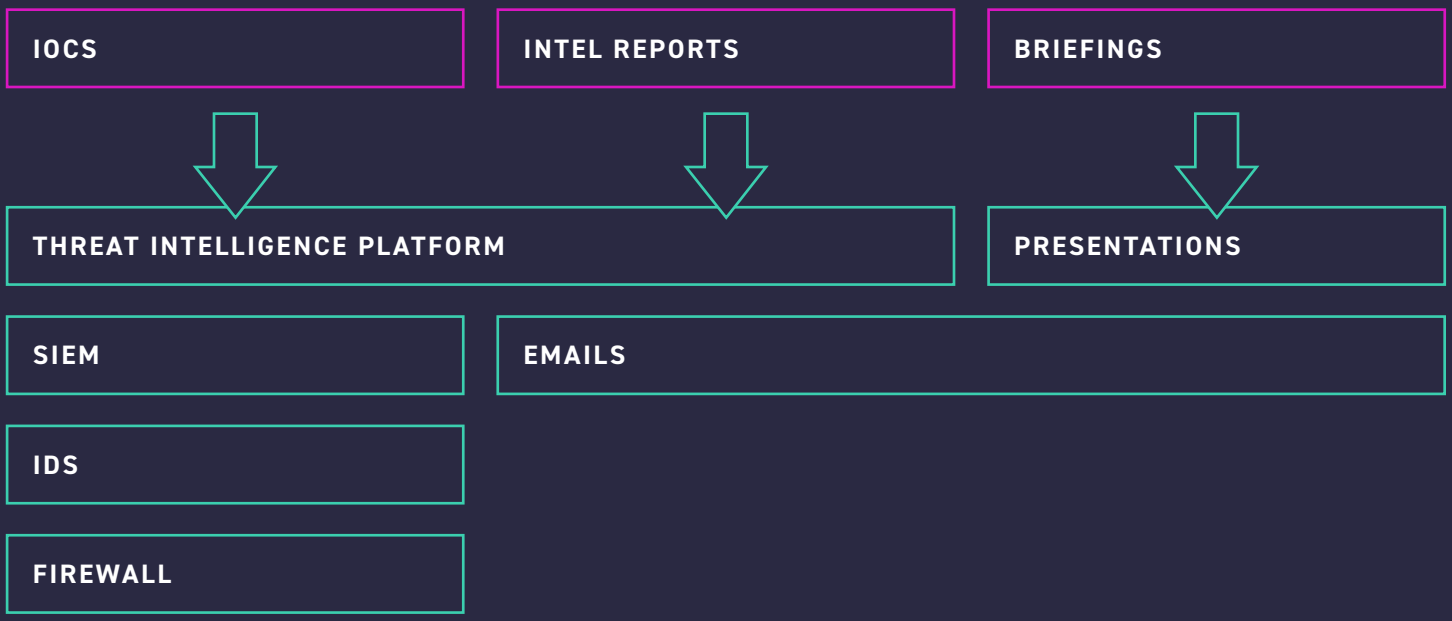
The most common action measures are:

BLOCK INDICATORS OF COMPROMISE

IDENTIFY GAPS BASED ON ATT&CK TTPS

PATCH PRIORITIZATION

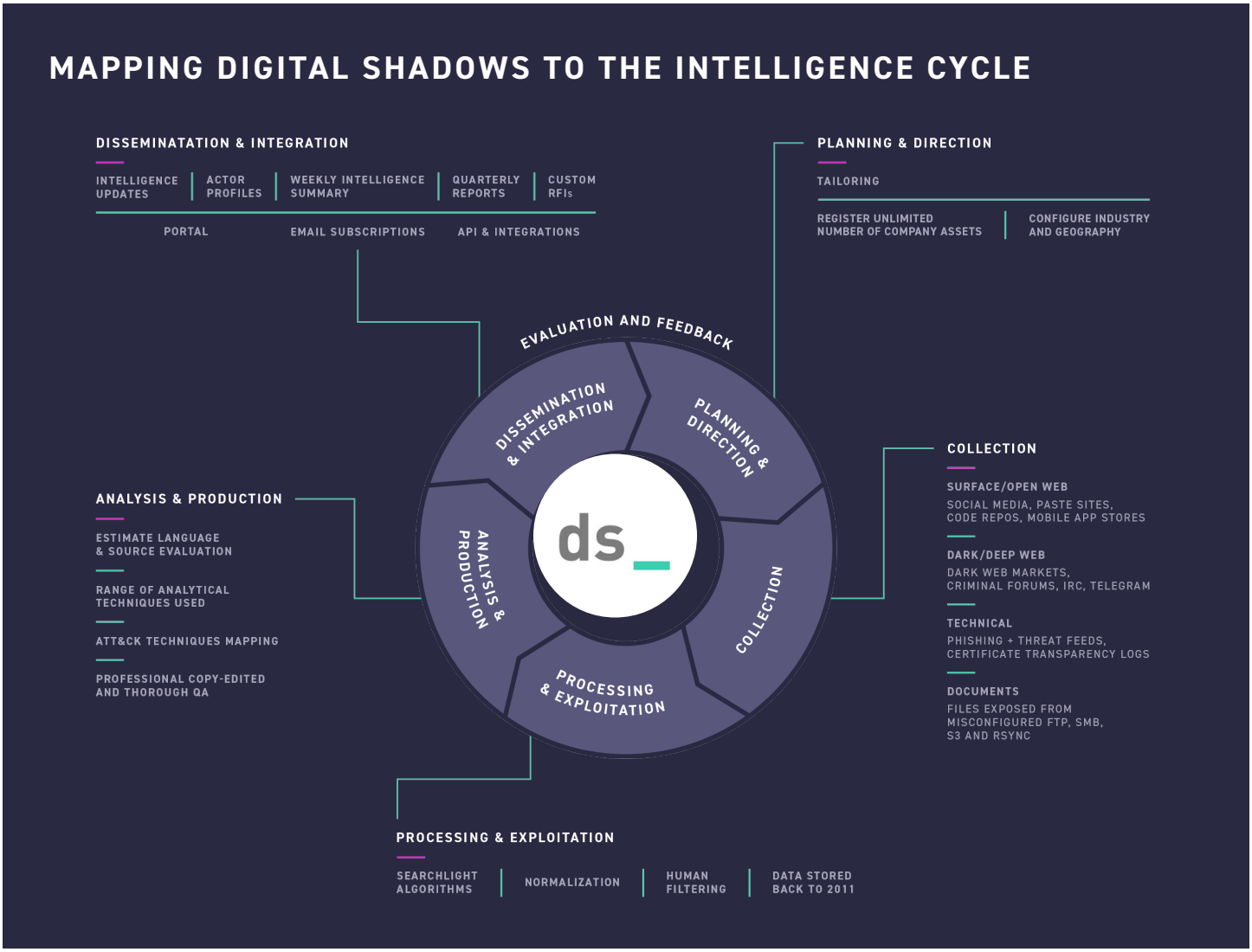
ADDED MONITORING



THE DIGITAL SHADOWS APPROACH

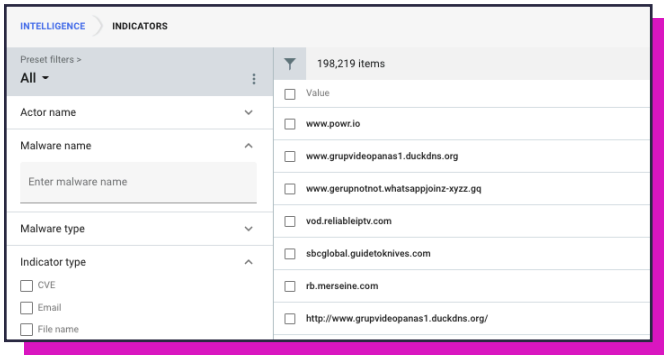
Digital Shadows SearchLight™ helps organizations to focus on the threats most relevant to their geography, sector, and threat model. SearchLight maintains a threat model for clients, based on their assets and then monitors threat actors relevant.

MAPPING DIGITAL SHADOWS TO THE INTELLIGENCE CYCLE



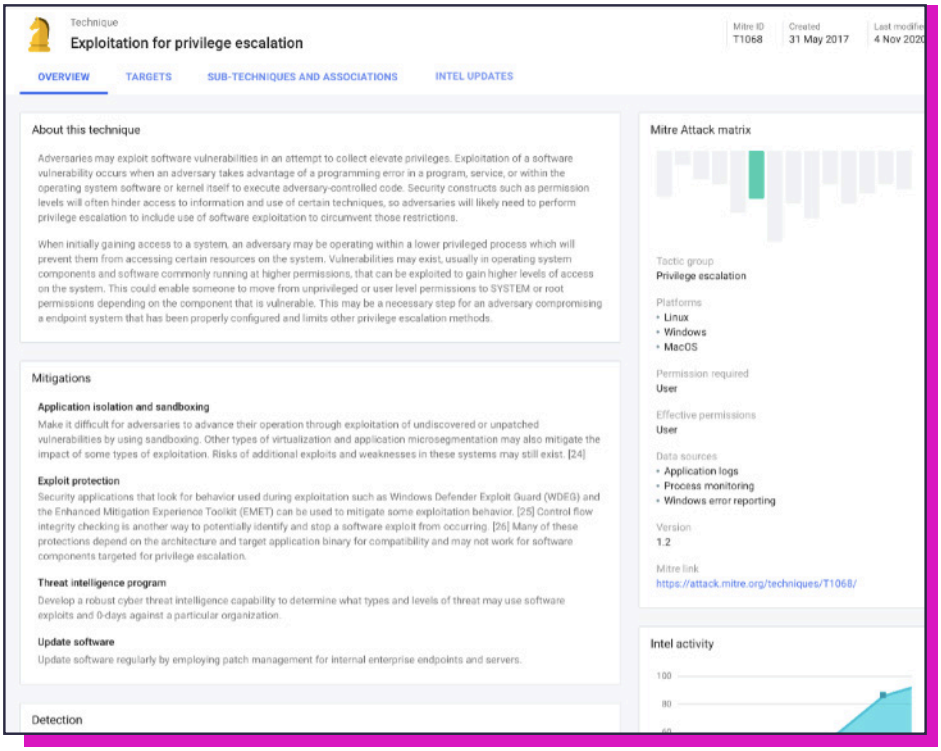
TACTICAL INDICATORS

SearchLight combines primary-sources indicators with those from APT reports, Urlhaus, Alienvault, OpenPhish, PhishTank. These are available within the Observables section and the dedicated Actor Profiles, both of which are exportable in STIX 2.1 format or as a simple csv.



MITRE ATT&CK TECHNIQUES

With ATT&CK techniques available within each actor profile, users can easily see the techniques most relevant to their sector and geography.



REPORTING

Benefit from extensive reporting options within SearchLight. This includes a Weekly Intelligence Summary, and Quarterly CVE reports, and Industry Threat Landscape reports. On top of this, users can create custom reports and schedule at their own need. For more bespoke requirements, we offer additional RFI (request for information) hours.

SearchLight integrates with SIEM and Threat Intelligence Platforms, but it also provides email subscriptions on specific areas of interest.


digital shadows_

Weekly Intelligence Summary

19 MAR 2021

In the spotlight this week: Four zero-day vulnerabilities in Microsoft Exchange Servers have been linked to more than 30,000 cyber attacks taking place in the week following their discovery. Prior to the flaws being revealed, Chinese nation-state threat actors had already exploited them to infiltrate numerous companies and access their data. Even since a patch was released, many other threat groups have found success using the vulnerabilities (including in ransomware attacks). This rapidly drove up the number of daily attacks between 11 and 17 of March 2021: from 700 to 7,200. Compounding the problem are proof of concept (PoC) exploit codes published on GitHub, which cybercriminals quickly shared on forums. The widespread use of the servers and distribution of PoCs will likely lead to persistent targeting of unpatched Exchange Servers in the short-term future (one to three months).

Microsoft Exchange Server flaws inspire 30,000-plus cyber attacks

Affected sectors	All
Affected geographies	All
Tactics, techniques, and procedures (TTPs)	Vulnerability exploitation, zero-day vulnerability, ransomware, cyber espionage

What happened?

On 02 Mar 2021, Microsoft published a security blog post disclosing four zero-day vulnerabilities in Microsoft Exchange Servers. The flaws had been actively exploited by "HAFNIUM", a People's Republic of China (PRC)-linked threat group known to target entities in the US. HAFNIUM allegedly exploited the vulnerabilities to gain entry to unpatched, on-premise Exchange Servers. That access granted an entryway to victims' email accounts and the opportunity to install malware and secure long-term access. The four zero-days are summarized as follows.

- **CVE-2021-26855 (aka ProxyLogon),** a server-side request forgery (SSRF) vulnerability in Exchange: This could enable threat actors to send arbitrary HTTP requests and authenticate as the Exchange Server.
- **CVE-2021-26857,** an insecure deserialization vulnerability in the Unified Messaging (UM) service: This enables threat actors to run code as SYSTEM on Exchange Servers, which requires an additional vulnerability or an administrator's permission to run.
- **CVE-2021-26858,** a post-authentication arbitrary file write vulnerability in Exchange: Threat actors authenticated with the Exchange Server could use this to write a file to any path on the server. They could also authenticate by exploiting CVE-2021-26855 or by compromising legitimate administrative credentials.
- **CVE-2021-27065,** a post-authentication arbitrary file write vulnerability in Exchange: Like CVE-2021-26858, this enables authenticated attackers to write files to any path on the server, and it could be exploited with CVE-2021-26855 or by compromising legitimate administrative credentials.

RESOURCES

GENERAL INTELLIGENCE TRADECRAFT

Psychology of Intelligence Analysis, Richards Heuer

Victims of Groupthink, Irving Janus

Strategic Intelligence for American World Policy, Sherman Kent

CIA Analytic Thinking and Presentation for Intelligence Analysis Training Handbook

Criminal Intelligence Manual for Analysts

JP 2-01, Joint and National Intelligence Support to Military Operations

There Is MOAR To Structured Analytic Techniques Than Just ACH!, Rick Holland

CTI-SPECIFIC RESOURCES

The Diamond Model of Intrusion Analysis

CTI is Better Served with Context: Getting better value from IOCs

Katie Nickels, A Cyber Threat Intelligence Self-Study Plan

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

MITRE ATT&CK™: Design and Philosophy

Brian Kime, Hack Your Stakeholder: Eliciting Intelligence Requirements with Design Thinking.

CTI FREE FEEDS

abuse.ch

blocklist.de/en/index.html

check.torproject.org/torbulkexitlist?ip=1.1.1.1

cinsscore.com/list/ci-badguys.txt

cybercrime-tracker.net

data.phishtank.com

isc.sans.edu/feeds

openphish.com

malwared.malwaremustdie.org

spamhaus.org

CTI FREE TOOLS

ACH .xls Template

PARC ACH 2.05

Robtex

BrightCloud® Threat Intelligence

AlienVault OTX

THANK YOU_

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threat. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight™, visit
www.digitalshadows.com

London
Columbus Building, Level 6,
7 Westferry Circus,
London, E14 4HD
+44 (0) 203 393 7001

San Francisco
One Market Street, 36th Floor
San Francisco, CA 94105
+1 (888) 889 4143

Dallas
5700 Granite Pkw
Suite 920
Plano, TX 75024