censys

YOUR GUIDE TO OUTSMARTING ADVERSARIES

Threat Hunting 101

Introduction

In a threat landscape overrun with increasingly sophisticated and successful threat actors, the need for proactive cybersecurity has never been more imperative.

Welcome to Threat Hunting 101: Your Guide to Outsmarting Adversaries. This ebook serves as your roadmap to the dynamic world of threat hunting, a practice that empowers organizations to anticipate and thwart security threats before they escalate into potentially catastrophic incidents.

Where We're Headed:

Threat Hunting: An Art, a Science, and a Mindset

Threat hunting is a proactive cybersecurity approach to identifying and mitigating hidden risks before they can evolve into full-blown threats. Threat hunting is not just about waiting for critical events to occur; it's about actively seeking out anomalies, suspicious activities, and elusive adversaries within an organization's digital landscape.

We can think of threat hunters as detectives, relying on a keen ability to recognize patterns, collect evidence, and make sense of incomplete information. And like detectives, a threat hunter's job is just as much about having the right mindset as it is leveraging the right resources. For even with all of the necessary tools and data sources in hand, doing the job well still requires thinking like a threat hunter, with an unwavering commitment to curiosity and relentless pursuit of the unknown.

Yet, unlike detectives, who are hot on the trails of criminals in flight, threat hunters hope to track down bad actors *before* they get away with the crime. **Which brings us to why threat hunters have such an important role to play in cybersecurity.**

Threat Hunting Is Critical to Modern Cybersecurity

Ask any CISO about what would happen if their organization fell victim to a successful cyber attack, and you'll get a list of consequences a mile long. Cyber attacks are incredibly expensive (the average cost of a breach in the U.S. is $9.48 million dollars) and they typically cause a slew of negative ripple effects, including loss of customer data and damage to brand reputation.

These are the makings of CISO nightmares – and unfortunately, most security leaders can probably speak to these nightmares from firsthand experience. ***In our 2023 State of Security Leadership Report, 93% of surveyed security leaders said their organization experienced a cyber attack with a material impact within the last year***. Fifty-two percent had experienced two to five successful cyberattacks within the last year. It's clear that adversaries are gaining ground.

THE NEED FOR A PROACTIVE SECURITY POSTURE

Organizations can no longer rely on traditional threat detection methods alone to prevent cyber attacks. That's because adversaries are constantly thinking of new ways to launch attacks, and are increasingly sophisticated in their approaches.

For example, cyber criminals have recently shifted their focus to compromising entire software and hardware supply chains. By infiltrating trusted suppliers and vendors, attackers can inject malware, backdoors, or vulnerabilities into widely-used software or hardware products. Attacks against Managed File Transfer tools, which the Censys Research Team investigated, are further examples of this new focus on supply chain targets.

Threat detection is an important part of any cybersecurity strategy, but it primarily relies on recognizing known threat patterns and signatures. Threat detection approaches therefore can be more reactive in nature – dependent on alerts that trigger action – whereas threat hunting is proactive and can fill security gaps that threat detection alone may miss.

Organizations' rapidly-expanding digital footprints also warrant the kind of proactive security posture that threat hunting can provide. A study from JupiterOne finds that organizations' external attack surfaces are growing at a rate of approximately 133% per year. More assets can mean more opportunities for attackers to "shoot their shot" and attempt a breach. Teams who rely exclusively on traditional methods to detect threats across these expanding, sometimes unregulated, attack surfaces can have their work cut out for them.

THREAT HUNTING IS NEEDED. BUT THREAT HUNTERS NEED DIRECTION.

Censys research finds that 50% of surveyed companies say that the ability to proactively hunt for threats is one of their top priorities. Organizations may recognize threat hunting as imperative, but in many, the practice is far from formalized and lacks dedicated resources.

Rather, threat hunting can be just one SecOps responsibility to be prioritized against a host of others, leaving practitioners little opportunity to sharpen their skills. And as a largely self-taught endeavor, many practitioners are left to cobble together tips and tricks as they go along. This can make it challenging for threat hunters to feel confident that the threats they uncover are truly credible and worth taking action against.

If that kind of uncertainty sounds familiar, you've arrived at the right resource! In the following pages, you'll find information about each step of a typical threat hunting investigation. This guidance is meant to give shape to your investigations, but is not designed to be overly prescriptive. After all, threat hunting is part art, science, and mindset. The science offers a framework, shared below, but the art and mindset guide the details – and those are up to you!

STEP 1:

How to Prepare for a Hunt

Any good investigative work requires proper preparation, so before you start your sleuthing, consider the following groundwork.

AT THE STARTING LINE: TERMS TO KNOW

Let's begin with two threat hunting terms that are important to understand: Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs).

Tactics, Techniques, and Procedures:

TTPs represent the ways in which adversaries plan, execute, and manage their activities during the course of a cyberattack or other malicious operations.

Tactics

Tactics refer to the high-level goals or objectives that adversaries aim to achieve during an attack. For example, one of the most common attacker tactics is Data Exfiltration. Using this tactic, attackers seek to compromise data integrity and confidentiality by stealing sensitive data from a target network or system.

Techniques

Techniques are the specific methods and approaches that adversaries employ to accomplish their tactical objectives. If an attacker was pursuing a Data Exfiltration tactic, described above, the technique they might deploy to carry out the tactic could be data compression. Data compression involves compressing stolen files into smaller files before exfiltrating them.

Procedures

Procedures are the step-by-step, detailed processes that adversaries follow to implement their chosen techniques. In the context of data exfiltration through data compression, a procedure could involve using a specific tool or script to compress files, encrypt the compressed data, and then transfer it to an external server using a predefined protocol.

Indicators of Compromise:

IOCs are critical pieces of information or characteristics that threat hunters can use to identify and detect potential security incidents or breaches within a computer network or system. These indicators are typically anomalies or signs that suggest unauthorized or malicious activity.

- Common IOCs include malicious IP addresses, increased database activity, excessive requests on important files, unusual outbound network traffic, or unusual DNS requests, among many others.

Threat hunters therefore apply what they know about adversary TTPs to identify IOCs within their own organization.

With these definitions in mind, we can turn to four important ways to prepare for a threat hunt.

Four Ways to Prepare for a Threat Hunt

1 Understand Your Attack Surface

Threat hunting to defend an organization's security perimeter requires that hunters first understand what the organization owns. What might adversaries look to compromise? This means threat hunters need full visibility into their attack surface. Attack surfaces are made up of all external-facing, internet-connected assets that could be subject to an attack.

Building a view of your attack surface can be accomplished through efforts like subdomain enumeration, which can require a fair amount of manual effort. Organizations with External Attack Surface Management (EASM) solutions, like Censys, however, can gain visibility into their attack surface while benefiting from additional efficiencies. EASM solutions provide automated, real-time attack surface monitoring, and include the discovery of assets that were previously unknown to the organization.

2 Establish Baseline Activity

After you've achieved an understanding of your attack surface, it's important to determine what baseline activity looks like at your organization. Doing so will make it easier to spot those IOCs. To understand baseline activity, you might:

- Determine which activity is most relevant to understand. This could include network traffic, user behavior, system activity, or any other relevant aspect of your environment.
- Identify the data sources you need to collect and analyze for baselining. Common sources include logs from network devices, endpoints, servers, and security tools like firewalls and intrusion detection systems.
- Gather historical data for a sufficient period, typically at least several weeks. The longer the historical data, the more accurate your baseline will be.

3 Become Familiar with Adversary Tactics

Though adversaries are continuously evolving their approaches, threat hunters can use what they know about current tactics to anticipate how attackers might adapt and evolve them going forward. You can dive deeper into the techniques hackers are using to deploy common attacks, including malware, phishing, and ransomware attacks, by referencing the MITRE ATT&CK framework.

MITRE ATT&CK is a "globally accessible knowledge base of adversary tactics and techniques based on real-world organizations." The MITRE ATT&CK framework has detailed insight into the TTPs that hackers use.

4 Know Thy Enemy

Are there cyber attack techniques that have been frequently used on other companies in your industry, or against other companies who use similar technologies? As you conduct your research, think about how an adversary is most likely to take action against your specific organization.

For example, in recent years many educational institutions in the U.S. have been prime targets of ransomware attacks. If you were conducting threat hunting investigations for an educational institution in the U.S., looking for signs of ransomware would be a logical place to start.

STEP 2:

Use a Threat Modeling Mindset to Establish a Hypothesis

It's now time to narrow focus and establish your threat hunting hypothesis. Without a strong hypothesis, a threat hunting investigation can become directionless. To avoid this, threat hunters need to develop an educated guess about what kind of threat they are setting out to find, and where evidence of that threat could be observed. That educated guess – your hypothesis – should be the guiding light that informs the start of your hunt.

Threat hunters can adopt a threat modeling mindset to establish their hypothesis. **Threat modeling is the practice of analyzing a system's architecture and potential attack vectors to identify and assess risk**. Threat modeling can be a robust, formalized exercise that occurs independently of a threat hunt. However, adopting a threat modeling mindset can be relevant to developing a threat hunting hypothesis, as it raises questions like: Where are we most vulnerable? Where are attackers most likely to strike?

Consider the following questions, inspired by a threat modeling mindset:

- **Past Action:** How have attackers successfully breached your organization in the past? Is there a chance you're still vulnerable to this tactic?
- **Known Weak Spots:** Does your attack surface have any vulnerabilities or exposures we know we haven't remediated? Are there risky user behaviors across our workforce that an attacker could exploit?
- **Industry Trends:** As mentioned above, give thought to what's happening to other organizations in your space. How are attackers targeting other companies in our industry?
- **Technology Targets:** How are attackers targeting companies that use the same technology services we use?
- **Geolocation:** What other attacks have occurred against organizations in our region? Attackers may use geolocation data to craft targeted campaigns, or may be looking to disrupt entities in certain regions as a result of geopolitical factors.

As ideas for your threat hypothesis percolate, keep in mind that a hypothesis should be specific enough to provide focused direction, but not too specific so as to lead you down a rabbit hole.

A Hypothesis That's Just Right

We think we could be subject to a targeted phishing campaign that's attempting to exploit a recently disclosed vulnerability in our email system. We'll begin by evaluating emails with suspicious attachments and hyperlinks.

A threat hunting hypothesis should also be actionable and verifiable. This can be accomplished in part with the right level of focus (as discussed above), but will also depend on the resources at your disposal. This brings us to threat hunting tools.

STEP 3:

Building Your Threat Hunting Toolbox

There is no singular “threat hunting tool” that can do it all, soup to nuts. Today’s threat hunters rely on many different tools and intelligence sources to carry out effective hunts. Your choice of tools will likely vary based on your investigation’s specific needs. However, a common resource that all threat hunting toolboxes should have is access to superior internet intelligence.

SUPERIOR INTERNET INTELLIGENCE: A TABLE STAKES REQUIREMENT

Superior internet intelligence is a must for any successful threat hunt. If the internet intelligence you’re using to inform your hunt is stale, incomplete, inaccurate, or difficult to parse, identifying threats with confidence will be a challenge. If you’re going to ring the alarm to your organization’s leadership, you want to be sure you know what you’re looking at.

Threat hunters therefore need internet intelligence that is:

- **Comprehensive:** Global, multiperspective scanning of the publicly-visible internet infrastructure should be conducted.
- **Up-to-Date:** Top ports and all services should be scanned daily.
- **Accurate:** Data should have a low rate of false positives.
- **Contextualized:** Data should include deep protocol scans and indexed protocol fields.

WHERE CAN THREAT HUNTERS FIND SUPERIOR INTEL?

There are many different internet intelligence sources available to threat hunters, but not all offer the same quality of data. Only the Censys Internet Map, which powers the Censys Internet Intelligence Platform, gives threat hunters the breadth and depth of data they need to outsmart their adversaries.

The Censys Internet Map's industry leading data provides the most complete, contextual, and up-to-date index of hosts and services on the internet. Censys is the only vendor to:

- Conduct daily comprehensive scans of the top 100+ ports
- Conduct proprietary ML-based discovery across all 65,000 ports
- Refresh all services daily to eliminate false positives
- Provide detailed visibility into open ports and protocols, regardless of standard port assignment, to understand host intent

Threat hunters can access Censys Internet Map data using Censys Search, which is available for use as a free community tool. Advanced Search capabilities (like access to more historical data, regular expression queries, and matched services) are available to threat hunters with an upgraded subscription.

ROUNDING OUT YOUR TOOLBOX

In addition to a leading internet intelligence source, threat hunters will likely rely on a number of other tools to carry out their hunt. You can find examples of a few below.

Security Information and Event Management (SIEM)

SIEM solutions provide data logs of activity across an organization's hardware and software. Threat hunters can review these logs during their investigation to look for indicators of compromise. Internet intelligence vendors, like Censys, can integrate with SIEM solutions to enrich SIEM data logs.

Endpoint Detection and Response (EDR) Solutions

EDR solutions monitor endpoints (workstations, servers, and other devices) for suspicious activities, including file changes, process execution, and network connections. Threat hunters can use EDR tools to investigate endpoint-specific threats.

External Attack Surface Management

EASM solutions provide a comprehensive view of an organization's internet-facing assets and vulnerabilities. Threat hunters can leverage this solution to proactively identify potential weak points and misconfigurations, helping them stay ahead of adversaries who might exploit these external entry points to infiltrate the network.

Network Traffic Analysis

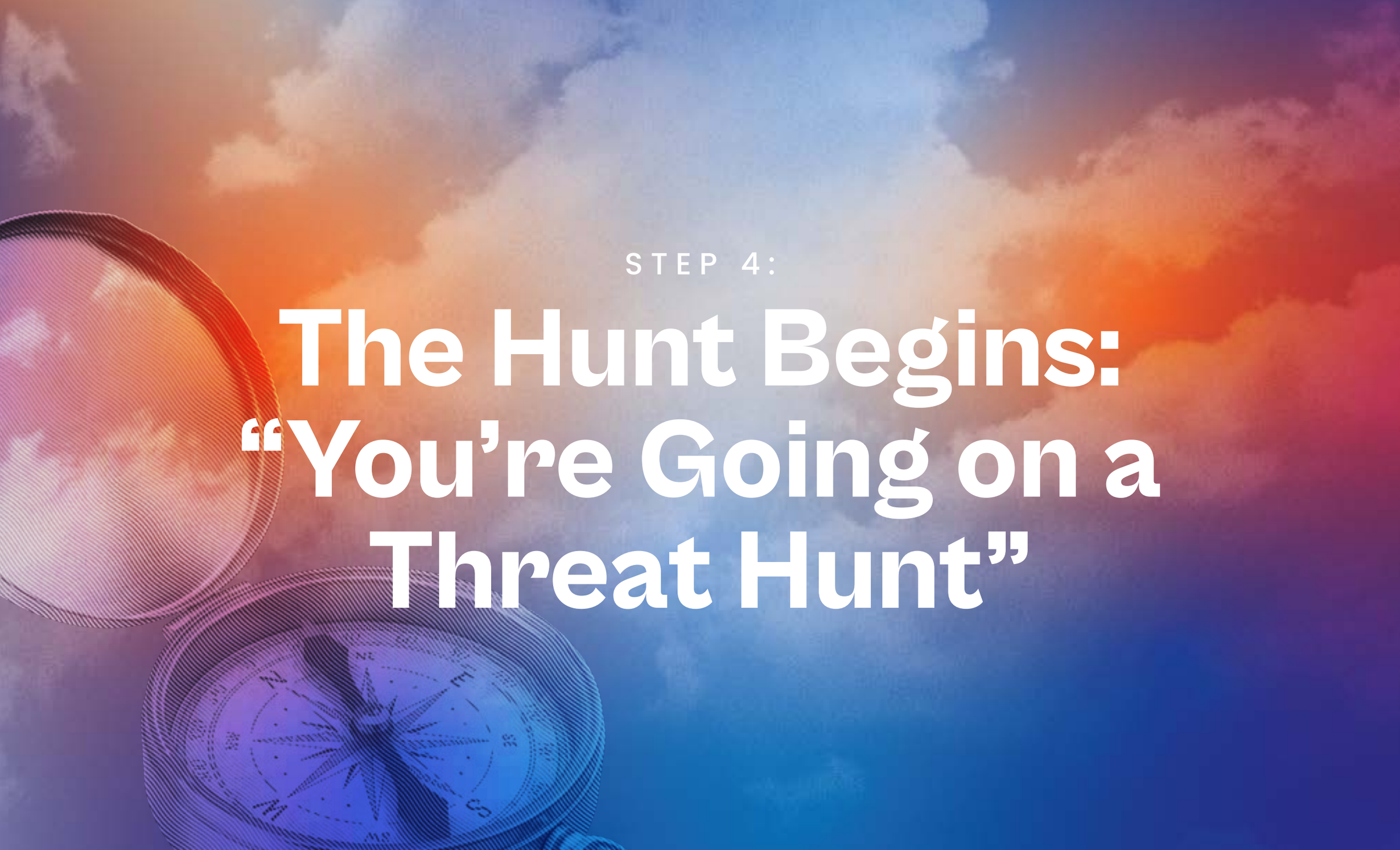
These tools capture and analyze network traffic to identify unusual patterns or activities that might suggest a network intrusion or compromise.

Open-Source Intelligence (OSINT) Tools

OSINT tools enable threat hunters to gather information from publicly-available sources on the internet, helping them identify potential threats or attackers' tactics, techniques, and procedures (TTPs).

YARA Rules and Signature-Based Detection

Threat hunters often create custom YARA rules or use existing signatures to search for specific patterns or malware in the organization's environment.



STEP 4:

The Hunt Begins: “You’re Going on a Threat Hunt”

Now that you've established a hypothesis and have your threat hunting toolbox at the ready, it's time to launch your investigation! Many threat hunting investigations begin with an exploration into logs and data feeds, as it is here that unusual activity, suspicious patterns, and other hints of undetected IOCs can be uncovered.

EXPLORING HOSTS, CERTIFICATES, DEVICES & MORE WITH CENSYS SEARCH

In addition to enriching SIEM tools, Censys data can be a primary source for threat hunters to explore when accessed through the Censys Search tool. Threat hunters can use Censys Search to run queries on an expansive database of hosts and certificates to look for suspicious activity across IP addresses, servers, IoT devices, operating systems, autonomous systems, locations, and more. As mentioned, Censys maintains the best view of global internet infrastructure available, which gives threat hunters a treasure trove of intelligence to comb through.

When beginning an investigation, threat hunters can use Censys Search to:

Identify Vulnerable Services

Identify devices or services with known vulnerabilities. By querying specific service banners, software versions, or configurations, you can pinpoint systems that require immediate patching or remediation.

Discover Rogue Assets

Search for devices and services that do not belong to the organization's known inventory. This helps identify rogue or unauthorized assets that may pose a security risk.

Monitor SSL/TLS Certificates

Track SSL/TLS certificates and search for expired or misconfigured certificates, identify certificate authorities used.

Identify Malicious Infrastructure

Detect malicious infrastructure, such as command and control servers, phishing websites, and other suspicious domains or IP addresses.

- Deimos C2: same_service((services.http.response.html_title="Deimos C2" or services.tls.certificates.leaf_data.subject.organization="Acme Co") and services.port: 8443)
- Posh C2: services.tls.certificates.leaf_data.subject_dn: "C=US, ST=Minnesota, L=Minnetonka, O=Pajfds, OU=Jethpro, CN=P18055077"

OTHER FIRST STEPS TO INVESTIGATE THREATS

Every threat hunting investigation is unique. Yours may start with information that another tool in your toolbox provides. For additional examples of ways to begin an investigation into common threats, consider:

Advanced Persistent Threats (APTs)

APTs are long-term, targeted cyberattacks often associated with nation-state actors or highly organized cybercriminal groups. To start a search for indicators of APT activity, you might: Closely monitor network traffic for unusual or long-term patterns of communication. APTs often establish persistent connections with command and control servers, which can be detected through unusual traffic patterns.

Zero-Day Exploits

Zero-day exploits are vulnerabilities in software or hardware that are unknown to the vendor. These threats can be challenging to detect using traditional security tools, which makes threat hunting efforts crucial for early detection. You could start to look for clues of zero-day exploits by looking for unusual or unauthorized access to sensitive data, repeated failed login attempts, or data exfiltration patterns.

- Note: You can also use Censys Search queries to identify and respond to zero-day exploits. The Censys Research Team publishes zero-day queries in Rapid Response blog articles.

Ransomware

When looking for signs of ransomware activity, you might want to start your search by looking for unusual encryption processes, unauthorized changes to files, or ransom notes left on compromised systems.

Phishing & Social Engineering

You might start by reviewing email traffic for suspicious attachments or links, monitoring user behavior for signs of compromised credentials, and identifying phishing domains or fake login pages.

No matter how you start your threat hunt, it's crucial to focus on anomalies rather than preconceived notions of what an attack may look like. Look for subtle and persistent IOCs that may go unnoticed by traditional security tools, as these often hold the key to identifying and mitigating emerging threats.

STEP 5:

It's Time to P-I-V-O-T!!

Unless luck is on your side, you're unlikely to find a proverbial smoking gun to prove or disprove your threat hunting hypothesis right out of the gate. Threat hunting is typically an iterative process, requiring a healthy dose of patience, curiosity, and a willingness to go where the evidence leads you.

When a shift of focus is warranted, your investigation "pivots" and your hypothesis is refined based upon the new information at hand.

The ability to pivot is one of the most critical skills in threat hunting. Pivoting is important because threats are rarely isolated; they often have multiple points of entry, lateral movement paths, or associated indicators. By pivoting effectively, threat hunters can uncover hidden relationships, patterns, and attack paths, allowing them to trace the entire attack chain and gain a holistic view of the threat landscape. This approach not only helps in identifying the root cause and the full extent of an incident, but allows for a more proactive and comprehensive response to mitigate future risks.

Examples of ways you can pivot your threat hunting investigation include:

Uncovering Historical Data

If you come across a suspicious domain or IP address, you can pivot to explore its historical data and understand how it has evolved over time, revealing changes in infrastructure or potential attacks. Censys archives more than seven years of historical information about internet-connected devices.

Tracking Certificate Information

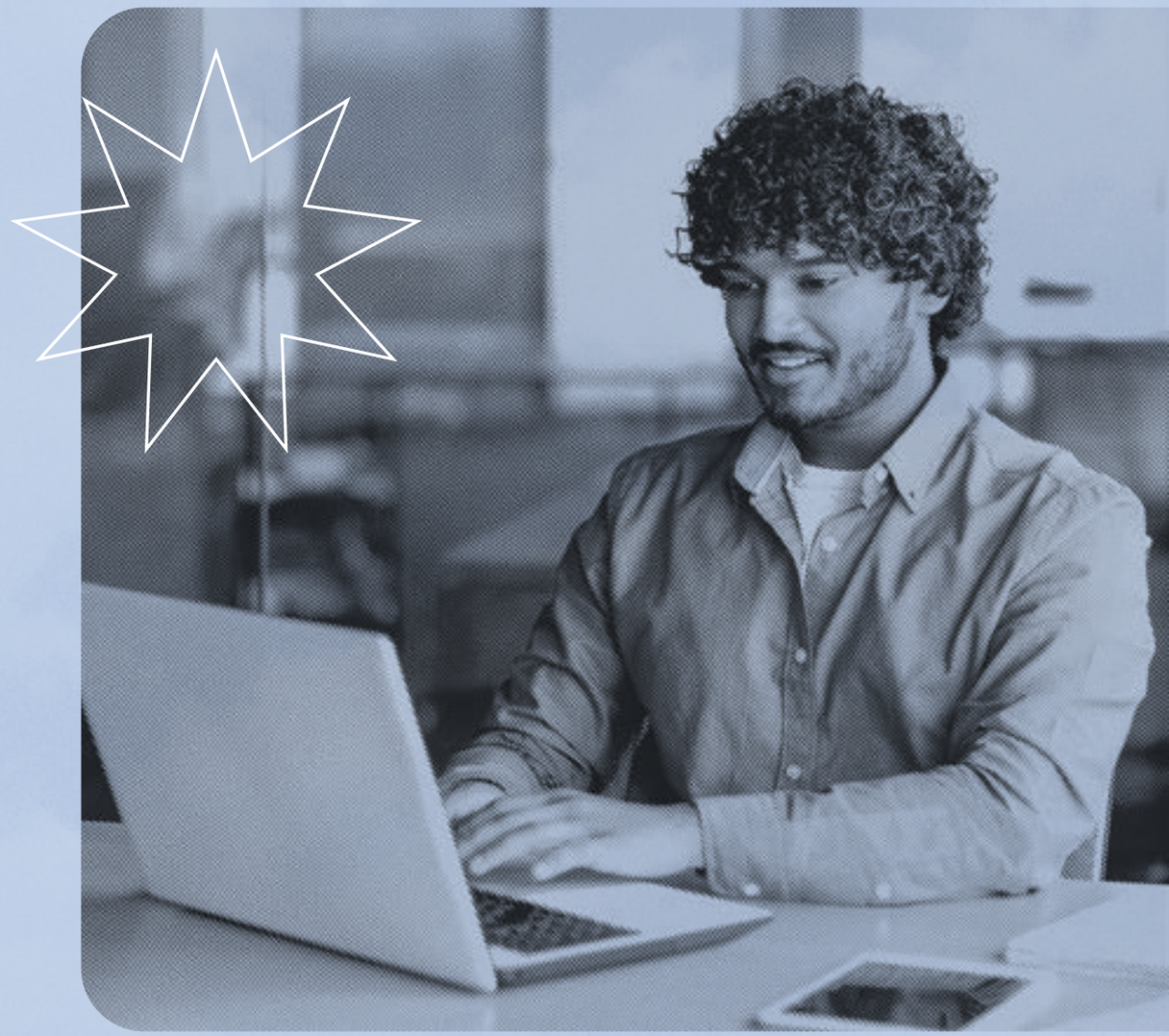
If you come across a malicious SSL certificate during your investigation, you can pivot to explore all certificates issued by the same entity or used across multiple domains, potentially identifying a larger attack infrastructure. Censys has the world's largest repository of x.509 certificates.

Exploring Autonomous Systems

Threat actors often use specific ASNs or network providers for their operations. You can pivot using Censys to investigate an ASN and discover all IP addresses, domains, and services linked to that network, helping to uncover a broader scope of potential threats.

Pro Tip:

Use the “Explore” feature in Censys Search to quickly pivot to identify related hosts, certificates, and more.



Threat Hunting in the Wild: A Case Study

How Citizen Lab Exposed Mercenary Spyware using Censys

Before we continue on with our Threat Hunting 101 framework, let's take a detour to see how threat hunting principles were applied to an actual threat hunting investigation conducted by Citizen Lab.

Researchers from the University of Toronto's Citizen Lab used Censys data to understand spyware used to target human rights workers, journalists, and activists.

Citizen Lab is a research institute at the intersection of human rights and information technology that focuses on research, policy, and advocacy. One unique aspect of Citizen Lab's mission is their investigations into the technical practices used to target activists and journalists.

Attacker Profile

Citizen Lab set its sights on Candiru, a private sector offensive actor already known for selling malware to governments. Candiru's core product offering is spyware that can be installed through a number of infection vectors on a target's Apple, Windows, or Android device. Candiru claims their products are "untraceable," which makes finding domains, certificates, and other C&C infrastructure affiliated with their software especially challenging.

Threat Hunting Goal

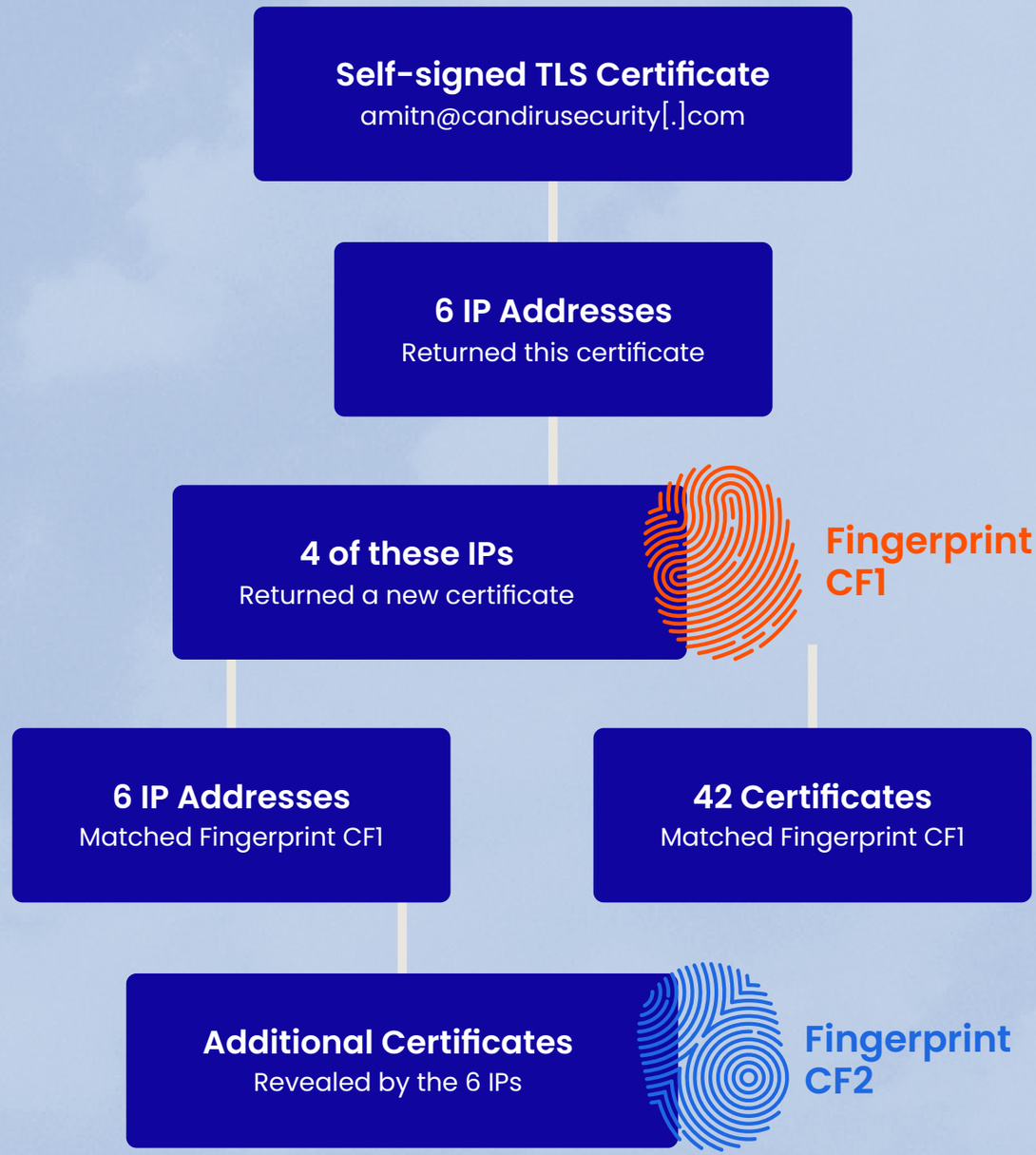
Understand Candiru's global footprint by mapping out command and control infrastructure, including IPs, domains, certificates.

The Investigation

Citizen Lab used Censys Internet Map data, which details IPv4 and IPv6 hosts and services and provides the world's largest certificate repository, to map Candiru's command and control infrastructure, and to understand the websites that Candiru's spyware has been used to target.

Citizen Lab found a self-signed certificate on Censys Search that was associated with Candiru. This certificate finding was significant because it allowed the team to pivot and uncover other attacker infrastructure using Censys' historical dataset.

Citizen Lab then queried the Censys IPv4 dataset to locate the IP addresses that were serving the certificate and potentially affiliated with Candiru. The team iterated between IPv4 hosts and certificates, surfacing certificates for over 750 websites that Candiru spyware infrastructure was impersonating.



The Outcome

Citizen Lab shared a signature that allowed Microsoft to identify two previously undisclosed privilege escalation vulnerabilities exploited by Candiru malware as well as identify more than 100 other human rights defenders, journalists, activists, and politicians who were targeted by Candiru's spyware.

Read The Full Report

You can read more about Citizen Lab's investigation into Candiru spyware here.


censys

How Censys Helped Citizen Lab Expose Mercenary Spyware Vendor – Candiru

Attacker Profile

Citizen Lab Launches an Investigation Into Candiru

Citizen Lab's Threat Hunting Goal

STEP 6:

Identifying Threats That Are Critically Understood

You've been deep in the weeds of your threat hunting investigation, sussed out IOCs, pivoted where the data has taken you, and accumulated a trail of evidence that seems to point to a threat. Is it time to alert the team?

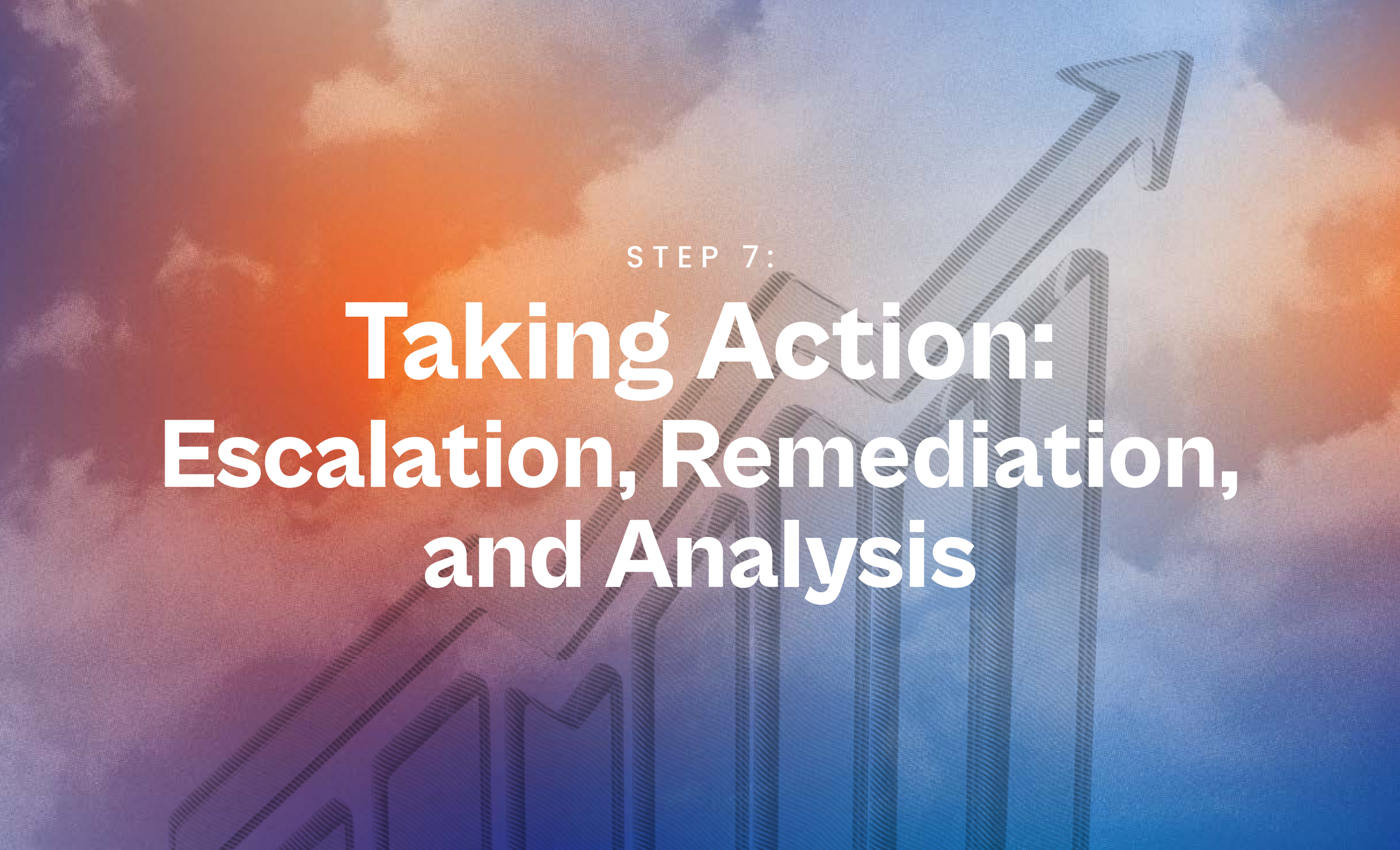
Possibly. Before you take action, a good question to ask is: "Can I say that this threat is critically understood?"

A threat is critically understood when there's a nuanced understanding of its nature, scope, and potential impact. In other words: a threat hunter is able to explain how each piece of evidence connects to the next, and why that evidence indicates that activity poses a credible threat to the organization.

Critically understanding threats is crucial for informed decision-making. It allows organizations to accurately assess the level of risk and prioritize the response, and helps teams craft an effective and tailored mitigation strategy, whether it involves isolating compromised systems, patching vulnerabilities, or enhancing security controls. Deep insight into the threat also aids in threat attribution, which can inform responses involving legal actions or law enforcement cooperation.

Don't Forget the TTPs

Remember the Tactics, Techniques, and Procedures we talked about earlier? If a threat is critically understood, a threat hunter should have a solid understanding of the TTPs that an adversary deployed. An understanding of TTPs is particularly important to communicate when taking action against a threat, as it can help organizations respond accurately and adapt security strategies to prevent similar threats in the future.



STEP 7:

Taking Action: Escalation, Remediation, and Analysis

Once your threat is critically understood, prompt escalation and remediation should occur, followed by analysis that should be used to operationalize your findings.

1 Escalation

Notify appropriate stakeholders within your organization (incident response teams, your CISO, senior management) that a threat has been identified. To do so, you'll likely need to provide a detailed report outlining the nature of the threat, its potential impact, and any evidence supporting your conclusions. It's crucial to be concise and clear in communicating the technical and business implications of the threat to ensure that decision-makers understand the urgency and severity of the situation.

2 Remediation

Once a threat has been escalated to the right parties, it's time to collaborate closely with incident responders in the organization to contain and eradicate the threat. Remediation efforts may involve isolating compromised systems, patching vulnerabilities, updating security policies, and monitoring for any lateral movement or persistence attempts by the threat actor. Continuous monitoring and analysis are crucial during this phase to ensure that the threat is fully eradicated and that any residual risks are mitigated.

After conducting remediation activities, verify that the threat is no longer present. You could do this by running queries again, re-checking logs, or using your External Attack Surface Management tool to confirm that an exposure no longer appears on your attack surface.

3 Analysis

Conduct a thorough post-incident analysis to assess the root cause and identify lessons learned. This knowledge can then be used to improve your organization's overall security posture, enhancing its ability to proactively detect and respond to threats in the future.

Documentation:

Good post-incident analysis and operationalization will involve referring back to documentation about the IOCs you uncovered and the TTPs that were used by the threat actor.

Threat hunters running investigations in Censys Search can document key aspects like function, make/model, owner, and location serviced by the asset. Tags also let you quickly return to hosts and track your progress. Additionally, you can use the Comment section at the bottom of the host summary page to detail exposures and add context to share with your colleagues.


Threat Hunters Are Needed. Fight the Good Fight!

And there you have it – we've come to the conclusion of our Threat Hunting 101 framework. Though there is no exact "threat hunting formula," for threat hunters to follow, we hope that with insights from our 101 framework, you'll be able to approach your next investigation with the clarity and confidence you need to go toe-to-toe with adversaries.

Threat Hunting 101 Key Takeaways:

1 Prepare for Your Investigation

Prepare for an investigation by gaining a view of your attack surface, baselining your organization's activity, and becoming familiar with current TTPs.

2 Establish a Hypothesis

Use what you know about your attack surface, TTPs, and answers to other threat modeling questions to establish an actionable, verifiable threat hunting hypothesis.

3 Build Your Toolbox

Build out your threat hunting toolbox with a wide variety of resources, including access to superior internet intelligence.

4 Test Your Hypothesis

Set out to prove or disprove your hypothesis by looking for IOCs. Review data sources and other tools to identify suspicious activity and anomalies.

5 Pivot As Necessary

Follow your curiosity and use your tools to pivot your investigation as needed. Threat hunting is an iterative process!

6 Ensure Critical Understanding

Once you've built a trail of evidence, check to ensure that your threat is critically understood. You should have an idea of the TTPs the adversary used.

7 Escalate & Operationalize

Escalate a critically understood threat to relevant parties and share documented findings. Look for opportunities to operationalize to prevent a similar attack in the future.

Threat hunting is poised to become even more critical to organizations' cybersecurity efforts as adversaries advance their efforts and the digital landscape continues to evolve. If you're responsible for threat hunting efforts at your organization, know that your work matters. It may be the only thing standing between an adversary and a successful attack.

Happy hunting!

Threat Hunting with Censys

Threat hunters can accelerate their investigations into advanced threats with leading internet intelligence from Censys. Censys provides the most comprehensive, accurate, and up-to-date view of global internet infrastructure available.

WHY DO THREAT HUNTERS USE CENSYS?

Unlike other data sources, the Censys offers a deep, contextualized, attributed internet infrastructure map that supports multiple use cases. We don't just collect banners or detect service presence, we create a structured snapshot of every host and running service down to the protocol level. We enrich the dataset with running software, TLS configurations, and so much more. Threat hunters can easily make sense of their findings and pivot as needed thanks to the robust context the Censys provides.

GETTING STARTED WITH CENSYS SEARCH

Censys Internet Map data is available to threat hunters through our query-based Censys Search tool. Censys Search allows threat hunters to run search queries against our database of leading internet intelligence, so that they can more successfully pursue tasks like identifying malicious command and control infrastructure, locating vulnerabile or compromised hosts, remediating risks to prevent further compromise, and strengthening their overall security posture.

You can see Censys Internet Map data in action by visiting our Censys Search tool at http://search.censys.io! For access to enhanced Censys Search features, check out our self-service packages for individuals and small teams.

Interested in learning more about how Censys can support your threat hunting efforts? We'd love to talk. Reach out to us today to start a conversation at http://censys.com/contact.

censys

Censys is the leading Internet Intelligence Platform for Threat Hunting and Exposure Management. We provide governments, enterprises, and researchers with the most comprehensive, accurate, and up-to-date map of the internet to defend attack surfaces and hunt for threats. Censys scans 63% more services than the nearest competitor across the world's largest certificate database (>10B), reducing the likelihood of a breach by 50%.

Founded by the creators of ZMap, trusted by the U.S. Government and over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the Internet.

www.censys.com