censys

7 Steps for Launching a Threat Hunting Investigation

Gain the clarity and confidence you need to go toe-to-toe with adversaries with these seven steps for launching a strategic threat hunting investigation.

Step 1

Prepare for Your Investigation

Gain a view of your attack surface:
What internet-facing assets do you own, and which could be vulnerable to an attack?

Baseline your organization's activity:
Collect data to determine what 'normal' looks like for your organization.

Become familiar with Tactics, Techniques, and Procedures (TTPs):
Learn more about how adversaries deploy common attacks. The MITRE ATT&CK Framework is a great resource for learning more about TTPs.

Step 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.

EXAMPLE:
"We think we could be vulnerable to a phishing campaign that might exploit a recently disclosed vulnerability in our email system. We can start by reviewing email traffic for suspicious attachments or links."

Step 3

Build Your Toolbox

Threat hunters rely on a wide variety of tools, including SIEM systems, External Attack Surface Management solutions, network traffic analysis tools, and internet intelligence sources.

PRO TIP:
You can access the most comprehensive, accurate, and up-to-date map of global internet infrastructure from the Censys Search tool, which is used by threat hunters around the world.

Step 4

Test Your Hypothesis

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

You might start by looking for vulnerable services, rogue assets, malicious infrastructure, signs of unauthorized access, or unusual network traffic.

Step 5

Pivot As Necessary

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

PRO TIP:
If you're using Censys Search to conduct a threat hunting investigation, you can take advantage of the Explore feature, which identifies ways to pivot on findings when looking at a specific host or certificate.

Step 6

Ensure Critical Understanding

Once you've built a trail of evidence, check to ensure that your threat is critically understood. You should feel comfortable explaining how each piece of evidence connects to the next, and why that evidence indicates that activity poses a credible threat to the organization.

Step 7

Escalate and Operationalize

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

PRO TIP:
You can use tags and comments in Censys Search to categorize hosts and certificates, as well as add context that can be shared directly with colleagues.

Interested in learning more about threat hunting? Check out our comprehensive Threat Hunting 101: Your Guide to Outsmarting Adversaries ebook.

censys

VISIT censys.com

CONTACT hello@censys.com

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.