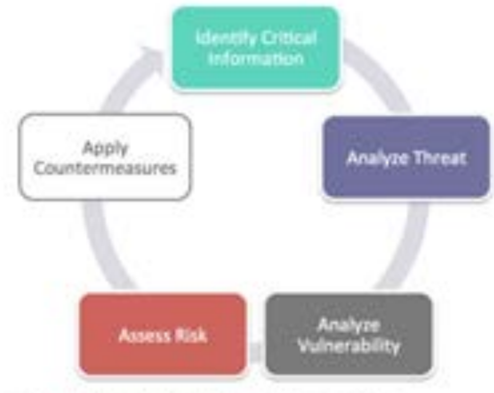
A 5-Step OPSEC Program For Defenders

digital shadows_

A 5-Step OPSEC Program for Defenders

Just as adversaries want to build resiliency into their activities, defenders must advance the resiliency of their cyber security programs. Strong OPSEC should be a cornerstone of your strategy. Fortunately, the National Operations Security Program Process provides a five-step OPSEC program that defenders can tailor to mature their OPSEC capabilities.



Step 1: Identification of critical information

First, organizations need to identify their critical business functions which, in turn, lead to identifying their "crown jewels." Work with enterprise risk teams and map the assets, people and data that are aligned to these critical business functions. Discover any externally available information associated with these entities. Don't forget to consider seemingly innocuous information that could be aggregated with other information to put this critical information at risk. Once you have taken the necessary measures to understand what information is leaking outside of your organization, you can begin to formulate an idea of what might be of interest to an adversary.

Step 2: Analysis of threats

Once critical information has been identified, organizations can then undertake an analysis of threats relevant to their business. What adversaries target your industry? What adversaries target the critical information you possess? What tactics, techniques and procedures (TTPs) do they employ? What are their motivations, intentions and capabilities? The less mature an adversary's OPSEC, the more details you can learn about their operations; you can capitalize on this.

Step 3: Analysis of vulnerabilities

Vulnerability analysis obviously includes the types of data revealed from vulnerability scanning solutions, but must also consider weaknesses in people and process. This could include broken business processes that expose vulnerabilities such as:

- Inadvertent leakage of confidentially marked information like business plans or forecasts
- Technical leakage of source code to public software repositories like GitHub
- Leakage of travel plans that could lead to wire fraud social engineering attacks against your CEO and CFO

Step 4: Assessment of risks

Once you have visibility into what you are trying to protect, how it is vulnerable, and who might be targeting it, you can prioritize the response to the risks that you face. Instead of operating in a vacuum with limited context, you now can make informed decisions about how to apply limited resources to the most significant internal and external threats.

Step 5: Application of appropriate countermeasures

Armed with better insight into risks, organizations can begin to take measures to strengthen their controls in anticipation of adversaries' activities or internal processes that put them at risk. Examples include:

- Tailoring security awareness training to include education on types of documents being unintentionally leaked
- Updating Data Loss Prevention solutions' detection rule set to prevent technical leakage of source code
- Changing the wire approval process to require multiple authorizers to decrease the ability of a fraudulent wire request to be approved

Lapses in OPSEC can have significant implications for defenders and attackers alike. With a strong OPSEC program that is able to evolve with a changing environment you can build a flexible and resilient cyber security program. Download our full whitepaper to learn more on how to mature your OPSEC capabilities.

About Digital Shadows

Digital Shadows provides cyber situational awareness that helps organizations protect against cyber attacks, loss of intellectual property, and loss of brand and reputational integrity.

Its flagship solution, Digital Shadows SearchLight™, is a scalable and easy-to-use data analysis platform that provides a complete view of an organization's digital footprint and the profile of its attackers. It is complemented with security analyst expertise to ensure extensive coverage, tailored intelligence and frictionless deployment. It continually monitors more than 100 million data sources in 27 languages across the visible, deep and dark web and other online sources to create an up-to-the minute view of an organization and the risks requiring mitigation.
The company is jointly headquartered in London and San Francisco.

digitalshadows.com

London

Level 39, One Canada Square, London, E14 5AB

☎ +44 (0) 203 393 7001 ✉ info@digitalshadows.com

San Francisco

332 Pine St. Suite 600, San Francisco, CA 94104

☎ +1 (888) 889 4143

digital shadows_