WHITEPAPER

Applying the National Intelligence Process to Information Security

The "Intelligence" approach to information security is growing in popularity, but many are still struggling to define. Red Canary has drawn upon the time-tested and well-defined procedures followed by practitioners of secret intelligence - spies, satellites, drones, etc. - in order to explain how to build and manage an intelligence process that will effectively inform corporate decision-makers in the most focused way possible. This paper defines the key phases of the intelligence process, along with the way it applies to an intelligence-focused information security process.

Red Canary

2531 W. 62nd Court
Denver, CO 80221

www.redcanary.co

Identify your intelligence requirements

The first step in the intelligence process is determining the objectives you are working to meet. Without properly addressing this first important step, the rest of the process will be flawed and inefficient.

Comprehensively answering questions about your organization, objectives, and stakeholders will greatly improve the quality of any intelligence process.

Key Questions to Consider

- What does the CISO care about?
- What keeps them awake at night?
- What information is going to help them make more timely and effective decisions that help harden the enterprise against attack and make responding to an attack more efficient?

Identify your intelligence priorities

The next phase involves "racking-and-stacking" those requirements according to their priority in your specific business environment. "Identify the next terrorist attack" may be a requirement of a country's intelligence apparatus, but "terrorist attack" is a broad requirement. What do you care most about? Terrorists taking over airplanes? Lone-wolves in a shopping mall?

The same goes for an information security program. You certainly want to prevent a breach if possible, but would you respond to a breach by an insider with a different priority than by an outsider? Of all the systems and data you're protecting, what do you care the most about?

Curate your sources

You have identified and prioritized your specific intelligence requirements, so now you must determine what sources of information will inform your answers to those questions. The first place to start is internally; logs from servers, infrastructure devices, security appliances are likely candidates. Most organizations also add in SIEMs, NetFlow, and related sources as well. Then there are outside sources such as anti-virus companies, security communities, and threat intelligence providers to consider. You can draw on these and similar sources to support your intelligence requirements. The list of sources is continually growing and requires you to understand what is available and what best supports your intelligence-enabled decision making process.

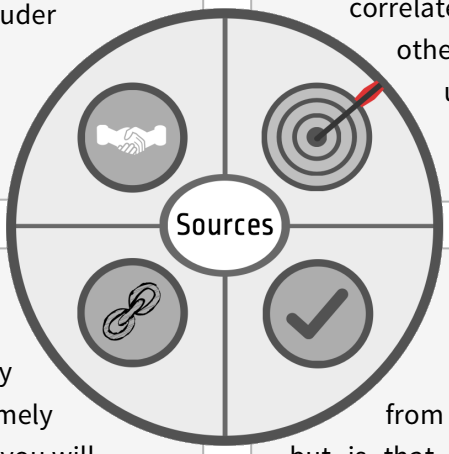
Four Essential Attributes of Intel Sources

Trustworthiness

When dealing with intelligence sources of any type, an analyst or decision maker must continually assess their trustworthiness and value to the overall intelligence process. Is what they are telling me true? The process is different if you're dealing with a human being as opposed to logs produced by a server, but the concern is the same: is my source misleading me? In the case of a human source, they may mislead you intentionally (because of some ulterior motive), or it could be unintentional (the information may be from a second-hand source, who has an ulterior motive). In the case of system logs, computers don't intentionally lie, but an intruder could doctor log entries or delete them altogether.

Accuracy

Eyewitness testimony in court can be very powerful, but eyewitnesses are notoriously unreliable for myriad reasons. Likewise, an intelligence source may believe that they are providing very precise and accurate information when in fact they are not. Unfortunately, accuracy is a quality that can rarely be tested until it is too late to correct. Tracking the historical accuracy of any source - human or electronic - is critical for the long-term success of an intelligence-enabled process. For large organizations consuming dozens of intelligence sources, the ability to correlate sources of data with each other gives you a powerful way to understand the true value of the Intelligence.



Reliability

Can you call on your source at any time and will they respond in a timely manner? For the bulk of the data you will collect the answer is probably "yes." However, if you plan to draw on sources from the security underground, or rely on a third-party, you need to understand what kind of timeframe a source will respond in. Reliability also encompasses the factors of accuracy and trustworthiness. A reliable source is one you can call upon and have a high level of confidence that what they say is factual and precise.

Relevancy

You have a lot of sources from which you can extract data, but is that data actually going to help answer your intelligence requirements? Few potential sources of intelligence data are completely without any value, but the practical value of each will vary based on the type of question you plan to answer with the data. The relevance – and cost effectiveness – of some data sources will be clearly obvious, but some may require a more intricate and ongoing evaluation process.

Apply processes to turn data into intelligence

"Intelligence" helps inform decision-making, and it is something that is built up over time and with considerable effort. The process starts with many discrete sources of "data" that are combined to form "information" that is subjected to analytic processes and turned into "intelligence."

In the case of national intelligence, "data" about individuals with known terrorist links and their communications comes together as "information". Automated pattern recognition and correlation that is then reviewed by an analyst leads to the "intelligence" that an attack on a specific target is imminent.

Looking at information security, a multitude of data including endpoint and network activity becomes information about what is happening in an organization. Threat detection algorithms and processes identify potentially threatening events that a human analyst then reviews to eliminate false positives to produce intelligence about a threat.

Communicate the resulting intelligence

The decision makers in your organization will drive the content, format, and timeliness of the intelligence. Highly technical and tactical leaders at the operational level may want frequent detailed reports or even raw data from your sources. Executives may want concise reports and slides that allow them to compare their security posture over time and to other similar organizations. The key is to communicate the intelligence without losing any meaning that could impact the decision-making process.

Examine the usefulness of your intelligence

You might collect terabytes of data from a wide variety of sources and subject that data to the most robust analytic processes available, but if you're not answering the questions needed to make correct decisions, your process has failed. Intelligence is meant to be informative, not instructional. Just as you gathered, vetted, and analyzed data, so too is a decision-maker vetting and analyzing what you have provided with other sources.

"Intelligence is meant to be informative, not instructional."

Improving Your Security Posture

It is important to understand that a strong intelligence capability does not guarantee immunity from adverse security events - intelligence "failures" have featured prominently in world events over the past decades. A strong security posture based on sound intelligence will reduce the number and severity of such events by providing you with strategic warning and shortening the time between when a threat appears and when it impacts your organization.

Learn More

Red Canary's endpoint security service uses this intelligence-based methodology to bring world-class endpoint visibility, threat detection, and response to organizations of every size – not just those with the largest security budgets. Our process involves:

- An endpoint sensor that records OS-level activity across your Windows, OS X, and Linux endpoints, whether they be physical, virtualized, or in the cloud.
- A Threat Detection Engine designed to process massive amounts of endpoint activity and detect threats throughout their lifecycle by combining proprietary technology with best-of-breed industry products, services, and threat intelligence sources.
- Security Operations Centers operated by security experts trained in endpoint security that review every potentially threatening event to organizations and eliminates false positives so customers are only alerted to confirmed threats.
- A cloud based Portal that delivers concise and actionable information about detected threats, powerful reporting, and grants visibility into activity happening across every monitored endpoint.

Ready to evaluate Red Canary to defend your endpoints from threats ranging from malware to advanced attackers to malicious insiders? Contact us at info@redcanary.co to schedule a demo.

About Red Canary

For security-conscious organizations, Red Canary simplifies the complexity of endpoint threat detection and response with its multi-dimensional detection system that eliminates false positive alerts. Whether protecting 500 or 100,000 endpoints, Red Canary delivers a platform that combines the industry's best-in-breed detection technologies with proven techniques and human analysts to quickly assess thousands of potentially malicious events per day and deliver meaningful threat detections and expedited response. Founded by a team of information security and big data processing experts in 2014, Red Canary is headquartered in Denver, Colorado.