# The value of threat intelligence

One of the most effective uses of threat intelligence is to stay on top of system vulnerabilities

**Allan Liska**
Intelligence Analyst,
Recorded Future

**WITH NEW VULNERABILITIES** being discovered every day, the threat landscape is constantly changing. But government agencies don't need to worry about every emerging threat — only the ones that concern the systems they use. They need to know which systems are deployed within their networks and in the cloud, how those systems are interconnected, and what threats are actually targeting those systems in the real world.

It's this delta between vulnerabilities and extant dangers that threat intelligence can help organizations home in on, maximizing their efficient use of security resources.



Beyond understanding just your organization's risk, you also need to be aware of the threats aimed at industry partners and suppliers. Threat intelligence can provide real-time context on the risks posed by third parties, allowing agencies to take appropriate steps to protect their supply chain.

## The role of machine learning

A good vulnerability management program is essential. If an agency understands the vulnerabilities that are currently being exploited and how threat actors are taking advantage of those vulnerabilities, the security team can prioritize patching faster, protecting the agency from 90 percent of attacks. Then, the agency will have more time to focus analysis and incident response resources on that last 10 percent — the attacks that might not be foreseeable.

Machine learning can help security teams meet the promise of uniting people, process and technology against cyber risk. For example, it might take an employee 10 minutes to close one incident. Applying machine learning to a SIEM or an IR system can create automated processes that could handle such actions and deliver a report at the end of the day — reducing the hundreds of man-hours involved in routine responses to minutes.

## Finding a common sense of purpose

The value of threat intelligence extends beyond the security operations, analyst and vulnerability management teams to every part of an agency. But to help everyone understand the threats and how to prevent them, security experts need to tell a story that everyone in the organization can understand, rather than share numbers and technical indicators that only make sense to them.

Security teams should explain why a particular threat is important and what actions the organization should take to protect itself. Technical indicators have their place, but there must be a story and a course of action to take in order to help the whole organization understand the agency's cybersecurity needs.

With context provided by threat intelligence, agencies can better allocate budgets and security resources, and stop threats before they happen. ■

**Allan Liska** is an intelligence analyst at Recorded Future.