

Sharing Threat Intelligence to Curb Targeted Attacks



ServiceNow® Trusted Security Circles

Actionable threat intelligence is key

Threat intelligence is an important part of security response, providing teams with greater context about threats to their environment. It can help teams proactively prevent security breaches. However, threat intelligence is only useful to an organization if it is actionable.

Mass market threat intelligence isn't always relevant or timely. Frequently, data feeds from external sources require the security team to evaluate whether the information is applicable to them. Open source feeds can increase false positives¹. Also, mass market threat intelligence often doesn't consider that attackers commonly employ the same exploit against multiple targets in an industry or community.

Anonymously share observable data

Because common groups are often hit with the same attacks, organizations with similar interests (such as industry) have created their own groups to facilitate the sharing of threat intelligence. These ISACs (Information Sharing and Analysis Centers) work together to share highly relevant threat information within their groups.

ServiceNow has taken this concept of threat intelligence sharing and added automation as well as anonymity to create ServiceNow Trusted Security Circles. With Trusted Security Circles, security teams can anonymously share observable data with industry peers, members of their supply chain, or a global circle. A sightings search is automatically performed against the shared observables, and the sightings count is returned as a response. When data from multiple circles is compared, patterns may emerge to identify targeted attacks against a specific group or industry. This also serves as an early warning system to other members of a circle, and a security incident can be automatically created when thresholds are met.

A suspicious incident example

Let's examine a suspicious incident at a fictional bank to see how the process works. Big Bank uses ServiceNow® Security Operations, which creates a security incident based on suspicious activity seen by the bank's endpoint protection product. It might be an attack, but Big Bank's security tools can't confirm the presence of malware. It has a good amount of observable data in the form of IP addresses, URLs, and file hashes, but its traditional threat intelligence feeds don't reveal much. It would be helpful for Big Bank to know if other organizations are seeing the same thing.

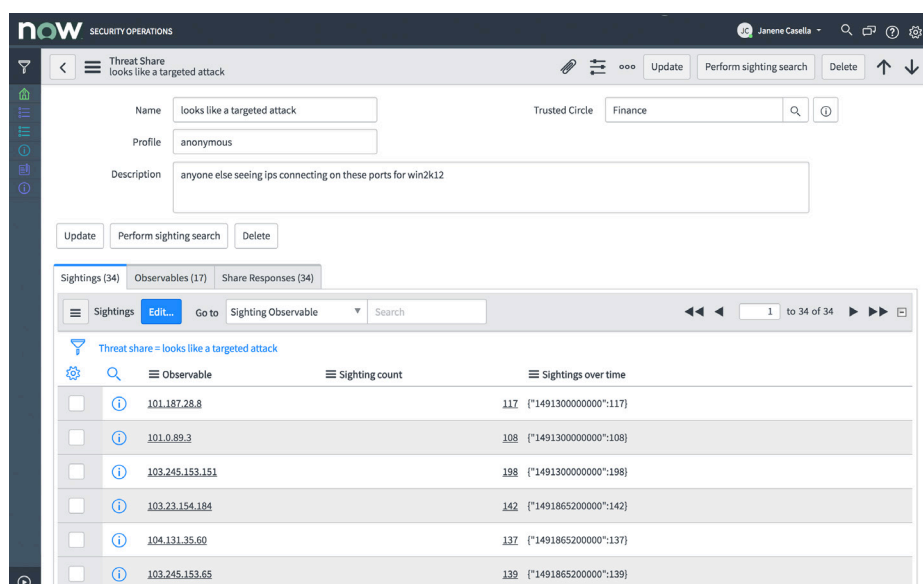
Fortunately, Big Bank participates in ServiceNow Trusted Security Circles, which means it can send a query to other circle members. It belongs to both the global circle and a private circle made up of other banks. Anonymously, it sends the observable data, along with context about where and how the data was found, to the global circle, and members of the global circle anonymously reply with the number of times each observable is present in their own environments. The numbers are low, though. Generally, they are just a fraction compared to Big Bank's total sightings.

At the same time, Big Bank also sends the same observables to its private Trusted Security Circle of fellow banks. It doesn't choose to be anonymous in this smaller circle of peers because the CISOs of these participating banks know and trust each other. The results from this query are quite different.

Wall Street Bank reports far more sightings than members of the global circle, and

With Trusted Security Circles, security teams can anonymously share observable data with industry peers, members of their supply chain, or a global circle

1. SANS Institute, Threat Intelligence: What It Is, and How to Use It Effectively, September 2016



Easily share threat intelligence with ServiceNow Trusted Security Circles

Great Credit Bank has even more. In fact, the count exceeds the sightings threshold set by Great Credit Bank's security team and automatically triggers the creation of a security incident in their own ServiceNow instance. This new incident includes all the observables received in the query from Big Bank.

Based on the responses received from other banks, it appears to Big Bank that this is an attack against the banking industry, so it starts taking steps to remediate these threats before any data can be compromised or lost. The threat intelligence information received through ServiceNow Trusted Security Circles allows Big Bank to act faster to prevent a possible data breach.

Security orchestration, automation, and response

ServiceNow Trusted Security Circles is part of ServiceNow Security Operations, a security orchestration, automation, and response engine built on the Now Platform®. It is designed to help security teams respond faster and more efficiently to incidents and vulnerabilities. Security Operations uses intelligent workflows, automation, and a deep connection with IT to streamline security response.

For more information or to request a demo, visit www.servicenow.com/sec-ops

