CELERIUM™

PROACTIVE CYBER DEFENSE

How Celerium Utilizes Intelligence to Improve Cyber Threat Defense

Equifax. The City of Atlanta. Britain's National Health Service. Anthem. Target. Under Armour. Quora. Facebook. The list of companies and organizations that have been affected by cyberattacks is long, and grows longer every day. Companies of all sizes in all sectors, both for-profit and non-profit, are vulnerable to cyberattack and the results can be devastating: interrupted business continuity, theft of intellectual property or sensitive data, and even harm to a company's reputation.

Prudent organizations can stay ahead of bad actors by making use of cyber threat intelligence, but gathering intelligence and creating a strategy can be overwhelming. How does an organization determine what pieces of intelligence are relevant to them? What actions should they take? Where does cyber threat intelligence even come from, anyway?

What is cyber threat intelligence?

Cyber threat intelligence (CTI) is data about current and potential attacks that threaten an organization's systems. This information could be about threat actors, malicious IP addresses, or other indicators. It is typically data structured for machine use, often in a common language such as STIX.

Who uses cyber threat intelligence?

Threat intelligence is used by security analysts to develop theories of attack, and by engineers to develop sensors for weak points and vulnerabilities that need protection and controls to stop attacks in progress. Cyber threat intelligence is also useful to system administrators and other IT security professionals. Because more of our physical security measures are connected to the Internet, cyber threat intelligence may also be relevant to physical security professionals.

SPEED + CONTROL

Where does cyber threat intelligence come from?

Cyber threat intelligence for most organizations comes from three main avenues: public sources, private sources, and sharing communities.

Public cyber threat intelligence comes from government feeds and other open-source feeds that are often powered by government entities. This intelligence is relevant to victims and is mostly victim-focused, because it is intelligence about attacks that have already happened. These feeds are broad, and not industry focused; therefore, they tend to have low degrees of relevancy for most organizations.

Private cyber threat intelligence refers to intelligence that has been purchased. Companies in this market are selling intelligence they have gathered on their own. Because they want to sell to as wide a market as possible, this also tends to have a low degree of relevancy to most organizations, because the source casts such wide a net.

Sharing communities such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) exist to promote intelligence sharing among similar organizations. For example, a bank would be part of a sharing community with other banks and financial institutions. The data in these community streams tends to be most relevant, because similar organizations face similar types of threats. However, relevant data doesn't mean actionable data. This data tends to be very threat specific, and may not factor in the capacity that organizations have to deal with the information.

But where does highly relevant cyber threat intelligence come from?

The most overlooked source of relevant, actionable cyber threat intelligence is that which an organization generates itself. Just about every cyber security tool, from SIEMs to firewalls, keeps logs. These logs are where cyber security professionals can spot intelligence within their own networks. When intelligence comes from outside sources, as mentioned above, you alone have to sift through it and find its relevance to your organization to make it actionable. With internal intelligence, however, it's already relevant, and already actionable.

Example 1:

Say you allow Facebook through your firewall because some employees have to manage the company's social media presence. However, you start seeing log data showing that your backend servers— servers that have no human use— are accessing Facebook. That's anomalous behavior; a server with no human shouldn't be accessing Facebook. This could be a Trojan horse "phoning home," meaning the malware is transferring data to the hacker who installed it. On further investigation, you discover that one of your employees clicked a bad link that downloaded the Trojan, and the hacker is using Facebook Messenger to communicate with it to cause mayhem.

Example 2:

Bob is one of your employees. You allow your employees access to the network after hours, but Bob's role generally doesn't require him to work overtime. You also have offices in the US and Japan, so communications to and from Japan on your network are common. However, one day while Bob's on vacation, you see log data that Bob's user account is accessing your network after hours from Japan. That's anomalous; while it could be perfectly fine (maybe Bob got a phone call from the Japanese office), it could also indicate a problem.

In each of these scenarios, you are collecting data that is directly relevant to your organization. When combined with data from outside your organization, you can then build a proactive cyber defense strategy to close vulnerabilities and protect from future attacks. Celerium's machine automation solution, Soltra Edge®, can help you marry the best of both worlds, while streamlining your processes to greatly improve your response time.

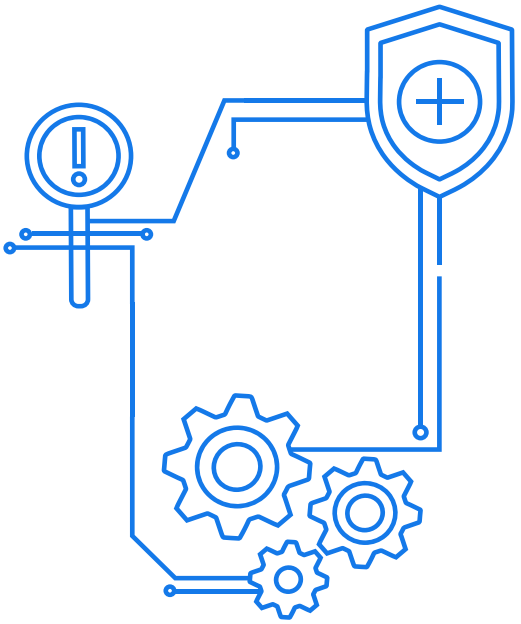
What is Celerium's machine automation solution?

Celerium's machine automation solution is a threat communication platform and threat repository. It is a solution for aggregating, normalizing, managing, sharing, automating and routing cyber threat intelligence for action. It is the intelligence sharing hub for critical infrastructure ISACs and similar communities, and is also used by community participants to receive and share back threat intelligence.

Celerium's automation solution is the recognized leader in streamlining cyber threat data sharing. Together with Celerium's solution for person-to-person collaboration on cyber threats, Celerium's solutions have been used by the most successful cyber exchange communities in the world across a host of government agencies, law enforcement and critical infrastructure including:

U.S. Department of Homeland Security
U.S. Dept. of Health and Human Services
U.S. Department of the Treasury
Electricity ISAC
Health ISAC
ICT-ISAC Japan
Canadian Cyber Threat Exchange
National Defense ISAC
Defense Security Information Exchange
City of Los Angeles
Automotive ISAC
Aviation ISAC

How do Celerium solutions help organizations?



Celerium solutions integrate with other system tools like log aggregators (such as Splunk) to help you spot anomalies on your network. By itself, a log aggregator maintains all of your log data, but doesn't know what's bad. Armed with relevant threat data from your various sources, Celerium solutions alert you to the data from your logs that doesn't belong, making your other tools even more valuable and allowing you to take action at the first sign of trouble.

Celerium's solutions also eliminate duplicates of intelligence from multiple feeds to streamline your repository to feed into other solutions, both internal and external. You can set up feeds that are most useful to you and your team, and help your threat analysts plan more effectively. These intelligence threat analysts build theories of attack to protect the things organizations value most. Here's an example:

> *Jane is an analyst for a bank. She knows that banks are most frequently targeted by organized crime actors so she researches in her organization's Celerium cyber threat repository for threat actors with ties to organized crime. She learns about who the actors are, what tools they typically use, and how they operate. She can then look at the organizational assets she is charged with protecting to see how they are vulnerable. She goes to the engineering team to learn what sensors and controls are already in place to detect intrusions. From there, she develops a theory of attack, and evaluates many possible ways for bad actors to cause mayhem for her bank. She can then go back to her engineering team to develop courses of action. Thanks to the research she did with Celerium's solutions, using both internal and external intelligence, she is able to develop courses of action for observables at all parts of the kill chain, preventing chaos for her organization.*

How Do I Get Started with Celerium's automation solution?

Celerium makes it easy to get started with free, open-source cyber threat intelligence with our PickUpStix (PIX) feed. PIX uses open source, non-commercialized data. Currently, PIX uses three public feeds and distributes about 100 new pieces of intelligence each day. PIX translates the various feeds into STIX, which can communicate with any TAXII server.

The data is free to use and is a great way to begin using threat intelligence out of the box.

Get started today with a 90-day free trial of Celerium's automation solution. At the end of your trial, if you don't want to keep the full featured version, you will still be able to use the Limited Edition version to collect cyber threat intelligence and manage your threat data. If you need access to plugins or other additional features, we have several licensing plans available.

More Questions?

Contact Us : info@celerium.com
USA & Rest of World: +1 877 624 3771