The Challenge

Ever-increasing interconnectivity is changing the threat landscape. Operational Technology (OT) networks were historically completely separate from corporate IT networks, but are becoming closely connected, increasing cyber security risk and creating new pathways for attackers to exploit vulnerabilities and gain access to corporate systems. Compromise of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks is a newer and particularly concerning attack vector, since a breach of ICS/SCADA systems can result in large-scale logical and physical damage. ICS and SCADA systems pose a unique set of challenges:

› OT networks are full of legacy systems with unpatched vulnerabilities that can be exploited. Fear of business disruption delays upgrades and updates. Attackers focus on cost-effective targets, like those that haven’t been hardened.
› OT networks require specific technical expertise that’s different from traditional IT skill sets, and is less common. The risk of social engineering attacks is ever present.
› Non-ICS threats are evolving to exploit industrial targets. For example:
   » The retooling of Remote Access Trojans, such as HAVEX, used by Energetic Bear
   » The refresh of the BlackEnergy rootkit, to deploy against industrial targets
   » "Watering hole" attacks that compromise sites used by ICS/SCADA system operators to update firmware or software

As a result, ICS environments are generally slow to respond to emerging threats.

The Solution

Recorded Future’s real-time threat intelligence enables analysts teams to now effectively collect, organize, and analyze leading indicators of compromise from hundreds of thousands of sources of threat data scattered across the web. Recorded Future Cyber offers:

› Real-time threat analytics of over 650,000 open web sources, in 7 languages, 24/7.
› Automated harvesting of data from Internet sources globally to gain better insight into threat actors, new vulnerabilities, and emerging threat indicators.
› Patented Web Intelligence Engine that organizes the open web for threat intelligence analysis, at a speed and scale not possible by manual means.
› Tailored alerts on potential and trending cyber security threats.

Why Recorded Future

- Real-time threat intelligence to improve ICS/SCADA threat forecasting
- Help leaders make informed decisions
- Better identify and reduce risks
- Minimize FUD

“...We were able to use Recorded Future to set up alerts so that on a daily basis we were getting the freshest information, the freshest intel possible.”

- Brian Wilson, Cyber Security Threat Intelligence Team Lead, Cimation
The Results

Credible, timely, and actionable threat intelligence results in better data analysis and the ability to anticipate security events—ultimately driving down breaches and data loss by espionage.

Leverage leading indicators of compromise to avoid being blindsided by cyber attacks:

› Better identify and reduce risks: Using Recorded Future, analysts can create a comprehensive, holistic picture of the hacktivists’ tactics, techniques, and procedures.
  > In the case of the Havex malware for example, Recorded Future customer Cimation was able to connect together critical pieces of information found by Recorded Future.
  > Various other sources found pieces of information, calling the Trojan by different names. Recorded Future had the ability to link all the different names together so that Cimation received all the pertinent information on the threat, regardless of what it was being called.

› Improved threat forecasting: Up-to-the-minute alerts allowed the company to build a timeline analysis of trends, new threats and vulnerabilities, and emerging indicators of compromise.
  > Hacktivist monitoring: In another example, with OpPetrol, Cimation was able to build a timeline and link analyses to learn how and when adversaries were likely to attack.
  > OpPetrol: Started in early April 2014: A group of Muslim hacktivists targeting the oil and gas industry. Posted a manifesto, tracked and translated by Recorded Future.

› Allowed Cimation to issue “spot reports” to alert the oil and gas community to impending threats.

“\nWe used Recorded Future’s timeline analysis to show the build-up of the hacktivist activity, and then we were able to use the timeline analysis to predict based on activity that was reported a year prior and what was being forecasted what was going to come down the line.”

- Brian Wilson, Cyber Security Threat Intelligence Team Lead, Cimation

Visualization of #OpPetrol build up generated using Recorded Future.

› Minimize FUD and help leaders make informed decisions: By correlating events and alerts in one unified report produced by Recorded Future, security teams can reduce the fear, uncertainty, and doubt (FUD) that normally accompanies threat information. Analysts can provide organization leaders with insightful reports with rich context and visualizations that help answer important questions for stakeholders: Is it a threat? Is it a threat to us? Do we need to do anything?

Visualization of #OpPetrol build up generated using Recorded Future.

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the open Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA
© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.