Nonprofit Security Firm Helps 19,000 Members Automate Malware Analysis

Center for Internet Security deploys Cisco® advanced malware security to accelerate response time to malicious attacks on U.S. government entities.

EXECUTIVE SUMMARY

CENTER FOR INTERNET SECURITY

- Security
- Albany, New York

CHALLENGE

- Resolve malware incidents for member organizations
- Automate malware analysis for prompt, accurate response
- Scale easily with increased incidents

SOLUTION

- A scalable infrastructure for analyzing thousands of malware samples
- An easy-to-use API for automated malware submission and resolution
- Threat intelligence feeds for real-time analysis of potential threats

BUSINESS RESULTS

- Cost-effective, automated malware analysis
- Context-rich threat content for timely and accurate action
- Deeper insights for proactive malware defense

Challenge

The Center for Internet Security (CIS) is a nonprofit organization that helps public and private sector entities improve their cybersecurity. CIS is also home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), a program designated by the U.S. Department of Homeland Security as a key cybersecurity resource for state, local, tribal, and territorial (SLTT) governments. The MS-ISAC includes members from all U.S. state governments, as well as U.S territories and tribal entities, along with hundreds of local governments.

Member or not, any SLTT government organization can take advantage of MS-ISAC cybersecurity assistance through its 24/7 operations center, which provides services such as managed security, incident response, malware analysis, and computer forensics.

Due to an ever-increasing number of malware attacks, CIS realized it needed a more scalable solution with a larger infrastructure and automated malware analysis for its MS-ISAC services. “There are millions of malware samples released into the public domain daily, and that number is increasing,” says Adnan Baykal, CIS vice president of security services. “In addition, the number of nation-state actor attacks is also growing, increasing our need for automated malware analysis in a trusted environment.”

CIS initially considered building an in-house infrastructure, but after further investigation determined it would be a cost-prohibitive approach for a nonprofit organization with limited resources. CIS began a search for a solution with an infrastructure that could manage a small volume initially, and then scale to handle thousands of malware submissions as needed. “At first we looked at many open-sourced solutions, but they didn’t offer the scalability we wanted,” says Baykal. “Plus, open source solutions are in the public domain, where the attackers are lurking. If they discovered our investigations, they could change their TTPs, or tools, tactics, and procedures, and make resolving the issues more challenging.”

Solution

Out of the many malware analysis platforms in the market, CIS chose Cisco AMP Threat Grid, which combines dynamic malware analysis and threat intelligence in a single solution. It also provides real-time behavior analysis and up-to-the-minute threat intelligence feeds, so CIS can respond quickly to its members.

> “We wanted a partner we could trust with a scalable infrastructure that could handle hundreds of thousands of malware samples a day. And that’s exactly what this solution provides for us.”
> **— Adnan Baykal, Vice President, Security Services, Center for Internet Security**

Baykal describes the solution as one that has the ability and ease to pivot around different malware samples in many different ways. “With Threat Grid, we can analyze a malware sample, and through just a click of a mouse button, pivot from a specific indicator and pull all the different malware samples that have the same indicator.” This gives CIS the ability to understand what the malware is doing or attempting to do, the scope of the threat it poses, and how to defend against it.

CIS uses Threat Grid to identify malicious code that is designed to evade analysis and analyze samples in real time with proprietary techniques that include static and dynamic analysis. In addition, the solution uses behavioral indicators and a malware knowledge base sourced from around the globe to identify whether a sample is malicious, suspicious, or benign—and why.

Using this context-rich threat content, the solution helps CIS understand specific threats that may need deeper analysis through Threat Grid. If there is an indicator for a specific domain, URL, or IP address, Threat Grid can provide thousands of indicators and malware samples, so CIS can identify whether or not it is a common threat. “Threat Grid provides the context we need to understand who is behind this attack and whether this specific threat is more general or targeted at a certain entity,” says Baykal. “The solution helps us cluster threat information and turn it into meaningful data. It allows us to correlate different malware samples in unique ways that tell us more about the malware and what we’re dealing with.”

Another capability of Threat Grid that Baykal and his team appreciate is the solution’s feature-rich API. “We built a completely different front end and customized the solution’s infrastructure to better serve the specific needs of our team and our members through role-based access controls,” says Baykal. The front end is named MCAP, which stands for malicious code analysis platform. “MCAP enables our members to build communities so that their incident response teams can submit and tag malware samples, and see other ones without sharing the specific nature of their samples with other community members.”

“We wanted a partner we could trust with a scalable infrastructure that could handle hundreds of thousands of malware samples a day. And that’s exactly what this solution provides for us,” says Baykal. “The depth of analysis is just what we needed, as was the ability to customize the solution for our members.”

Results

From the infrastructure perspective, the scalability of Cisco AMP Threat Grid is ideal for CIS, as are the advanced malware analysis capabilities and threat intelligence feeds. “When we submit malware, we get timely and accurate results,” says Baykal. “Plus, the threat intelligence feeds give us access to millions of malware samples and their indicators, which helps us to correlate and analyze malware samples from around the globe and build a complete threat picture.”

The MCAP front end is helpful to constituents as well. “When people use MCAP, they can submit information about malware, such as what kind of assistance—onsite or a phone call—they need, through a series of pull-down menus,” says Baykal. “After a submission, usually within minutes, they get their analysis results of the malware behavior. They’ll have an idea of the scope of the issue and all the indicators that they need to develop a reliable and accurate remediation recommendation.” For instance, network indicators most likely are shared with an entity’s network group to take precautionary measures at their perimeter firewalls or core routers to block specific IP addresses or domains.

With the breadth and depth of Threat Grid, CIS can see a more global threat picture. From there, CIS can decide on the appropriate actions, such as sending an advisory out to all its members with the malware indicators, so the entities can be more proactive with their defenses. And when government organizations need more guidance, CIS provides that, too, helping entities understand what they are dealing with, such as what a specific threat actor does, how it moves around, and what response is needed. If necessary, CIS can deploy a team onsite and help them with the incident response process.

“The transparency of the solution’s operation, the communication, and the uptime—which is critical—all confirm for us that we’re dealing with a partner that we can trust,” concludes Baykal. “We know we can rely on Cisco and that our members can rely on us.”

For More Information

To learn more about Cisco AMP Threat Grid, go to www.cisco.com/go/amptg, or view the CIS video case study here.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C36-735041-00 06/15