HOW A COMMON LANGUAGE FOR CYBER THREATS BOOSTS SECURITY

Cyber attacks are increasing in frequency, and government agencies are under constant attack. This nonstop assault is facilitated by the rapidly growing complexity of today's networks. Cloud-based services, internet-of-things devices, bring-your-own-device programs and wireless connectivity have dramatically expanded the threat landscape, creating a greater number and diversity of vulnerabilities.

To combat these threats, most agencies have stacked their security strategy with multiple security devices, typically from multiple vendors.

The problem is those devices often don't talk to one another. These interoperability challenges can hamper efforts to share cyber threat information across and between networks and frustrate attempts to respond to threats in a timely manner.

HIGHLIGHTS

Driven by the needs to standardize threat intelligence communications across various business applications on the network, implement open architectures and automate security tasks, security requirements for federal and local governments are in a state of flux. To remain responsive, resilient and agile, government organizations must adopt open, integrated and automated security architectures.

CREATING SPECIFICATIONS

The federal government and private sector agree on the need for a common language to enable the rapid exchange of intelligence. The first step, then, in sharing threat information is to standardize the structure and format of threat data so that it is interoperable across various networks and platforms.

Several groups have created technical specifications for this purpose. The U.S. Computer Emergency Readiness Team strongly encourages the use of the Trusted Automated eXchange of Indicator Information, or TAXII, the Structured Threat Information eXpression, or STIX, and the Cyber Observable eXpression, or CybOX. TAXII, STIX and CybOX are free, community-driven technical specifications that represent cyber threat information in a standardized format. They enable automated information sharing and thus foster cybersecurity situational awareness, real-time network defense and sophisticated threat analysis.

The National Cybersecurity and Communications Integration Center (part of DHS' Office of Cybersecurity and Communications) and US-CERT are supporting global adoption of these standards to be used around the world in order to enable nations to share information in the battle against cybercrime.

WHY INTEROPERABILITY IS CRITICAL

Interoperability between security tools is enabled by standardizing threat intelligence formats. Using an open API architecture, products and systems from different vendors can connect, share information and work as a unified security platform. Such a platform also supports end-to-end visibility across all components of a security architecture. This advantage is a force multiplier and the reason why government acquisition requirements specify open architectures and connectivity.

Another element that facilitates easier enforcement of government standards is an open architecture. This is the idea behind the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." This publication defines everything government agencies, and organizations working with government agencies, must have in place to secure their systems along with what is often extremely sensitive data.

ENABLING AUTOMATION

Orchestration and automation may be the most significant advantages governments obtain when they adopt standard threat information formats. It's no secret there is a cybersecurity talent shortage. To manage a growing volume of increasingly sophisticated threats, it is critical to have infrastructure and security tools that enable quick, automated and synchronized responses without human intervention.

The goal of Open C2 and other groups work is to expand the development of orchestration software and standardized command and control languages. Central to the OpenC2 movement's platform is the idea that standardizing language between machines enables rapid response to shared threat intelligence.

As the OpenC2 forum states, "Future defenses will require the sharing of indicators, the coordination of responses between domains, synchronization of cyber defense mechanisms and automated actions at machine speed against current and pending attacks."

Another benefit of standardized command and control languages and interfaces is they simplify integration. There's no need to train staff on every new technology in order to support enterprise adaptation and integration.

A HOLISTIC NETWORK SECURITY APPROACH

The vision for a more secure network is a holistic approach that automates the processing and analysis of threat information from many different sources. A system like this would rapidly detect network threats and then respond with a coordinated effort. These would be labor-intensive and time-consuming tasks to perform manually, but an automated process enables a security response almost instantaneous.

By standardizing threat information and command and control language and using open architecture, global cooperation is possible. This not only strengthens network security, but it also helps government agencies prevent breaches—all without adding to the payroll. The technology exists today to make this vision a reality, which should be pursued to maximize the safety of government and citizen data.

ABOUT FORTINET FEDERAL

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. We empower our customers with intelligent, seamless protection across the expanding attack surface, and with the ability to take on ever-increasing performance requirements of the borderless network - today and into the future. Our federal solutions protect the classified and unclassified systems used by 12 of 15 cabinet-level agencies, and those of numerous independent agencies, utilizing Fortinet's specially configured USG product line. These platforms comply with federal certification requirements including NIST FIPS 140-2, NIAP Common Criteria certification, and are on the Commercial Solutions for Classified Programs (CSfC) approved Components List. Learn more at www.FortinetFederal.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

Fortinet Federal, Inc.
12005 Sunrise Valley Drive
Suite 204
Reston, VA 20191
Tel: 703-815-7197
federalsales@fortinet.com
www.fortinetfederal.com