splunk>

Splunk's Input to the Commission on Enhancing National Cybersecurity

September 9, 2016

Executive Summary

The Commission on Enhancing National Cybersecurity issued a request for information about current and future states of cybersecurity in the digital economy. Splunk provides the following recommendations related to the topics of critical infrastructure cybersecurity, cybersecurity workforce, and cybersecurity R&D:

- Promote investment in infrastructure instrumentation to improve situational awareness in commercial and government organizations
- Advance the concept of "security by design"
- Promote adaptive security architecture and coordinated response
- Leverage machine learning, data analytics, and automation to help address cybersecurity workforce shortages
- Focus on big data analytics technology and infrastructure instrumentation in cybersecurity R&D that is conducted and funded by government agencies

Introduction

Splunk works with over 12,000 companies, government agencies, and universities to improve cybersecurity and information technology operations. Splunk provides a software platform for analyzing machine data and an industry-leading solution suite for security. A robust analytics-driven security solution can serve as a nerve center for an organization's cybersecurity operations. Because Splunk works closely with a range of government agencies and companies in key sectors of the economy, it is well-positioned to provide recommendations to improve the nation's cybersecurity posture.

From a broad point of view, improving cybersecurity at the national level will require a focus on several areas, including the following: developing a robust information-sharing architecture and

solution platform; promoting sound investments and best practices in the private sector; bolstering the cybersecurity posture of the federal government; strengthening national-level incident response capabilities; developing new capabilities to address cyber threats through innovation and technology leverage; and implementing an international strategy for deterring cyber threats.

Drawing on its area of expertise in the cybersecurity ecosystem, Splunk prepared the following more-targeted recommendations, which can complement recommendations provided by other stakeholders.

Promote investment in infrastructure instrumentation

A key challenge in cybersecurity defense is limited situational awareness about vulnerabilities and cyber threats. One promising approach to address this challenge is increased "instrumentation," which includes a network of sensors that collects data across all layers of the compute infrastructure and forwards data to a centralized location for analysis. The centralized location must have the ability to synthesize all available data sources into renderings that can facilitate decision-making to better protect the organization. Commercial and government organizations need to invest in increased instrumentation. Increased visibility into an organization's infrastructure can enable that organization to observe, orient, decide, and act at a pace quick enough to counter dynamic adversary movement.

Recommendation: Promote investment in infrastructure instrumentation to improve situational awareness in commercial and government organizations.

Advance the Concept of "Security by Design"

A second key challenge is that security is often added on as an afterthought, leading to a host of vulnerabilities that can be exploited by malicious actors. "Security by design" is a key approach to address this challenge. Security needs to be implanted in technology and information technology infrastructure from the early stages of conceptualization and design.

Recommendation: Advance the concept of "security by design" in best practices that are developed for and implemented by commercial and government organizations.

Promote Adaptive Security Architecture

A third key challenge relates to a heavy focus on prevention and manual response in a world where perimeter defenses are often inadequate and security breaches are constantly morphing and inevitable. The approach of "adaptive security architecture," which was included in Gartner's list of top ten strategic technology trends for 2016, focuses more on detecting and responding to incidents on a continuous basis. This approach can be implemented more effectively when various security technologies can work together seamlessly in a single environment.

Recommendation: Promote investment in "adaptive security architecture" and "coordinated response" in commercial and government organizations.

Leverage Technology to Help Address Cybersecurity Workforce Shortages

A number of studies have highlighted the shortage of cybersecurity workers. Training and education are key elements for addressing this challenge. Machine learning, data analytics, and automation can also play an important role in addressing the shortage by improving productivity of the cybersecurity workforce. Machine learning can be used to automatically correlate events, reduce alert noise, and conduct predictive analysis to warn of impending attacks. With this capability implemented, organizations can focus a limited cadre of cybersecurity workers on complex high-impact activities such as incident analysis, process improvement, tradecraft development, and advanced threat detection.

Recommendation: Leverage machine learning, data analytics, and automation to help address cybersecurity workforce shortages.

Promote Advances in Big Data Analytics Technology for Cybersecurity Through R&D

The Commission stated its interest in emerging technology trends and innovations, and the effect these trends and innovations will have on cybersecurity. Big data analytics is a transformational technology for cybersecurity. Advanced threats have permanently changed how organizations need to think about cybersecurity. It is no longer enough to monitor for known threats or to rely solely on security point products that provide a narrow view. Security teams need a holistic infrastructure-wide view of activities in order to identify, understand, and stop attackers. Analytics-driven security approaches, leveraging all sources of machine data, can enable better and faster human decision making by taking a risk-based approach to

cybersecurity. Big data analytics technology is already playing an important role in helping commercial and government organizations to improve cybersecurity, but there is great potential over the next several years to advance the state of the technology through innovation and robust R&D.

Recommendation: Focus on big data analytics and instrumentation in cybersecurity R&D that is conducted and funded by government agencies.

For additional information, please contact: cyber@splunk.com