Holistic Network Protection

Abstract

As organizations search for better ways to protect against cyber threats and data exfiltration, traditional techniques such as securing the perimeter and endpoints are known to be insufficient. Once inside, outsider threat actors are free to roam. Conversely, bad actors are already inside the enterprise with access to the network landscape. *Ever-present and current security threats beg the question: What is the best way to protect the enterprise while maintaining throughput?*

The emergence of Software Defined Networking and the power it offers through automation and orchestration, provides a new method of securing the network: Software Defined Secure Network (SD-SN). SD-SN allows organizations to operate the entire network as a single enforcement domain that makes every element a policy enforcement point. SD-SN is built upon these attributes:

Simplified Policy: Centrally managed across all network elements.
Distributed Detection: Sharing multi-source threat intelligence through a common cloud-based feed.
Immediate Enforcement: Adapting policy in real-time to all network elements.

LEARNING OBJECTIVES

At the end of this seminar, attendees will understand how SD-SN:

- Leverages the entire network to deliver a secure network and is comprised of three main components, using a bottoms-up and tops-down approach:
- Utilizes entire network infrastructure and the ecosystem itself, which includes all network elements such as switches, routers and firewalls, and that each element can provide threat intelligence and detect threats.
- Employs cloud-based threat defenses, which includes security intelligence feeds from all sources. It also includes cloud-based, scalable malware detection.
- Contains elements of a centralized, dynamic policy engine and controller that addresses all network components.

Speaker:

Danielle Zeedick, Ed.D., CISM, CBCP
Senior Cybersecurity Strategist, Juniper Networks
Dr. Zeedick is a professional consultant and educator with three decades of experience combining academic theory with practical industry experience. Her current areas of interest are in critical infrastructure protection including cybersecurity policy, governance, and risk management framework development for the US government and intelligence community. Dr. Zeedick's past experience included the development of large-scale, multi-site network systems and customized software applications for US government entities. She is a DOD 8570.01M/8140.01 IAM Tier III level (CISM) and a certified business continuity professional (CBCP). Her academic experience encompasses teaching at two NSA Centers of Academic Excellence in cybersecurity at Norwich University, a senior military academy in Vermont and The George Washington University in Washington D.C. where she is currently a professorial lecturer in computer science teaching information law and policy.