SOLUTION BRIEF

Communications Service Providers
Network Security

Rohde & Schwarz R&S®Net Sensor TAS Delivers Cyberattack Data

R&S®Net Sensor TAS utilizes Intel technology and open source Hyperscan software to help organizations protect against AI-powered threats with real-time network probing on up to 100 Gbps networks.

ROHDE&SCHWARZ

Introduction

Artificial intelligence (AI) and machine learning are two technologies that will have a significant impact on network and data center cybersecurity. The industry is preparing to utilize AI techniques in cybersecurity analytics programs to more quickly uncover potential attacks. These new tools, combined with layered security approaches that provide multiple roadblocks for cyberattacks, are being put in place to decrease the likelihood of successful penetration.

The success of these new defenses depends on a real-time flow of data packets provided by network probes that collect and process data packets, extracting metadata and content needed by these security systems in order to catch attacks as quickly as possible. The Rohde & Schwarz R&S®Net Sensor threat analytics system (TAS) leverages Intel® technology and open source software to provide the packet collection and processing needed on networks running at up to 100 Gbps.

Today's Cybersecurity Reality

Today's cybersecurity reality is that attackers are persistently probing defense systems and launching multiple attacks simultaneously in their search for profitable stolen data. Hackers are also turning to AI tools to better use bots for spam or phishing attacks, prevent attack detection with obfuscation techniques, and more efficiently use brute force methods for password cracking, among other techniques.

Information security executives are countering these trends with AI-powered systems of their own that utilize the technology in a range of security analytics products to better detect attacks and more quickly end them. Added to this technology advance is the use of "defense-in-depth" or "defense-in-concert" security strategies, which comprise multiple security layers surrounding the firm's most important data assets. The goal is to make a cyberattack have to break through all of the systems, which both slows the impact of the attack and increases the chances that one of the systems will detect the breach and stop it.

Some of the AI-powered security systems that are involved in a tiered defense include intrusion detection systems (IDS), inline intrusion prevention systems (IPS), network security monitoring (NSM), and online packet capture (pcap). These solutions typically perform high-speed content inspection by way of pattern matching, which is the ability to inspect all data against a database of security signatures.

All of these systems need access to data packets from the network with metadata and content extracted and ready for analysis. With a heritage in both service provider and enterprise networks, R&S®Net Sensor threat analytics systems (TAS) network probe by Rohde & Schwarz is leveraging Intel technology for use

on networks operating at up to 100 Gbps, ensuring that packets from the most vulnerable networks are available for advanced security inspection.

R&S®Net Sensor TAS

R&S®Net Sensor TAS by Rohde & Schwarz is a deep packet inspection network probe that offers a multifaceted approach to traffic analysis for cybersecurity. Employing the R&S®Net PACE 2 DPI engine to extract the traffic metadata and statistics, the DPI probe runs real-time filters with complex regular expression criteria powered by Hyperscan, an open-source software pattern-matching library, originally created by Intel. This allows third party threat analytics platforms to both be aware of the known types of intrusions, but also to build baselines, recognize anomalies, and perform advanced threat analysis.

R&S®Net Sensor

R&S®Net Sensor is an IP probe that allows enterprises, network operators, and service providers to extract meaningful network traffic and subscriber behavior data as well as to identify statistical trends. R&S®Net Sensor is designed to use network taps on a wide range of IP networks at speeds up to 100 Gbps to collect data, allowing the system to passively probe data center, enterprise, mobile, fixed, and converged networks at line speed.

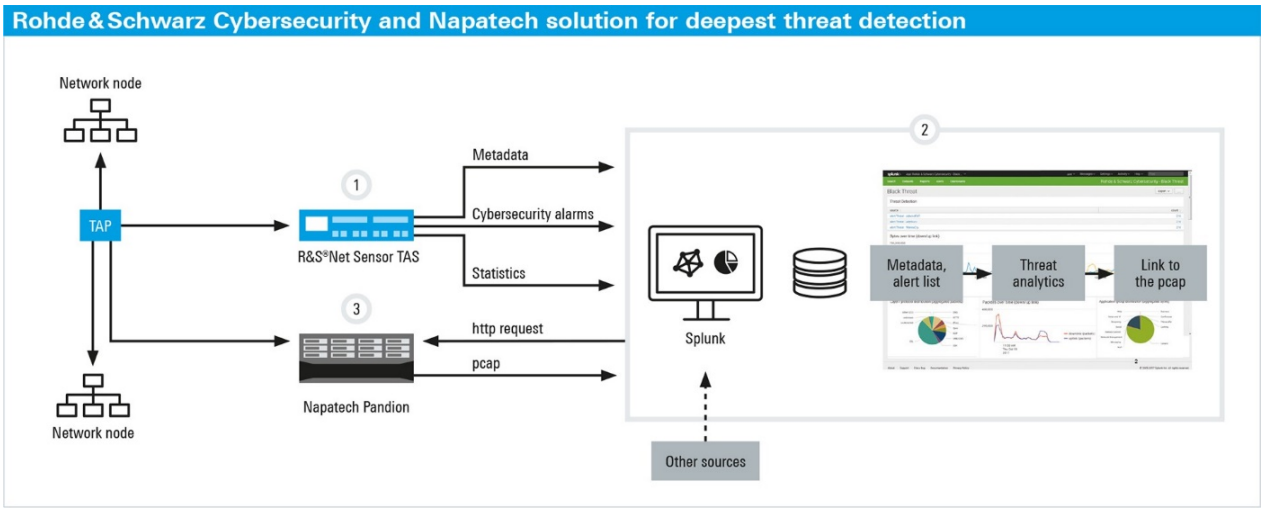

Figure 1. R&S Net Sensor capturing and processing data packets[1]

R&S®Net Sensor fully examines each data packet for attack possibilities at layers 3 to 7 and above. These classification results—as well as the control plane data (e.g., GTP-C, RADIUS, DHCP)—are communicated to other key R&S applications and security systems to provide specialized cybersecurity analytics.

For example, using the R&S®PACE 2 application classification engine, R&S®Net Sensor delivers high accuracy application and protocol detection of the 2,000 most-used applications and protocols from all geographical regions and across various business fields.

Detailed threat analysis comes from utilizing R&S®PACE 2, a state-of-the-art software library that uses deep packet inspection (DPI) and behavioral, heuristic, and statistical analysis to help protect against threats such as viruses, malware, and cyberattacks. The DPI analysis lets R&S®PACE 2 classify network protocols and applications and extract highly accurate metadata in real time, even if attackers utilize AI-based obfuscation or encryption techniques.

Employing the R&S®PACE 2 DPI engine to extract the traffic metadata and statistics, the DPI probe runs real-time filters using Hyperscan for complex regular expression criteria. Hyperscan is designed for IPS, AV, UTM, DPI, and other security applications that scan large data volumes at high speeds. The Hyperscan software develops, tests, and documents sets of operating system (OS)-independent, multithreaded pattern matching libraries.

Figure 2. Intel® Xeon® processor-powered R&S Net Sensor

Intel® Xeon® Processor Performance

The R&S®Net Sensor TAS software runs on appliances that leverage the Intel Xeon processor E5-2600 v4 family. Built on 14 nm processor technology, the Intel Xeon processor E5-2600 v4 family offers up to 22 cores/44 threads per socket and 55 MB last-level cache (LLC) per socket for increased performance, as well as Intel® Transactional Synchronization Extensions (Intel® TSX) for outstanding parallel workload performance.

For 10 Gbps and for 40 Gbps connections to terminal access points (TAPs), the R&S®Net Sensor utilizes Intel® Ethernet Converged Network Adapters X710 for flexible, high-performance network connectivity. For higher speed connections, the system has a TAP controller based on the Intel® Ethernet Multi-host controller FM10000. By leveraging this technology, the system can support connections with 50 Gbps, 100 Gbps or higher performance levels using load balancing functionality for high scalability.

Conclusion

The heart of evolving cybersecurity defenses is the network probe that collects and processes data packets for real-time distribution to security analysis systems. R&S®Net Sensor TAS delivers this data on Ethernet networks ranging up to 100 Gbps connectivity and high scalability. Utilizing Intel® CPUs, network controllers, and Hyperscan software, the R&S®Net Sensor TAS offers the performance to usher cybersecurity systems into an age of new AI-powered tools and network defenses.

About Rohde & Schwarz

The Rohde & Schwarz technology group develops, produces, and markets innovative information and communications technology products for professional users. Rohde & Schwarz focuses on test and measurement, broadcast and media, cybersecurity, security-enabled communications and monitoring and network testing, areas that address many different industry and government-sector market segments. Founded more than 80 years ago, the independent company has an extensive sales and service network in more than 70 countries. On June 30, 2017, Rohde & Schwarz had approximately 10,500 employees. The group achieved a net revenue of approximately EUR 1.9 billion in the 2016/2017 fiscal year (July to June). The company is headquartered in Munich, Germany, and also has regional hubs in Asia and the USA. www.rohde-schwarz.com

About ipoque

A Rohde & Schwarz company, ipoque is a global vendor of deep packet inspection software that adds protocol and application classification capabilities to network analytics, traffic management, and cybersecurity solutions. Rohde & Schwarz also provides a holistic network traffic analytics system for communication service providers that allows deep insights into network behavior, network performance and trends to optimize both quality of experience and quality of service. To find out more, go to www.ipoque.com

About Intel® Network Builders

Intel® Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at http://networkbuilders.intel.com.

[1] Figures provided courtesy of Rohde & Schwarz

0618/DO/H09/PDF ♻ Please Recycle 337736-001US