napatech

Case study: Advanced threat detection platform reduces response times

ROHDE&SCHWARZ
Cybersecurity

Industry pain points

In a world of software-defined everything, with trillions of endpoints and colossal volumes of data gushing through the network, the need for organizations to safeguard assets and resources is more acute than ever. According to Cybersecurity Ventures, attacks on businesses are up 15x in just two years – and damages are predicted to exceed $5 billion in 2017 alone, escalating from $325 million in 2015.

Threat intelligence platforms and Security Information Event Management (SIEM) systems provide an invaluable crutch for Security Operations (SecOps) teams to tackle attacks. But while these tools collect a substantial amount of event data, they cannot provide the complete packet history of what has been sent and received on the network. This requires a deeper layer of insight to substantiate, prioritize and resolve any events that look suspicious.

Challenge

Splunk is one of the most versatile SIEMs on the market, widely utilized to collect data from security, network, and server assets throughout the corporate infrastructure. However, in order to provide the needed insight into network security and performance, any unusual activity registered by Splunk must be prioritized and analyzed. This task involves condensing and ranking billions of logs, pushing SecOps teams to their utmost limit while gravely delaying incident response times.

"93 percent of security personnel are overwhelmed by alert data and unable to triage all potential threats."

Intel Security

Solution

To tackle this challenge, Rohde & Schwarz Cybersecurity partnered with Napatech to create an advanced network threat detection platform that leverages Splunk and other SIEMs. The platform provides 100% data visibility and granularity by capturing and logging every single packet, providing SecOps teams a tool to quickly pinpoint suspicious events and investigate these in depth.

Challenge

Any abnormal activity registered by Splunk or similar threat intelligence platforms must be prioritized and analyzed. This involves billions of logs, pushing SecOps teams to their utmost limit while gravely delaying incident response times.

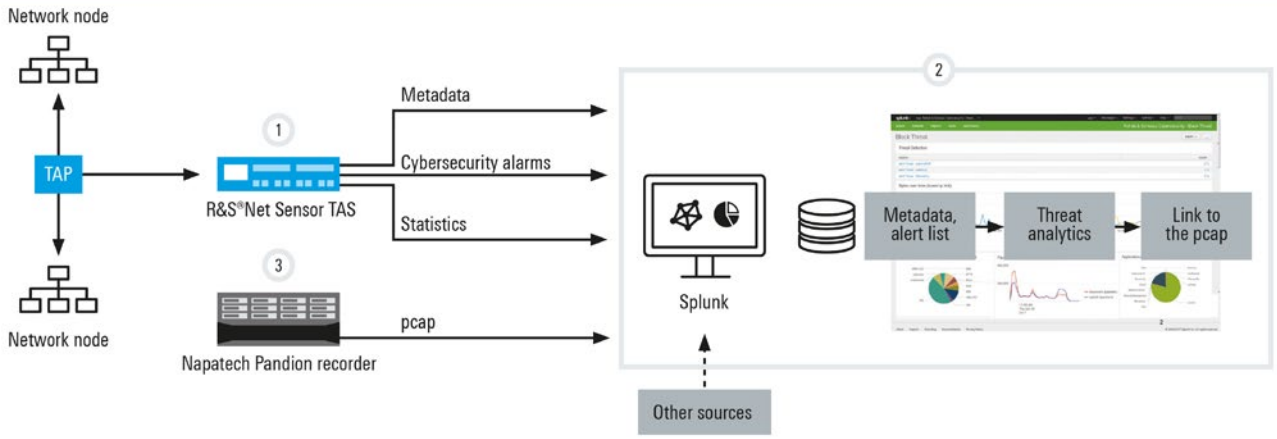
Solution

Rohde & Schwarz Cybersecurity partnered with Napatech to create an advanced network threat detection platform that leverages Splunk, allowing SecOps teams to quickly prioritize and investigate selected incidents at a granular level.

Benefits

- Full traffic visibility
- Instant access to detailed packet history
- Faster response times
- Seamless integration with existing Splunk or similar threat intelligence platform

Rohde&Schwarz Cybersecurity and Napatech solution for deepest threat detection



The solution takes a three-pronged approach:

1. **R&S Net Sensor TAS (Threat Analytics System)** performs deep packet inspection (DPI) on the traffic to extract metadata and traffic statistics and match these to known intrusion detection system (IDS) rules. TAS then forwards these findings to an analytics platform, e.g. Splunk.

2. **Splunk** presents the data acquired from TAS, performs additional threat analysis where needed based on the traffic metadata.

3. **Napatech Pandion Recorder** captures and logs every data packet in real time at up to 40Gbps. Large PCAP repositories can be maintained for extended periods, allowing Splunk, at any point in time, to instantly extract the desired data for further investigation.

Case

Consider a specific scenario where a security engineer is investigating a Splunk event, sent by TAS with a suspicious domain name. A corresponding event from the firewall indicates that a connection was attempted to the resolved address.

To further investigate this activity, the engineer clicks on the event in Splunk, uses the Pandion workflow, and in just a few seconds sees the full packet record corresponding to the name resolution and the subsequent connection.

Without this information, the decision to report or disregard the event would have been based on assumption alone. But by analyzing the packet data, the engineer can determine exactly what was sent/received to the suspicious address, whether a harmful document was downloaded, and if any information was sent out of the infrastructure.

Benefits

Based on this information, the security engineer can quickly resolve the Splunk event for severity and impact, determine the full scope of the event and instantly provide the needed remediation.

By combining classical IDS, full DPI and in-depth forensic capabilities, the platform empowers enterprises to detect known threats with a documented detection signature, as well as new anomalies that are difficult to spot using classical security tools. This increases visibility and greatly improves incident response times.

Key value adds include:

- Full traffic visibility
- Instant access to detailed packet history
- Faster response times
- Seamless integration with existing SIEMs

DN-1137 Rev. 1

EUROPE, MIDDLE EAST AND AFRICA
Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

NORTH AMERICA
Napatech inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.

Tel. +1 888 318 8288

info@napatech.com
www.napatech.com

APAC
Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

ntapacsales@napatech.com
www.napatech.com