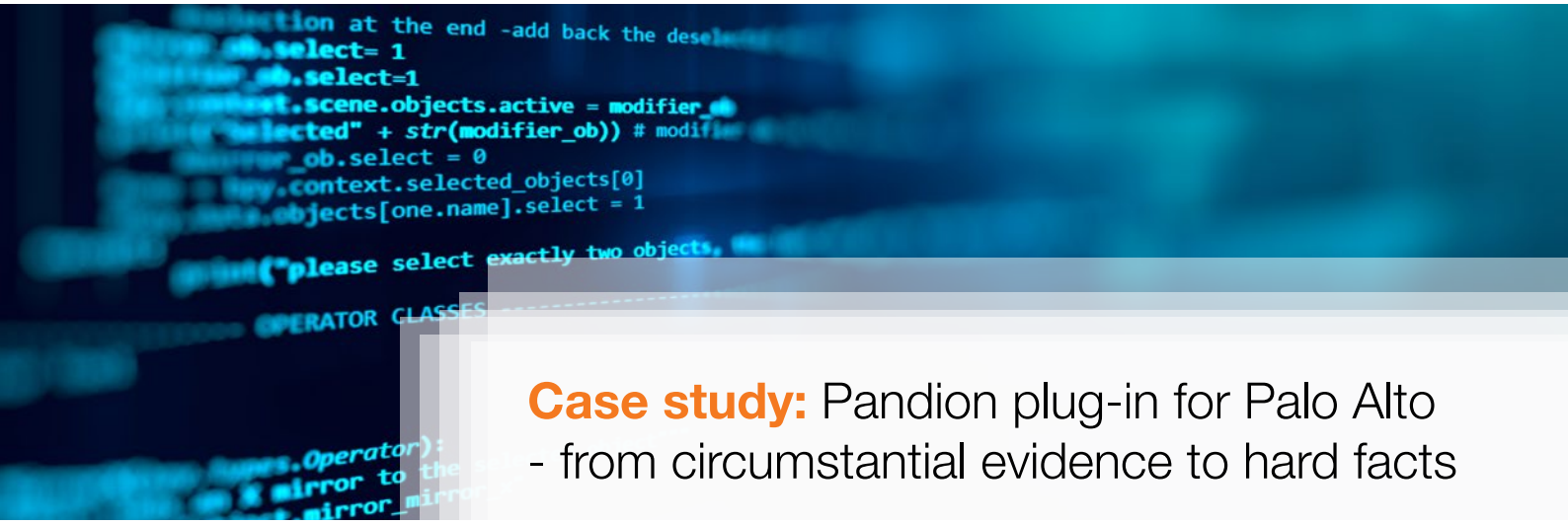
Credocom
WHEN IT HAS TO BE SAFE

napatech



Case study: Pandion plug-in for Palo Alto - from circumstantial evidence to hard facts

paloalto NETWORKS

Industry pain points

A key issue for security experts today is that the number of daily incidents massively exceeds their capacity. Ponemon Institute estimates that only about 4% of all malware alerts are investigated, which strongly suggests that organizations do not have the needed resources in place to detect or block malware.* In order to prioritize between the colossal volumes of events, quick determination of the incident severity is therefore paramount. But this requires instant and easy access to the hard facts.

"It costs organizations an average of $1.27 million per annum or approximately $25,000 per week in time wasted responding to erroneous malware alerts."

Ponemon Research

Challenge

Cybersecurity solutions such as Palo Alto firewalls are on the front line of preventing malicious attacks. But while Palo Alto excels at identifying, logging and dropping malicious flows, it lacks the ability to provide a retrospective forensic analysis of the context around the flow. The logs are high-level reports and offer circumstantial evidence at best, lacking the finer detail needed for full forensic/legal evidence. Users therefore need a fast and intuitive solution to investigate a specific security event.

Let us consider a specific scenario where a security administrator needs to view files downloaded from a specific website. The web security log flagged by Palo Alto informs the administrator that a user has downloaded a named file from the website - but it does not provide the needed capability to open the file and quickly determine whether or not the download is malicious.

To make that call, the security administrator needs an extra level of detail which can only be attained by looking at the actual packet trace associated with this session.

Challenge

While Palo Alto firewalls provide efficient logs for various security incidents, they cannot extract information on a detailed packet level. Many users therefore need a fast and intuitive solution to investigate specific security events and determine what needs to be prioritized.

Solution

Credocom, a Palo Alto Diamond partner and trusted provider of security solutions, has created a Palo Alto plug-in solution using the Napatech Pandion Network Recorder. This allows their customers to drill down into the details of each security incident.

Benefits

- Substantial time and resource savings
- Better context for more accurate forensic analysis
- Much faster detection and containment of breaches

* "The cost of Malware containment", Ponemon Research, January 2015

Solution

Credocom, a trusted provider of security solutions to IT organizations, has created a Palo Alto plug-in solution using the Napatech Pandion Network Recorder, which captures and writes all network data to disk at speeds from 1Gbps to 40Gbps without losing a single bit.

As a Diamond partner of Palo Alto, Credocom had the expertise and knowledge to create a log-link integration for the Napatech Pandion Network Recorder. The Palo Alto firewall provides a range of different log views of security incidents. These log views can be extended with “log-links” that allow external solutions to be “linked” with the log providing more details on the event in question. This allows the user to drill down for more detailed information based on network data packets captured to disk in real-time.

As part of the solution, Credocom created multiple ways to retrieve the data from the Napatech Pandion. One log-link opened the Napatech Pandion GUI interface with prefilled search fields relevant to the log in question. In addition, Credocom built a middleware solution that provided a quick and easy way to drill down and extract files related to specific logs.

Benefits

The Pandion Network Recorder provides the missing key ingredient for firewalls: by continuously capturing PCAP data to disk from tap points on the ingress links, the security administrator can retrospectively query the Pandion Network Recorder for the flow which was identified as malicious, logged and dropped by the Palo Alto firewall. The security administrator can also delve into the context around the flow providing him with hard detailed facts to the logged incident.

Value adds include:

- Substantial time and resource savings
- Better context for more accurate forensic analysis
- Much faster detection and containment of breaches

Napatech Pandion

In a time of data overload, relevance is everything. The Pandion network recorder enables you to seize all traffic in real time and retrieve only the relevant data on demand.

Napatech Pandion is based on Napatech SmartNICs available in a range of Ethernet interface options, with configurable storage and Napatech Pandion software.

Pandion builds on more than a decade of industry-proven Napatech FPGA technology and delivers 100% capture and write to disk for leading security analytics and compliance applications.

Find out more at:
www.napatech.com/products/napatech-pandion

Find more case studies at:
www.napatech.com/resources/case-studies

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