2018

Cybersecurity
RESEARCH

DEEP PACKET INSPECTION FOR THREAT HUNTING

ENEA
Qosmos Division

INTRODUCTION

Deep Packet Inspection (DPI) is one of the technologies frequently used in cybersecurity: DPI is embedded in products like NG firewalls, UTMs, secure gateways, and various threat analysis tools.

DPI sensors represent a new way of leveraging DPI: they strengthen an existing security tech stack inside high-end SOCs with detailed traffic intelligence and can significantly improve threat hunting for the most advanced attacks.

This report summarizes the findings of a survey by Cybersecurity Research among cybersecurity professionals, performed during the summer of 2018.

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Research

Cybersecurity
RESEARCH

THREAT HUNTING TEAMS

As cyber security threats have become more prevalent and more sophisticated, many organizations are creating threat hunting teams that use tools and tactics including advanced analytics to proactively find and address threats and vulnerabilities. Such a strategy will be necessary if enterprises and security service providers are to keep pace with the evolving threat landscape. Half of the survey respondents said their organization has a threat hunting team in place w hile the other half does not.

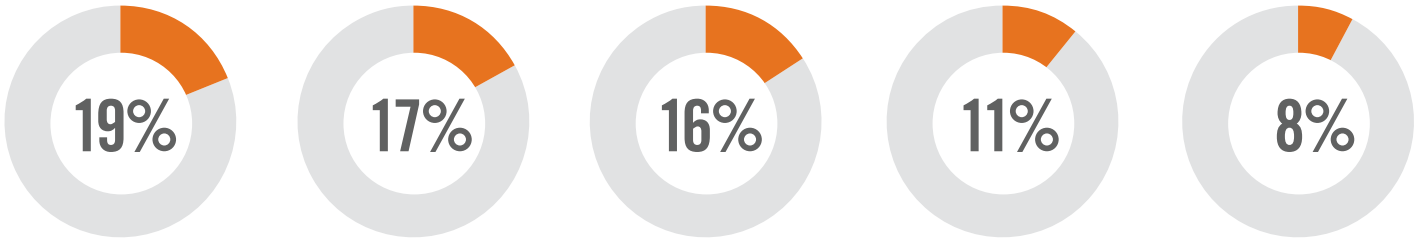
Do you have a Threat Hunting Team?

THREAT HUNTING TECHNOLOGIES

Respondents were asked to rank by importance, from 1 (most important) to 7 (least important), a variety of technologies they use or would use for cyber threat hunting purposes. About one quarter (24%) ranked security information and event management (SIEM) software as most important. Other key technologies include next-generation firewalls (cited by 19% as most important), intrusion detection systems/intrusion prevention systems (17%), DPI sensor (16%), full packet capture (11%), and anti-phishing (8%).

Which of these technologies do you use / would you use for Cyber Threat Hunting purposes?

24%
SIEM



NG Firewall

IDS/IPS

DPI
Deep Packet Inspection sensor

FPC
Full Packet Capture

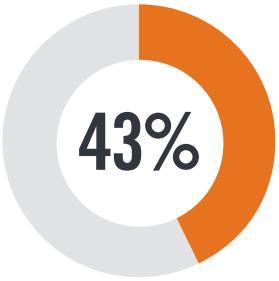
Anti-phishing

MAJOR CHALLENGES OF THREAT HUNTING

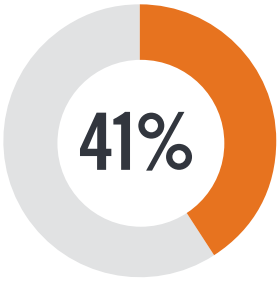
Easily the most common challenge organizations face regarding data for threat hunting is a lack of resources to analyze the data, cited by about two thirds of the respondents. Other challenges noted are that existing information is not precise enough (43%), there is too much data related to threat hunting (41%), and there is not enough data (22%).

What is your major challenge regarding Data for Threat Hunting?

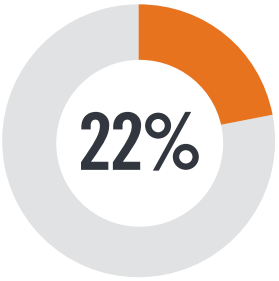
63% Lack of resources to analyze Data



Existing information not precise enough



Too much data



Not enough data

DPI SENSORS

Deep packet inspection (DPI) is an advanced method of analyzing network traffic: it identifies protocols and applications behind each IP flow, using a combination of advanced techniques including stateful inspection, behavioral and statistical analysis, and heuristics.

DPI software provides full visibility into network traffic up to Layer 7, including protocol details such as file types, file extensions, volume and content.

When asked if they were familiar with DPI sensors or probes, about two thirds of the respondents (64%) said they were familiar, while the remaining 36% were not.

Are you familiar with Deep Packet Inspection (DPI) sensors (or probes)?

DPI SENSORS FOR THREAT HUNTING

About one third of the organizations surveyed (31%) are using DPI sensors to strengthen cyber threat hunting. Another 45% are planning to use DPI sensors in the future and 24% have no plans yet to use the technology.

Do you use DPI sensors to strengthen cyber threat hunting?

Using today
31%

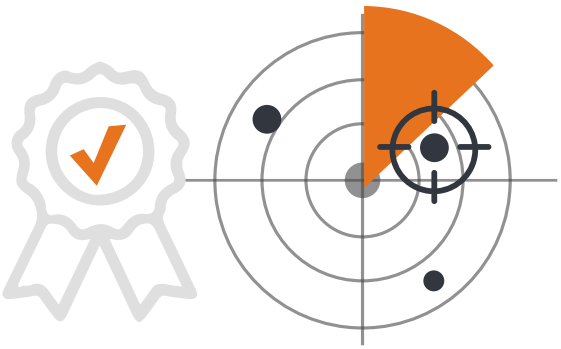
Planning to use in the future
45%

No plans yet
24%

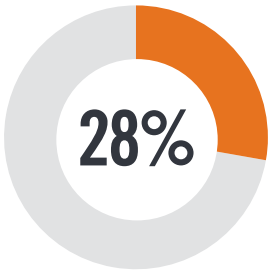
REASONS FOR USING DPI

Organizations are using DPI sensors for multiple reasons. When asked to rank the reasons by importance, 42% of the respondents gave "to improve network data visibility and analysis depth" the highest rank. Other reasons cited were "to strengthen IPS/IDS rules" (ranked as highest by 28%), "to shorten investigation time" (21%), and "to limit size of forensic data" (7%).

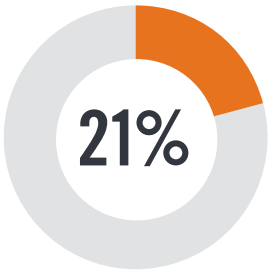
Why would you use DPI sensors?



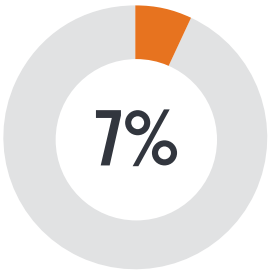
42% To improve network data visibility and analysis depth



To strengthen IPS/IDS rules



To shorten investigation time

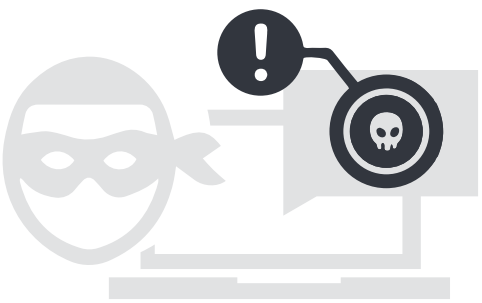


To limit size of forensic data

MITIGATING CYBER THREATS

DPI can help organizations mitigate a number of cyber threats. Respondents were asked to rank threats from 1 to 5, in terms of the impact of DPI in helping to mitigate threats. More than half of the respondents (50%) gave advanced persistent threats (APT) the highest rank. Other threats that DPI can help mitigate include malware and insider threats (50%).

Which cyber threats would DPI help to mitigate?



50% Advanced Persistent Threats (APT)

50% Others (Malware, Insider threats, etc.)

DPI SENSOR INTEGRATION

DPI sensors work in conjunction with a number of other security technologies. The largest percentage of respondents (65%) said DPI sensors should be integrated with SIEM systems. Next was IDS (61%), followed by sandboxing (58%), firewall (48%), and other technologies (26%).

With which systems should the DPI sensor be integrated?

65% SIEM

61%
IDS

58%
Sandboxing

48%
Firewall

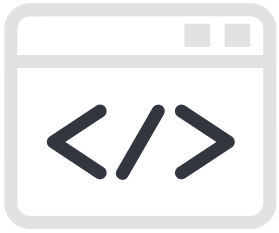
SOURCE OF FORENSIC INFORMATION

Organizations need to store a variety of information for forensic and other analysis purposes. At the top of the list is logs, cited by 89% of the respondents. Next most common are traffic metadata (URLs, email sender, file name, login, etc.), which was mentioned by 85%, and full packet capture (64%).

What information do you need to store for forensic or other analysis purposes?

89%

Logs



85%

Traffic metadata
(URLs, email sender, file name, login, etc.)

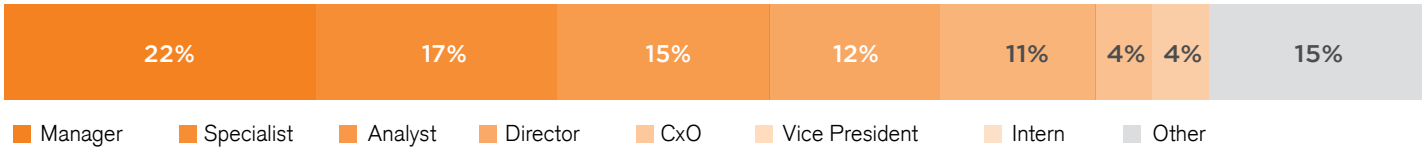
64%

Full Packet Capture (FPC)

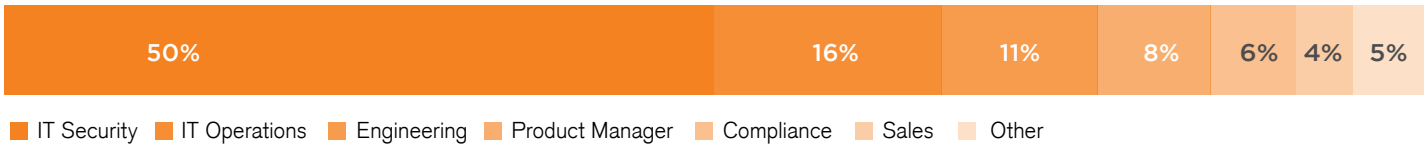
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest security threats faced by organizations and the solutions available to prevent and remediate them, including Deep Packet Inspection.

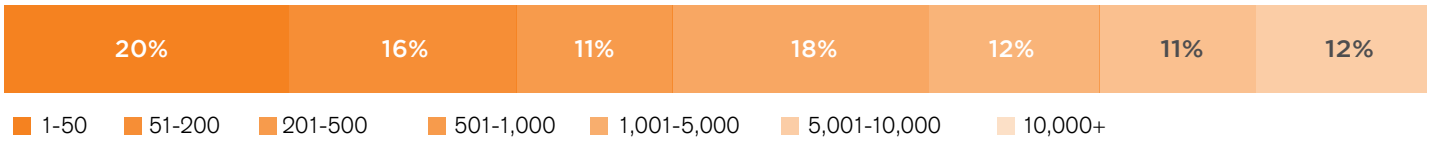
CAREER LEVEL



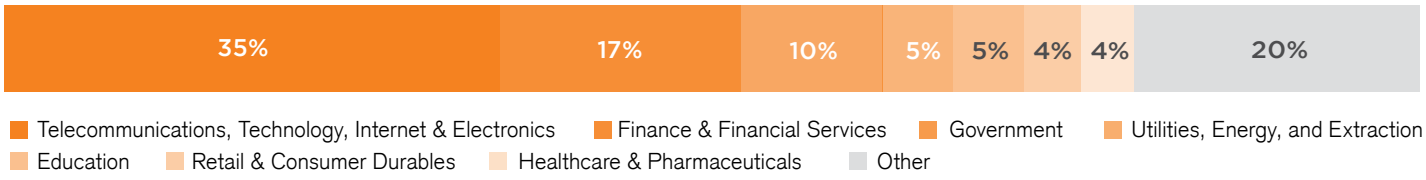
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSOR OVERVIEW

ENEA
Qosmos Division

ENEA Qosmos Division | www.qosmos.com

Enea develops the software foundation for the connected society. Solution vendors, systems integrators, and service providers use Enea to create new world-leading networking products and services. More than 3 billion people around the globe already rely on Enea technologies in their daily lives.

The Qosmos Division of Enea specializes in Deep Packet Inspection (DPI) software, which recognizes thousands of protocols and metadata to provide the most accurate picture of real-time data activity on networks. As a DPI Sensor, the Qosmos Cyber Probe strengthens threat hunting through efficient data analysis and traffic visibility up to the application level:

- Analysis of data flows in real time at n x 10 Gpbs, up to Layer 7
- Recognition of over 3100 protocols and ability to extract more than 5000 metadata
- Fewer false positives when using information from the probe to improve IDS rules
- Forensic data reduced by up to 150x compared to full packet capture