Network Security Forensics For GDPR Compliance

An effective network security forensics strategy can assist an organization in providing key compliance-related details as part of any post-incident GDPR investigation.

The European Union's General Data Protection Regulation (GDPR) will come into effect on May 25, 2018 and will apply to all organizations that provide services to residents of the European Union (EU), regardless of whether they are based in, or operating out of, EU territory. These regulations apply to the collection, handling, and storage of personal data from EU citizens.

In the event of a data breach, organizations risk severe penalties for noncompliance with the regulation. With that in mind, it is important for all organizations to understand the GDPR compliance requirements. Businesses should have processes and systems in place to not only prevent and detect data breaches but also to identify what data has been compromised, when the data breach occurred, how it happened, and why it happened.

There is a lot of discussion in the industry about security and attack prevention and detection, but given the level of potential fines for breaches and increasing number of successful attacks, organizations need to have a post-event investigation strategy in place.

GDPR Overview

In 1995, the European Parliament published data protection directive 95/46/EC on the protection of individuals regarding the processing of personal data and the free movement of such data. An EU directive was transposed by the individual 28 EU member states into local law.

The GDPR replaces this earlier directive. An EU regulation is different from a directive in that it is a legal act of the European Union that becomes enforceable as law in all member states simultaneously. It is the most important change in data privacy regulation in 20 years and has been developed to strengthen the online privacy, rights, and data protection of individuals residing within the EU. The GDPR was created to ensure "Privacy by Design" and modernizes the data protection obligations of businesses servicing EU citizens through a single regulation, and adds real penalties to organizations found in violation of regulations with fines of up to €20 million or 4 percent of their previous financial year's global annual turnover.

The key changes in the GDPR reform that will impact IT and network operations teams include:

- Individual Data Rights
  - Notification: Individuals' right to know when sensitive data relating to them has been breached. Organizations must notify the national supervisory authority of data breaches which could put individuals at risk and communicate to the person concerned all high-risk breaches as soon as possible so that users can take appropriate measures. Organizations are legally obligated to notify the national supervisory authority of serious data breaches within 72 hours.

- Penalties

  Organizations that do not comply with the GDPR rules can face fines of up to €20 million or 4 percent of their global annual turnover of the previous fiscal year, whichever is higher. The amount of the fine on a noncompliant organization is determined by the following ten criteria:

  1. Nature of infringement: Number of people affected, damage suffered, duration, and purpose of processing
  2. Intention: Whether the infringement is intentional or negligent
  3. Mitigation: Actions taken to mitigate damage to data subjects
  4. Preventative measures: Technical and organizational preparation the company or organization implemented to prevent noncompliance
  5. History: Past infringements, which could include any breaches under the previous data protection directive and not just the GDPR
  6. Cooperation: How cooperative the company or organization has been with the supervisory authority to remedy the infringement
  7. Data type: Type of data involved in the infringement
  8. Notification: Whether the breach was proactively reported to the supervisory authority by the company or organization itself or a third party
  9. Certification: Whether the company or organization qualified under approved certifications or adhered to approved codes of conduct
  10. Other: Other aggravating or mitigating factors may include financial impact on the firm from the infringement

- Applies Globally

  The GDPR applies to all organizations located within the EU as well as organizations located outside of the EU if they offer their goods and services (including free goods and services) to EU residents, or monitor the behavior of EU residents. It, therefore, applies to any multinational organization conducting business with EU residents and impacts how personal data is collected, accessed, stored, and exported outside of the EU.

Personal Data Defined

Article 4(1) of the GDPR defines personal data as follows:

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.

To ensure GDPR compliance, organizations must take comprehensive measures to not only mask and protect personal data of European citizens, but to quickly investigate and disclose the scope, impact, and details around any security breach. Identifying this information post-breach will require an effective network security forensics strategy.

Prevention, Identification, and Remediation

When it comes to data breaches and the protection of network integrity, significant time, energy, and resources are allocated toward preventative measures. According to security organization SANS Institute, nearly three-quarters of organizations allocated security budget for protection and prevention of threats, compared to fewer than one-third who were invested in discovery and forensics solutions.

In spite of significant resources focused on prevention, the number of disclosed security incidents globally involving loss of sensitive data increased to 1,093 in 2016 compared to 780 breaches reported in 2015, according to the Identify Theft Resource Center. This represents a 40 percent increase in one year.

Given an increased frequency, organizations need new strategies and solutions in place to respond quickly to security incidents, protect data subjects and business interests, comply with GDPR regulations and to facilitate any subsequent investigations that will follow.

In the event of a data breach, organizations must be able to identify what data was breached, when it happened, where in the network it happened, and why, and how data was breached. To comply with the GDPR, organizations have 72 hours to inform the national supervisory authority of breaches that may pose a risk to individuals and need to be able to determine the extent of the data breach.

If no personal data was involved in a data breach, and the breach poses no risk to individuals, the organization does not have to report the incident. It is therefore important to identify and have conclusive proof of the type of data involved in a breach to avoid unnecessary data breach notifications which could damage the organization's hard-won brand reputation.

Answering the Who, What, When, and Where

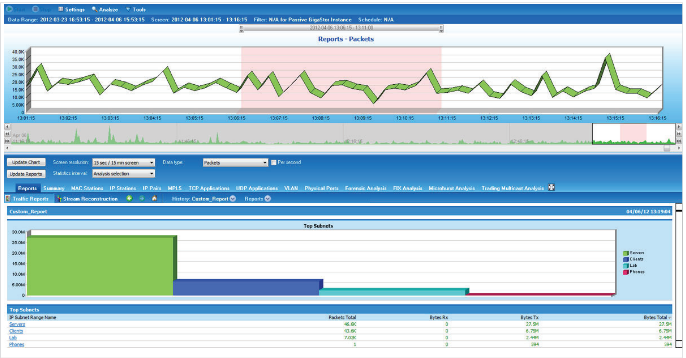
For GDPR compliance, it is critical that an organization can identify the extent of a data breach with regard to the type and the amount of data involved, the data subjects impacted, and the risk to those subjects as a result of the data breach. To detect and investigate breaches, organizations may use a variety of tools including intrusion prevention systems (IPS), security incident and event management (SIEM) systems, or third-party log analytics that draw either from metric-based data, including system log files or flow data for detection and analysis.

While these tools can monitor, prevent, and alert on security incidents, there are limitations in having only metrics as well as variability in quality of the logging data available. These factors can impede the investigation team's ability to understand the full nature of an attack and the extent to which it was successful in compromising an organization's IT assets and sensitive data.

Security operations teams frequently do not have access to important network forensics information like historical packet captures and packet-derived metadata to fully undertand and resolve security incidents. In reaching out to network teams, investigation efforts can tap into long-term packet monitoring solutions, commonly refered to as network performance monitoring and diagnostic (NPMD) solutions, that capture, store, replay, and analyze all network traffic. IT can use packets to reconstruct network conversations. These network conversations along with the underlying packets can provide the most complete picture of what exactly happened when a network-based security breach occurred, facilitating quick GDPR post-event security forensics investigations.

Long-Term Packet Capture: Critical to Security Forensics

The long-term capture of packet or wire data is best achieved by placing a dedicated appliance on the network to capture, encrypt using AES-256 encryption, and store all network packets, therefore recording and securing all network traffic without dropping, slicing, or manipulating the wire data in any way.



Data Range: 2012-03-23 16:53:15 - 2012-04-06 15:53:15 Screen: 2012-04-06 13:01:15 - 13:16:15 Filter: N/A for Passive GigaStor Instance Schedule: N/A

Screen resolution: 15 sec / 15 min screen
Statistics interval: Analysis selection
Data type: Packets
□ Per second

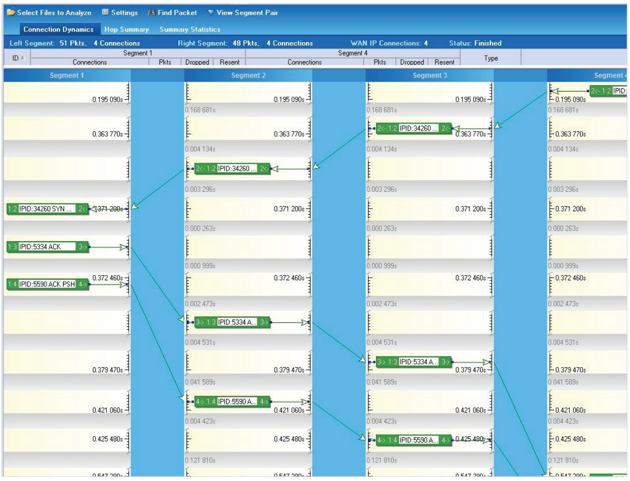
History: Custom_Report

Custom_Report 04/06/12 13:19:04

Top Subnets

IP Subnet Range Name	Packets Total	Bytes Rx	Bytes Tx	Bytes Total
Servers	46.6K	0	27.5M	27.5M
Clients	43.6K	0	6.75M	6.75M
Lab	7.02K	0	2.44M	2.44M
Phones	1	0	594	594

The appliance itself acts as a closed-circuit television (CCTV) system for the network, and with all network packets captured, encrypted, and safely stored, network traffic can be replayed and data breaches and attacks can be reconstructed as part of an investigation. The reconstruction can provide a complete picture of the circumstances surrounding an attack.



Left Segment: 51 Pkts, 4 Connections Right Segment: 48 Pkts, 4 Connections WAN IP Connections: 4 Status: Finished

ID	Segment 1				Segment 4				Type
	Connections	Pkts	Dropped	Resent	Connections	Pkts	Dropped	Resent	

Of the ten criteria used to determine the fines issued for organizations found to be forensics with the GDPR, complete capture of traffic can help organizations prove compliancy in terms of the following:

- Nature of infringement
- Intention
- Mitigation
- Preventative measures
- Cooperation
- Data Type

Capturing, encrypting, and storing all network traffic has many benefits, including:

1. Pre-incident auditing

Additionally, NPMD solutions with long-term capture can assist an organization in proving as part of any post-incident GDPR investigation, that it had taken sufficient preventative measures to protect against network attacks prior to a security incident occurring. Utilize application dependency maps derived from packet data to identify devices involved in the collection, analysis, and storage of personal data. This can be achieved by reconstructing network messages for a period prior to the attack as evidence that the breach did not occur because of insufficient security measures, but because of malicious external interference during the time of the attack. It can also prove that sufficient plans are in place to enable effective investigations into any data breaches.

2. Post-incident digital forensics investigations

Long-term packet capture and forensic analysis can assist an organization during an investigation with the following:

✓ Demonstrate innocence if there was a data breach and that no data was compromised, therefore proving that the nature of the infringement was not serious

✓ Prove that the infringement was not intentional, but due to unforeseen circumstances

✓ Prove that actions were taken to mitigate damage to data subjects

✓ Provide the organization with the required evidence and information to enable the organization to fully cooperate in a timely manner with the supervisory authority to remedy the infringement

✓ In the event of a serious infringement, long-term packet capture helps identify and document what data was compromised or touched, how access was achieved, and what time the data breach occurred

✓ Determine where an attack originated

✓ Identify any users involved in the breach

✓ Validate that any malware has been removed

Organizational Benefits

There are several reasons why network performance monitoring and diagnostic (NPMD) solutions will be of benefit to organizations and network operations including:

- NPMD will save time in understanding what data was breached and when it happened, and protect the reputation of the organization by allowing them to avoid any unnecessary data breach notifications where personal data was found to have been unimpacted by the data breach.
- Assisting in maintaining GDPR compliance by ensuring organizations have all the information needed to notify users within 72 hours following a data breach, and facilitate GDPR – related investigations.
- Troubleshooting application and network – related performance and security issues.
- Corroborating the network is free of malware.
- Identifying abnormal traffic in real time, or back-in-time.
- Providing forensic evidence for internal and external network attacks.

NPMD tools used for security investigations should meet the following requirements:

- Full Network Packet Capture – All network packets are captured, encrypted, and securely stored to enable the reconstruction of network conversations for forensic investigation purposes. Missing or dropped packets in a capture would mean missed analysis, and that could invalidate security analysis findings.
- AES-256 Encryption – Packets captured are encrypted with AES-256 encryption before being stored on disk.
- Future-Proof with 40 Gb Capabilities – Complete packet capture at gigabit and 10 Gb with 40 Gbps ingress network capture performance, allowing for network growth.

Viavi Solutions Overview

Viavi is a global leader in both network and service enablement, optical security, and network performance products and solutions.

Overview of Viavi Observer Platform:

The Viavi Observer Performance Management Platform enables IT organizations to capture packet-level data, ensuring that no data is missed in the investigation of a network security attack or breach.

At the heart of the packet capture solution is Observer GigaStor. Deployed as appliances, GigaStor can be easily mounted in a standard rack unit. The Observer nTAPs included in the product can be utilized to insert or remove a GigaStor appliance on the network without disruption to traffic flow. GigaStor reports back to Observer Analyzer Expert Edition and Suite consoles for in-depth analysis.

The Observer Platform is the first independently certified NPMD solution capable of capturing and storing network packets on gigabit, 10 Gb, and 40 Gb networks with 40 Gbps ingress network capture performance. It's the fastest independently validated NPMD packet capture, analytics, and storage solution that captures all data critical for the accurate reconstruction of end-user experience and security events. It is important that all data is captured as missing packets in a capture would mean missed analysis, and could invalidate security analysis findings.

The Observer Platform enables administrators to set baselines and alerts to identify anomalous traffic in real-time, or back-in-time with easy-to-use interfaces built on sophisticated analytics algorithms. It enables organizations to quickly understand key network security attack details, how it was perpetrated, the exploits used in the attack and the systems, intellectual property, or user data compromised during the attack.

The Observer Platform uses web-based trace extraction to integrate with third-party, real-time security tools for fast network security forensics investigations.

About the Author

Rynardt Spies is a Cloud Automation Consultant with a strong background in enterprise infrastructure design and implementation. He first started out in IT as an application developer in C++ and Oracle before moving to infrastructure in 2005. Having worked as a consultant in private and public sector government and defense infrastructure projects over the past 12 years, Rynardt has a thorough understanding of the entire infrastructure stack, with experience in the design and deployment of PCI-DSS compliant infrastructures in the banking sector, and secure infrastructures for defense organizations.

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.