SOLUTION GUIDE

GDPR: Meeting the 72-Hour Breach Notification Requirement

Recognizing the need to adopt consistent rules and regulations around the use and retention of personal data, the European Union (EU) consolidated many data privacy regulations into one law that standardizes many disparate rules and processes.

The intent of the General Data Protection Regulation (GDPR) is to protect EU citizens from personal breaches. Unlike previous privacy rules, it applies to the collection of personal data of EU citizens anywhere in the world, regardless of the physical location of the company doing the collecting. With the increased reliance by companies of all sizes on cloud services to store and manage data, this legislation will have a global scope.

One of the most significant changes from previous legislation is that organizations must report breaches that result in a "risk to the rights and freedoms of natural persons" within 72 hours. The potential penalty for organizations is up to 4% of annual global turnover (global revenue) or €20 Million (whichever is greater).

Lastline Defender™

- Delivers the automated detection and analysis of malicious behavior you need to quickly assess the scope of a breach to meet the 72-hour deadline.
- Identifies every malicious behavior and every system affected, from initial compromise to lateral movement of the attack to external C&C communication and data exfiltration (if any).

72 Hours for Breach Notification

After becoming aware of a breach, you have only 72 hours to assess the scope of the breach and determine your responsibility to report it. The reporting requirements described in Article 33 are very specific:

- The nature of the personal data breach including where possible:
  - The categories and approximate number of data subjects concerned
  - The categories and approximate number of personal data records concerned;
- The likely consequences of the personal data breach;
- The measures you'll take (or propose to be take) to address the personal data breach, including measures to mitigate its possible adverse effects.

In those few hours after you have determined a breach occurred, you will have to collect and analyze a wide range of information from across your network from a variety of sources. Two challenges most organizations will face in providing this information within the 72-hour window are:

1. Understanding the scope of a data breach, including the specific systems compromised, number of records and the type of data affected
2. Understanding the cause of the data breach and how you will mitigate the breach

The Need for Automated Detection and Analysis

The security products most organizations have deployed today lack the ability to perform automated breach detection and analysis in the context of GDPR reporting. They were designed to identify specific behavior at specific locations in your network, and the alerts they generate are often generic and lack context.

As a result of these design limitations, your incident response team has to spend significant amounts of time manually investigating these alerts, verifying their accuracy, and correlating related activity to generate an accurate analysis of any potential data breach.

With only 72 hours to create a complete picture of the cause and effect of any suspected breach, your incident response team will not have time to conduct the manual analysis it's doing today. You will need to automate much of the detection and analysis of the malicious activity to meet the reporting deadlines imposed by GDPR. Otherwise, you may spend the entire 72-hour time period simply trying to gather data.

Data Breaches By the Numbers

- 68% of breaches took months or longer to discover
- 48% of breaches included hacking
- 30% of breaches included malware
- 46% of ransomware incidents included malware
- 73% of breaches are perpetrated by outsiders.

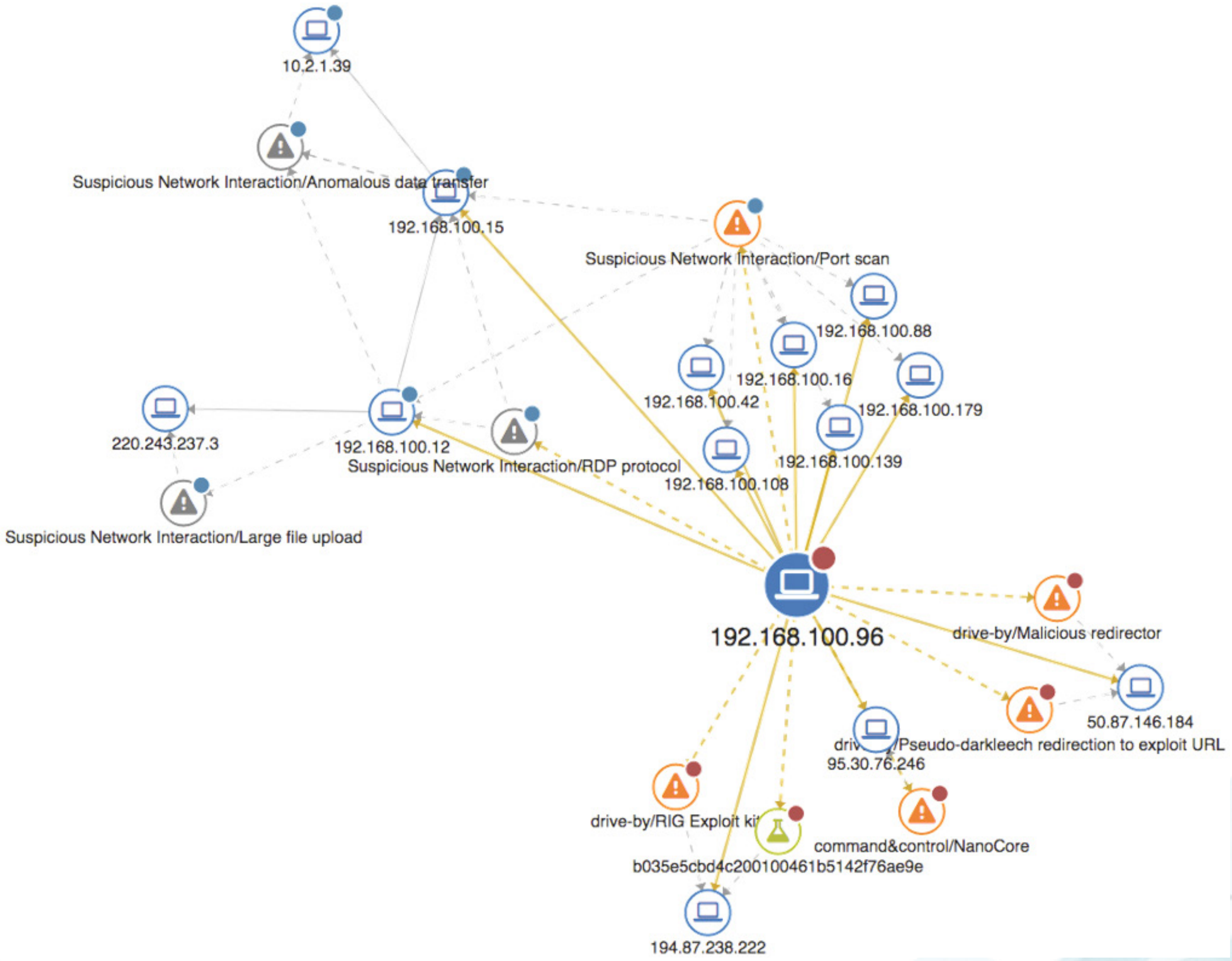
Verizon 2018 Data Breach Investigations Report

Lastline Defender: The Automation and Visibility You Need to Respond in 72 Hours

Lastline Defender delivers unmatched AI-powered network security. It provides you with the automated detection and analysis of malicious behavior, as well as complete network visibility you need to quickly assess the scope of a potential breach to meet the 72-hour deadline.

It enables your under-resourced security teams to respond faster and stop the most advanced threats from entering or operating within your network and causing business disruption. It accelerates and simplifies your ability to answer these critical questions:

- How did the threat actors initially compromise your network
- Once inside, how did they move across your network
- What systems, applications and data did they touch
- What external systems communicated with the compromised systems
- What data sets did they exfiltrate


10.2.1.39
Suspicious Network Interaction/Anomalous data transfer
192.168.100.15
Suspicious Network Interaction/Port scan
192.168.100.88
192.168.100.16
192.168.100.179
192.168.100.42
220.243.237.3
192.168.100.12
Suspicious Network Interaction/RDP protocol
192.168.100.108
192.168.100.139
Suspicious Network Interaction/Large file upload
192.168.100.96
drive-by/Malicious redirector
50.87.146.184
driv /Pseudo-darkleech redirection to exploit URL
95.30.76.246
drive-by/RIG Exploit kit
command&control/NanoCore
b035e5cbd4c200100461b5142f76ae9e
194.87.238.222

Complete Threat Visibility
Quickly understand the full scope of any suspected data breach, all affected systems, applications

Defeat Advanced Threats

It enables your under-resourced security teams to respond faster and Lastline Defender's unique approach to applying AI to network security significantly improves your cyber resilience and reduces your cyber risk. It secures your enterprise across the entire attack chain: it protects network and systems from inbound threats by blocking known and unknown attacks, it detects threats operating inside your environment, and it drives automated response.

Our AI learns from both Network Traffic Analysis (NTA) and malicious behaviors to eliminate false positives and deliver the highest fidelity insights possible into threats entering or operating within your network, including compromised personal devices and rogue IoT devices. This innovative approach to network security provides the critical context that other technologies lack.

The result is "AI Done Right."

AI Done Right

Your existing security team and security controls are more effective on day one with Lastline Defender. Its deterministic alerts eliminate false positives than other approaches and fewer generic alerts that require additional investigation. Your security team will finally have the confidence to automate many of your threat response workflows. This means better enterprise security with fewer resources.

AI-Powered Threat Detection

Lastline Defender uses a combination of three complementary techniques to deliver superior AI-powered network security:

- First, we leverage our Global Threat Intelligence Network to scan traffic metadata and payloads for variants of known threats
- Second, we apply unsupervised AI to an organization's network traffic to detect protocol and traffic anomalies
- Third, we use supervised AI to automatically create classifiers that recognize malicious network behaviors and previously unknown malware

Most AI-based network security products implement only the first two detection techniques. These probabilistic approaches lead to many false positives requiring additional investigation by your security team.

Lastline Defender is different. It leverages AI that is automatically trained both on network traffic and malicious behaviors. This unique combination enables deterministic detections and eliminates false positives.

Unmatched Awareness of Threats Entering Your Network

Lastline Defender also gives you unmatched visibility into threats attempting to enter your network by incorporating our industry leading, patented sandbox technology. It deconstructs every malicious behavior engineered into an object entering via mail or web traffic, such as a file attachment or download. It sees all instructions that a program executes, all memory content, and all operating system activity.

This visibility enables your security team to see a complete inventory of unique file behaviors that other tools fail to detect, such as activity observed when executing programs, opening documents, unpacking archives, and rendering web content.

Lastline Defender's superior visibility also makes the analysis much harder to evade. It detects advanced malware that's engineered to evade sandboxes, next-generation firewalls, and other next-gen tools.

Global Threat Intelligence

The Lastline® Global Threat Intelligence Network is a repository of tens of millions of indicators of compromise and historic threat data for files, domain names, and IP addresses. It is continuously updated and communicated to partners and customers as new threats (and new relationships among existing threats) emerge.

As a result, all Lastline customers and partners are immediately instrumented to detect any malicious object used to attack another member of our community. This "network effect" significantly increases your detection accuracy and reduces the need for you to conduct your own threat research.

Experience the Lastline Advantage

For more information please visit www.lastline.com

LASTLINE CORPORATE HEADQUARTERS
203 REDWOOD SHORES PARKWAY
SUITE 500
REDWOOD CITY, CA 94065

AMERICAS: +1 (877) 671 3239
EMEA: +44 (0) 207 749 5156
APAC: +65 6829 2207
WWW.LASTLINE.COM

lastline™