
SOARing Above the Clouds of GDPR Compliance

# Introduction

Happy GDPR Day! You're ready, right?

Kicked back, feeling relaxed and compliant?

Okay...maybe not.

Odds are, you are still grappling with these new regulations, as a recent Forbes Insights study found that just 6% of surveyed organizations feel they're fully prepared to meet the requirements of GDPR.

# Security Orchestration

No such thing as a silver bullet for complying with GDPR – or for anything in cybersecurity, for that matter – exists.

However, **security orchestration, automation, and response (SOAR)** inherently provide benefits that can help get your organization a little bit closer to reaching GDPR nirvana.

# What Is GDPR

We won't spend much time here, as the General Data Protection Regulation (GDPR) has been covered extensively since it was approved by the European Union (EU) Parliament on April 14, 2016. As a quick refresher, GDPR is legislation that updates and unifies data privacy laws across the European Union (EU). This directive is mainly intended to keep businesses more transparent and expand privacy rights of individuals and their personal information. The regulation applies to all data produced by EU citizens wherever it resides, as well as people whose data is stored in the EU, regardless of whether they're an EU citizen.

# Major Requirements of GDPR

Three major requirements of GDPR have the strongest impact on the day-to-day operations of security teams:

Security Level – organizations need to implement an appropriate level of security that will allow them to prevent data loss or any unauthorized data processing operations.

Security Auditing – organizations are expected to audit and maintain records of their security activities and take corrective action, where appropriate

Data Breach Notification – organizations must report breaches within 72 hours of awareness of the breach.

# Data Breach Notification

The third requirement is one that has caused much hand-wringing among companies subject to GDPR.


Seventy-two hours is a much faster timeline than we've seen in the majority of breaches – for reference, Equifax waited six weeks to disclose its breach to customers and Target only confirmed its breach after the KrebsOnSecurity blog reported it publicly.

# Data Breach Notification

The third requirement is one that has caused much hand-wringing among companies subject to GDPR. Seventy-two hours is a much faster timeline than we've seen in the majority of breaches – for reference, Equifax waited six weeks to disclose its breach to customers and Target only confirmed its breach after the KrebsOnSecurity blog reported it publicly. Rapid breach notification necessitates an overhaul of internal processes and infrastructure for most organizations, and even with two-years' notice of the new regulations, many companies still aren't prepared to meet this stringent criterion.

# Security Orchestration For GDPR

By its nature, **security orchestration solutions** provide SOC teams a high degree of visibility by bringing together disparate technologies and processes. When implemented and used correctly, having this bird's-eye view of your entire security footprint can result in the improved mean time to detect (MTTD) and mean time to respond (MTTR) as well as the ability to report accurately on security incidents. This gives your organization an advantage when trying to satisfy GDPR requirements, particularly those tied to the breach notification window.

# Advantage #1 : Playbooks

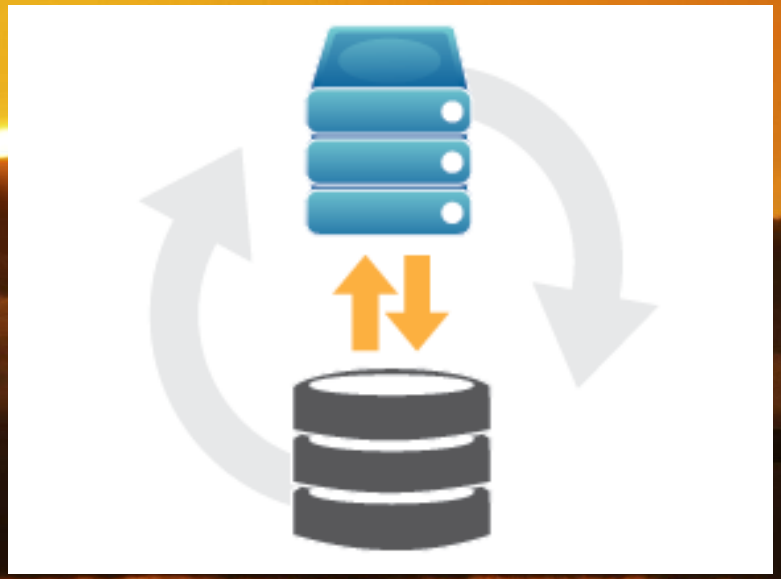
Many teams still rely on the individual experience of their analysts – or tribal knowledge – to drive processes. Operating in this manner not only leaves huge room for error but also makes for a ton of manual work when it comes to documenting and proving security levels and activities as required by GDPR. Playbooks as part of a SOAR solution codify security operations processes and ensure they are executed consistently throughout the SOC. And, when automation is applied to various playbook steps, security operations teams are able to identify and respond to security events more quickly.

# Advantage #2 : Auto Reporting

Security orchestration enables robust reporting, with the ability for teams to create customized dashboards for KPI tracking as well as output reports on individual alerts, cases, and incidents. Automatic reporting mechanisms that are part of some SOAR solutions take this a step further by making it possible for organizations to automatically alert customers as soon as something has happened, which can help companies as they work to achieve the 72-hour notification window prescribed by GDPR.

# Advantage #3 : Database Backup

Part of maintaining data privacy includes having a backup and restore capabilities in place to ensure that recovery is possible in any situation. As you look at SOAR solutions relative to GDPR, make sure your platform of choice has a built-in database backup and restore processes to keep sensitive data safe.



# Advantage #4 : Entity Explorer

Unique to Siemplify's **security orchestration and automation platform** – and arguably the most important attribute on this list as far as GDPR is concerned – is the ability to see all the data collected on a user in one click. The platform consolidates and labels data that is collected from a variety of systems in an organization. Analysts can quickly and easily drill down into a given entity and send the necessary data to a user on demand. This feature significantly accelerates the investigation and discovery of security events and streamlines an organization's ability to report and notify as necessary.

# Conclusion

So, take a deep breath and relax (a little). GDPR compliance is possible with the right mix of tools and processes plus smartly applied security orchestration to bring it all together.