

German MSSP greenhats Accelerates Ability to Provide Real-Time Identity Intelligence in Line with DORA, NIS2, and IT Security Act 2.0

Ensuring Oversight in Line with Policy


The European Union (EU) has led the charge of data protection and cybersecurity regulation. In 2018, the General Data Protection Regulation (GDPR) created the broad extraterritorial jurisdictional requirements that sought to protect EU citizens, wherever they live, and people residing in the EU, regardless of citizenship status. In 2022, the European Commission updated its Directive on Security of Network and Information Systems (NIS2) and required Member Countries to enact implementing laws to standardize compliance across the EU in 2024. To add to this onslaught of regulations, the European Parliament's Digital Operational Resilience Act (DORA), specific to financial services, went into effect on January 17, 2025.

Across these different regulatory compliance requirements, proactive threat detection and risk management is a fundamental commonality.

For example, DORA includes a definition for “threat-led penetration testing” as a framework mimicking threat actor tactics, techniques, and procedures (TTPs), information gained from threat intelligence. Meanwhile, NIS2 requires organizations to provide incident reports based on a threat's severity, including a final report within a month of submitting the notification that contains the type of threat or root cause that triggered the incident. As organizations across the EU work to implement the appropriate controls, many found that their previous processes for threat intelligence collection and dark web monitoring lacked comprehensive intelligence and efficiency needed.

The Customer

 German MSSP serving clients that provide essential services across financial services, energy, healthcare, manufacturing, and the consumer packaged goods industries

 Services include continuous threat exposure management (CTEM), external attack surface management (EASM), vulnerability management, real-time dark web monitoring, penetration testing, and code audit



With all the European Union and German data protection laws, customers want to have comprehensive coverage and understanding about their external threat exposures. Implementing automated identity intelligence monitoring made sense for our team and our customers.

- Paul Werther, CTO, greenhats

Challenge: Time-Consuming Manual Processes Created Inefficiencies

As a Germany-based MSSP, greenhats works with organizations across multiple highly regulated industries that fall within the definition of critical infrastructure, such as financial services, energy, healthcare, and manufacturing. These customers need to comply with European-wide data laws as well as Germany's IT Security Act 2.0 which expanded the third-party audit requirements for these customers. Because of these compliance requirements, customers across the German market are very conscious about data privacy and collection.

Most customers' leaked or stolen credentials would be found in clear web leaks, dark web forums, or illicit Telegram channels. However, greenhats struggled with time-consuming, resource intensive manual processes that limited their data scraping to twice per year, taking 1-2 days to complete. The organization found maintaining a current list of Tor addresses, Telegram channels, and dark web forums overwhelming as they continuously change. The security researchers would need to reinvestigate multiple resources before engaging in an actual investigation, meaning the MSSP struggled to gain real-time threat actor insights. To provide the proactive monitoring customers wanted and needed, greenhats sought out an identity intelligence solution.

Implementation: Near-Instant Added Visibility

After seeing the Flare solution in action, greenhats signed up for the free trial that provided unlimited access to the platform, including complete workflow capability. After the easy onboarding process, greenhats achieved near instant benefits by swiftly finding numerous previously unknown threats, including identification of compromised devices. While the MSSP had access to a large number of dark web sources prior to Flare, it could now engage in real-time monitoring. During the demo phase, greenhats gained which provided significant benefits including:

- Monitoring typosquatting domains
- Identifying domains registered for deploying targeted phishing attacks against customers
- Confirming data source accuracy

The greenhats penetration testing teams dramatically accelerated their information gathering by using Flare's automation capability and substantial data feeds, enabling them to conduct more sophisticated attacks. In true pentester fashion, greenhats has shared its past resources with Flare, which have contributed to improvements in the Flare platform. greenhats' offensive security expertise has promoted a fantastic partnership for both organizations!



Of course the onboarding process was really simple. We appreciated that everything we set up in the free trial and demo transferred over to production so we could get right into identity intelligence monitoring. In some other demo experiences we lost everything from the demo and had to start over.

- Paul Werther, CTO, greenhats

Ultimately, greenhats chose Flare because of the ease-of-use and straightforward pricing model that offered greater value, as competitors' packages cost more per identifier.

Benefits: Scaling Business, Generating Revenue, and Elevating Security Posture

After setting up the demo environment, greenhats was able to transfer all workflows and data from their free trial account to their subscriber account, simplifying the onboarding process. With Flare, greenhats is able to automate clear & dark web monitoring as well as structure the unstructured data. As a comprehensive API-first platform, greenhats was able to build custom tools and solutions around Flare, even during the trial phase. As they expanded these capabilities, they leveraged Flare's AI features to help them make rapid, informed decisions based on large data volumes. As a Flare customer, greenhats monitors its own domains and trademarks, upleveling its own security program. Recently, the Flare platform sent a low-priority alert identifying an open bucket with a file name containing its company name. In greenhats' investigation:

- They found the alert had identified a company logo image shared with external identities.
- As greenhats explored further, it identified another misconfigured S3 bucket containing sensitive data from a new supplier.
- The company reported the issue to the supplier and the supplier's IT team closed the bucket by the end of the day.

Although the S3 bucket had only been exposed for 2 days, Flare's real-time monitoring enabled the rapid response that protected the sensitive data. The supplier is also now a happy greenhats customer after seeing the value the MSSP brings by wielding the Flare platform. By integrating Flare into their services, greenhats scaled its business, even having customers on an internal waiting list for the new identity intelligence offering that included dark web monitoring. Using Flare to eliminate manual information gathering processes, greenhats security analysts focus on reviewing alerts to provide customers a zero-false-positives managed EASM to a wider range of customers and provides a standalone dark web monitoring product focused on smaller companies and government institutions.

Looking Ahead

In the future, greenhats seeks to expand its offerings by focusing on the health and critical infrastructure sectors. The new EU mandates require organizations to provide prompt incident notifications. However, these regulated organizations often struggle to find and retain qualified personnel with specialized sector experience. To meet these needs, greenhats plans to leverage Flare's capabilities with their threat intelligence platform to integrate more automated tasks while escalating critical events to their internal pentest and cyber defense experts.

Gartner 4.9
Peer Insights™ ★★★★★



[Sign Up for a Free Trial](#) →