ElastiFlow

CASE STUDY:

How mittwald Achieved Deep Visibility and Faster Threat Detection with ElastiFlow

Overview

mittwald, a German web hosting provider, supports a diverse range of business-to-business (B2B) customers, especially focusing on agencies. Its network team previously faced challenges with manual, limited traffic monitoring capabilities.

To overcome these challenges, mittwald adopted ElastiFlow NetObserv and, more recently, NetIntel. These solutions deliver deep visibility into network traffic, allowing the team to quickly detect and mitigate security threats like distributed denial of service (DDoS) attacks with increased efficiency.

mittwald.
Hosting neu gedacht

Challenge:

- Limited visibility made it difficult to detect smaller-scale DDoS attacks.
- Network growth and evolving threats require a more comprehensive observability solution for faster threat detection and risk mitigation.

Solution:

- Implemented NetObserv for enhanced network traffic visibility and deeper insights into data flows.
- Integrated NetIntel to enrich network traffic data, helping the team filter out noise and focus on real threats.

Results:

- Increased detection and shorter response times.
- Streamlined attack mitigation, with quicker identification of attack sources and the ability to respond faster.

Challenge

mittwald supports a variety of B2B customers that resell its services to their clients. As mittwald's network grew, the team faced challenges with existing traffic-monitoring processes and needed to improve visibility.

"Many of our network-monitoring tasks were tedious and time-consuming," says Fabian Kretschmer, network engineer at mittwald. "For some systems we had to look at the plain logs, and filter out the desired information manually, which wasn't an enjoyable process."

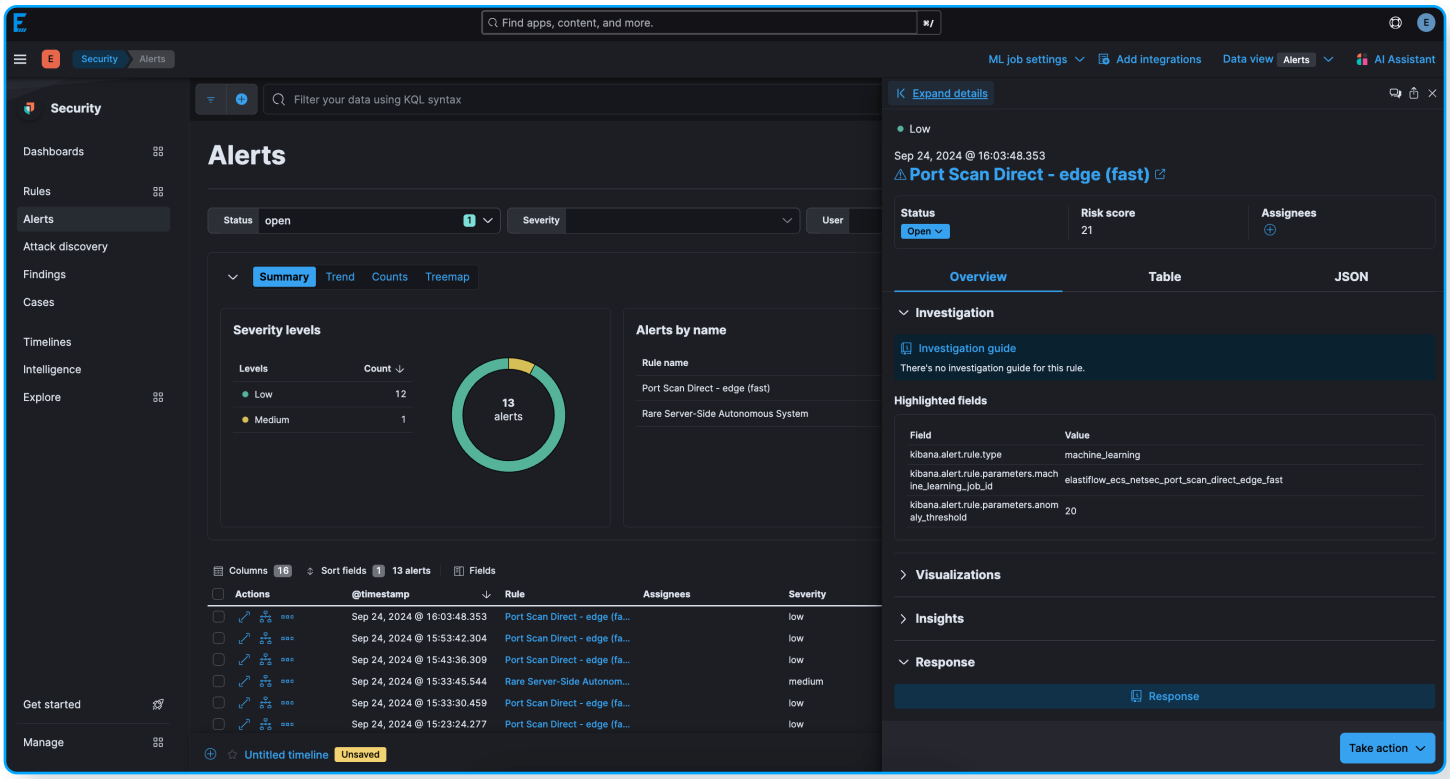
While the team could manually monitor some details, they lacked the depth and insight required into exact traffic flows to show what was happening on the network.

This limited visibility made it more challenging to detect and mitigate DDoS attacks. While larger-scale incidents were often easier to detect, smaller attacks required more-advanced detection tools.

> "Many of our network-monitoring tasks were tedious and time-consuming"
>
> **Fabian Kretschmer**, Network Engineer, mittwald

mittwald's team realized they needed a comprehensive network observability solution to provide deeper insights into traffic flows.

They sought a solution to improve their ability to detect and respond to threats faster, including keeping up with advancing DDoS threats.



Solution

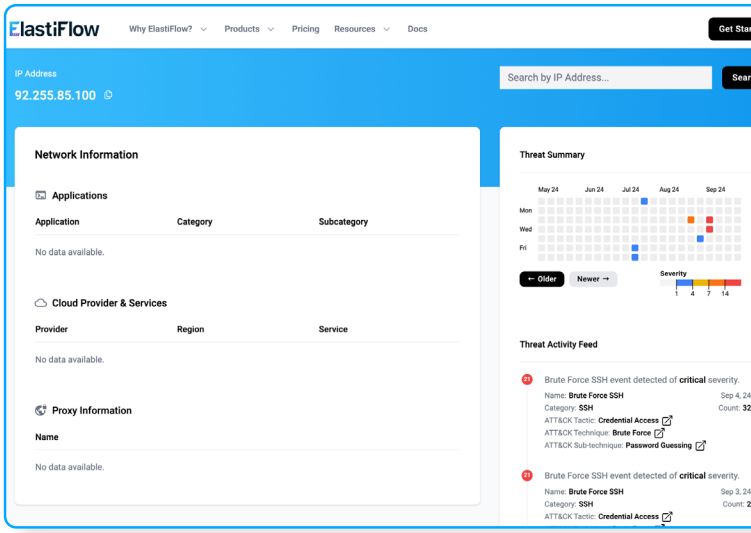
mittwald initially adopted the basic version of ElastiFlow to monitor its network traffic. This solution significantly improved its visibility into traffic flows compared to its previous technologies and manual processes.

“We got it up and running in a day,” says Kretschmer. “The documentation is well done—it walks you through the entire setup and even offers guides to implement flow monitoring for different vendors.”

> “We got it up and running in a day”
>
> **Fabian Kretschmer**, Network Engineer, mittwald

More recently, mittwald implemented ElastiFlow NetIntel to enhance its security capabilities. This feature enriches internal and external network traffic data, helping the team focus on genuine threats while filtering out noise.

“Getting started with NetIntel was simple,” Kretschmer explains. “We just added our license and it was ready to go.”



Key benefits of the NetIntel solution included:

Improved network flow visibility.

NetIntel helped Kretschmer’s team enrich traffic data with details like autonomous system numbers and geographic coordinates. “The enrichment feature was easy to implement and gives us deeper insights when querying data,” notes Kretschmer.

Faster threat detection and mitigation.

With NetObserv and NetIntel, mittwald can now detect and respond to security threats, such as DDoS attacks, far quicker than before. Automated notifications and response capabilities allow the team to minimize disruptions and protect customers.

Faster attack response.

The solution allows mittwald to quickly pinpoint the source of attacks, whether large-scale events or small ones, allowing them to take faster actions, such as IP blacklisting or activating “black holes,” to mitigate the impacts.

“With NetObserv and NetIntel, we are getting notified about the small attacks,” says Kretschmer. “Before using the solution, we only had our SNMP monitoring, which had very limited visibility, and now we really get the knowledge we need to respond quickly.”

Results

After implementing NetObserv and NetIntel, Kretschmer's team has achieved significant time savings compared to their previous approach, which relied on many manual processes. Key results include:

Increased threat detection and response

By leveraging NetIntel's easy integration, enabled with a simple license update, the team has improved its ability to detect and respond to security issues.

Faster mitigation of security threats

With detailed traffic insights from ElastiFlow, the team could easily identify the source of an attack and take quicker mitigation actions. "ElastiFlow has saved us a lot of time and trouble," notes Kretschmer.

Increased readiness for evolving threats

As attacks become more sophisticated and smaller in scale, high-frequency threats could go unnoticed. Kretschmer highlights the importance of having a solution like NetObserv and NetIntel to stay ahead of these risks.

Measurable impact on mitigation speed

Kretschmer notes that the ability to reduce security threat impacts is huge for his team. "We measure success by how fast we can mitigate a DDoS attack without impacting our customers, and that's really fast with NetObserv and NetIntel," says Kretschmer.

ElastiFlow

NetObserv and NetIntel have empowered mittwald to proactively address security threats, reduce the time required for detection and mitigation, and ensure ongoing network protection.

The solution's ease of use and effectiveness have positioned the team to handle the sophistication and scale of future threats and provide their customers with the best protection possible.

About ElastiFlow

ElastiFlow provides network flow data solutions that deliver valuable insights for network and security professionals. Whether for business, healthcare, entertainment or social connection, we all depend on the reliability, performance and security of network infrastructure. ElastiFlow was created to provide the visibility and insights necessary to make this world possible.

Additional information can be found at ElastiFlow Inc. (www.elastiflow.com) or connect with ElastiFlow on Twitter and LinkedIn.