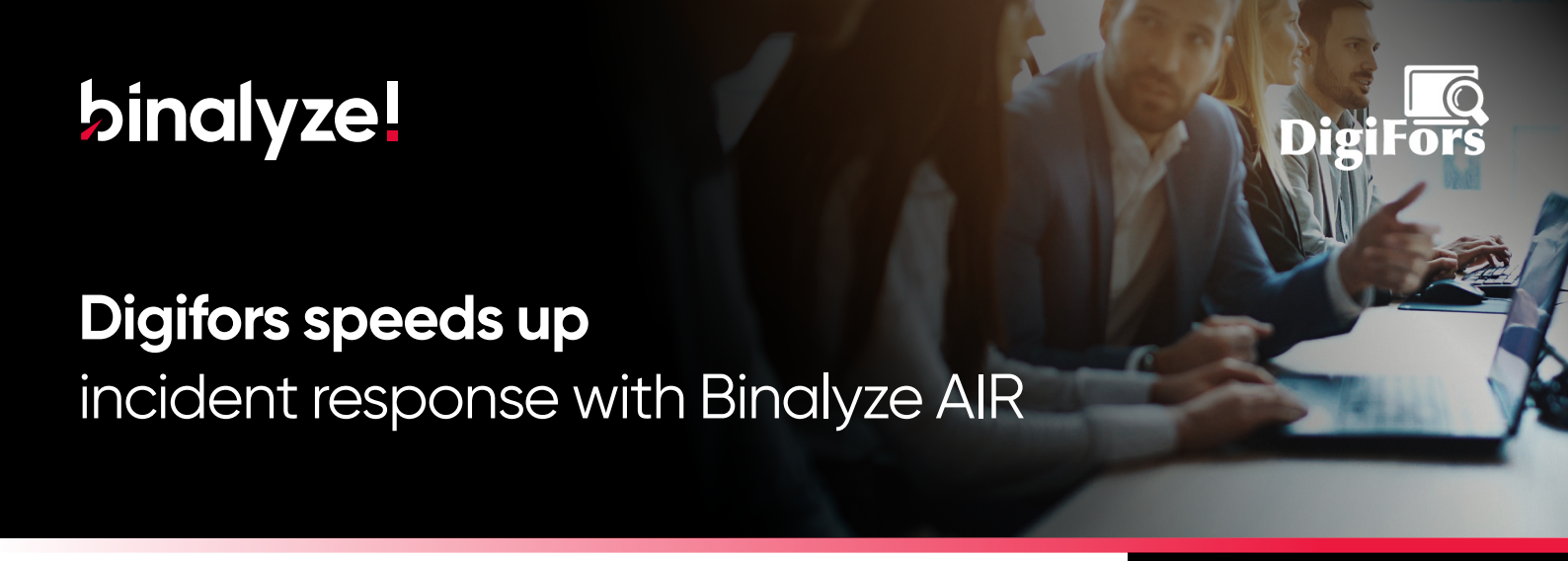

Digifors speeds up incident response with Binalyze AIR

Challenges

DigiFors needed a digital forensics and incident response platform that would help them capture evidence and investigate quickly at scale, remotely identify the assets requiring further focus, and accurately report information to their customers.

Introduction to Challenges and Problems

DigiFors is a respected German cybersecurity, digital forensics & incident response service provider that offers specially tailored services for public prosecutors, courts and other authorities, law firms and commercial organisations. Digifors helps increase data security or simplify the handling of data in connection with criminal or investigative proceedings.

Whilst delivering their services it is critical that DigiFors is able to investigate an incident, identify the nature of the breach, produce a professional and detailed report and communicate their findings to the customer as quickly and efficiently as possible.

"If it is a small case, just one computer, you call your client and ask them to send the computer for further investigations. But if the case is large, in some cases more than 1,000 computers have been involved in a case, it is challenging to do the investigations and solve the case in a timely manner.

This is one of the many reasons why we have implemented Binalyze AIR in the heart of our incident response activities. Binalyze AIR provides us the speed and the granularity that we need in our day-to-day incident response activities at enterprise scale" states Christian Klaus, Head of Threat Detection and Response at DigiFors. Prior to partnering with Binalyze, DigiFors analysts and consultants had to travel to the client's location to collect forensic disk images and extract data. Using legacy forensic solutions this was an extremely time-consuming, expensive and laborious task.

Working in this way slowedvdown individual investigations and limited the case capacity of the business as a whole.

With Binalyze AIR this process has been streamlined and forensic data can be collected in just a few minutes, remotely from the DigiFors lab in most cases.

Another pain point that DigiFors were experiencing was an inability to quickly identify which assets on the customers network have been affected by the breach being investigated.

DigiFors ability to provide granular answers about suspicious activity or an active attack to an anxious customer was also being impacted by a lack of fast working solutions.

Remote evidence acquisition Collecting evidence from a large number of endpoints simultaneously and finding the IoCs within thousands of artifacts is a challenging task for Incident Response providers like DigiFors.

By choosing to use Binalyze AIR, DigiFors can now collect, process and analyse more than 280 artifacts and evidence types, network PCAP data and files for eDiscovery in just a few minutes from hundreds of endpoints at the same time.

Customer
Digifors

Industry
Cyber security

Region
Europe

Success Highlights:

- **Decreased evidence** collection times from days to minutes
- **Improved efficiency** with remote evidence collection & automation
- **Collaborate more** efficiently and effectively
- **30% faster** case investigation times

Evidence can be collected on Windows, Linux and macOS, as well as Chromebooks, ESXi machines and any off network assets using standalone collectors.

Collected evidence is processed and presented in a highly optimised forensic case report which consolidates the work previously accomplished by multiple tools.

Triage at scale

Binalyze AIR also performs triage at scale using YARA, Sigma and Osquery directly on the endpoint asset. This has allowed DigiFors to easily widen the scope of an investigation and quickly perform compromise assessment to understand which assets are included in a breach, which endpoints require a deeper investigation or can be eliminated as a false positive.

The remote triage at scale with Binalyze AIR has delivered increased efficiency and allows DigiFors to quickly take control of the investigation and put the customers mind at ease.

Improved efficiency with automation and collaboration.

During an active investigation speed is the most important factor and can place Incident Response teams under pressure. Any tool that can improve collaborate and coordination, and remove inefficiencies by automating processes, can make a big different to service providers like DigiFors.

Binalyze AIR's Assisted Compromise Assessment module (DRONE) is delivering automation to the analysis of forensic case reports by automatically flagging evidence with verdicts and scores based on the findings of more than 20 proprietary analysers.

These findings are eliminating previously repetitive and manual activities, preventing unnecessary escalation to more experienced analysts, and dramatically speeding up their investigation.

The collaborative Timeline capability of AIR allows the DigiFors team to work in harmony on the same case, to investigate and come to a conclusion much faster than ever before.

With Binalyze AIR's automation and collaboration capabilities, the DigiFors team is now able to investigate cases 30% faster.

These efficiency gains have a material impact on the outcomes of the individual cases, reduce the costs associated with investigations and increase DigiFors' overall investigative capacity.

Decreased education & onboarding times.

Binalyze AIR has an easy-to-use interface that allows incident responders to quickly implement, configure and start using it for forensic and incident response needs in minutes.

"I can say that onboarding and learning how to use Binalzye AIR takes less than 30 minutes, which is very important for us, because spending a lot of time learning and configuring a tool, instead of using it for what it is purchased for, is time-consuming and that is something we want to avoid. Our goal is to deliver high quality service to our clients on time." states Christian Klaus, Head of Threat Detection and Response at DigiFors.

"I can say that onboarding and learning how to use Binalzye AIR takes less than 30 minutes, which is very important for us, because spending a lot of time learning and configuring a tool, instead of using it for what it is purchased for, is time-consuming and that is something we want to avoid. Our goal is to deliver highquality service to our clients on time."

– Christian Klaus, Head of Threat Detection and Response at DigiFors.

Conclusion

With Binalyze AIR, Digifors can now collect, analyze and collaboratively investigate more than 280 evidence types from endpoint assets across their customer base remotely, which has significantly reduced the time and resources required previously. Binlayze AIR's collaboration and automation tools have dramatically reduced the average investigation time by 30% allowing them to close cases faster, provide an enhanced service and increase case capacity.