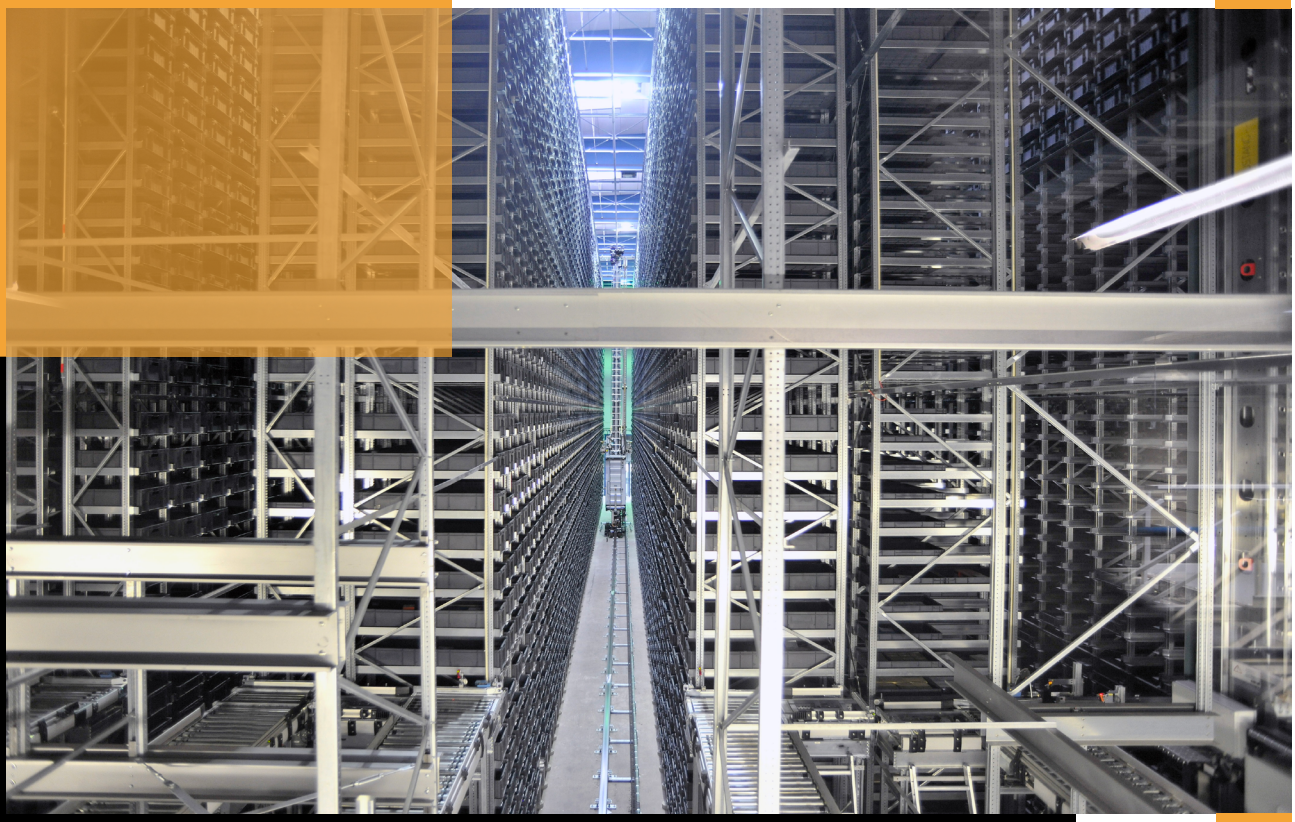
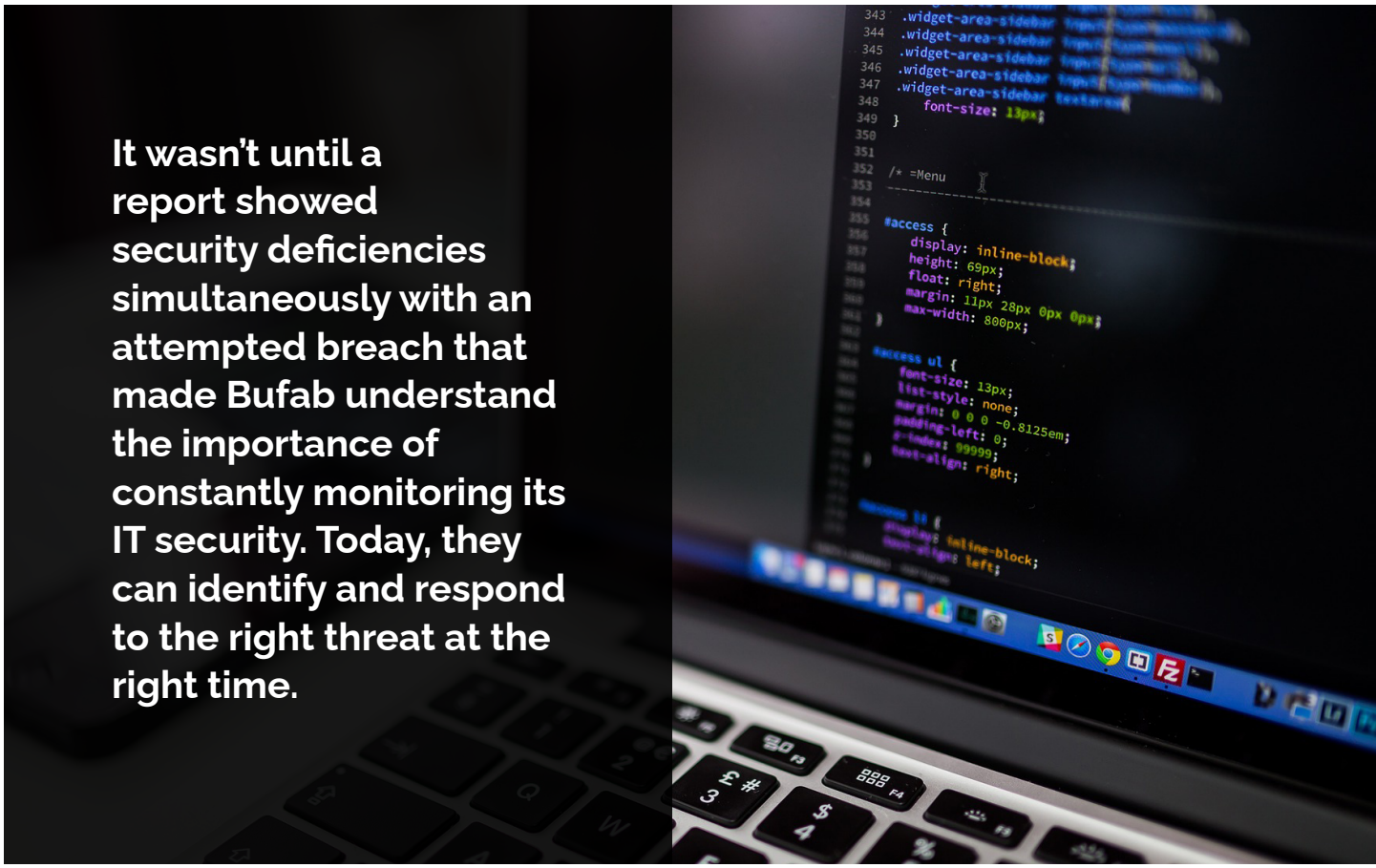
TRUESEC



CASE STUDY

How Bufab Solves Security Deficiencies Before They Appear

www.truesec.com/cases



How Bufab solves security deficiencies before they appear

In 2021, IT security is not about whether a company will be exposed to security threats and intrusion attempts or not; rather, it is when. For Bufab, it was not until autumn 2019 that a security report identified certain deficiencies simultaneously with an attempted breach. These two incidents combined made Bufab understand the importance of constantly monitoring its IT security.

BUFAB

About Bufab

- One of the world's leading suppliers of components to the manufacturing industry
- Head office in Värnamo and operations in 28 different countries
- Turnover 2020 was over 4 billion SEK

Bufab sources and sells various types of components (so-called C-parts) to large manufacturing companies worldwide. With a large and complex organization consisting of companies in 28 countries and subcontractors and dealers worldwide, security and the ability to detect security threats are critical to ensure their machinery runs smoothly.

The Report Identified Deficiencies in Security

The need for a better security solution appeared at the beginning of 2020 when Bufab Group gained new insights in a report that revealed security deficiencies.

"We ordered a report from PwC that examined our security from five different perspectives. Among other things, they looked at our capacity to find, respond to and prevent various types of IT security threats. There we had a range of deficiencies", according to Michael Exenberger, IT Manager at Bufab Group.

Around the same time, Bufab encountered an intrusion attempt that made the question of a new IT security solution even more relevant. Bufab spoke with several different suppliers and eventually chose Truesec as their partner.

"The partnership with Truesec began with them investigating the intrusion attempt. That incident in itself might not have been so serious, but the excellent collaboration with Truesec resulted in us choosing their SOC service over other suppliers", Michael Exenberger says.

> **"We currently discover maybe 10-20 times more threats than before"**
>
> *- Michael Exenberger, IT Manager at Bufab Group*

24/7/365 Security Monitoring

With Truesec's SOC (Security Operations Center), Bufab's systems are now monitored 24/7 for incidents and actions. Truesec's managed SOC also prioritizes alerts and ensures that critical warnigs are not lost within a flood of non-critical information.

An Endpoint Detection and Response (EDR) system is used, which can briefly be described as an "antivirus on steroids". An EDR inspects everything that manages to bypass an antivirus system. With the help of constantly updated rules, it will trigger alerts when possibly harmful activities are detected.

"Truesec has helped us to become more disciplined with respect to our incident logging which ensures that we can identify and respond to the correct threats. Before we started working with Truesec, we did not have the capability to monitor at the same level", says Michael Exenberger.

Truesec also uses its own algorithms and filters to find events, which makes the hit rate and the ability to detect threats and deficiencies today look entirely different from when Bufab did everything in-house.

"We currently discover maybe 10-20 times more threats than we did before. We also get help to sort out and prioritize so that we can act on the things we need to solve", says Michael Exenberger.

How Truesec helps Bufab

- Security Operations Center (SOC) monitoring of Bufab's environment 24/7
- Manual analysis and prioritization of threats by Truesec SOC operators who deliver reports containing recommended actions to Bufab.
- Continuously updating custom detection rules based on threat intelligence.

Security Operations Center (SOC)

The Detect & Disarm managed service utilizes our Security Operations Center (SOC) to monitor, analyse and maintain our customers information security and digital assets. It provides 24/7/365 monitoring, detection and disarm capabilities. Through real time observations, the SOC is able to identify, prioritize and respond to potential threats.