IT Operations Case Study: Equens

"In the past, we had no warning of any problems – the problems were reported to us by the customers themselves, now we have a very clear vision and real-time view into what is happening. With Prelert we are able to highlight situations of lack of traffic, or strong reductions of the same, even without having direct evidence of anomalies." -Maurizio Chiametti, team manager of Equens' COA

COMPANY TYPE
Europe's biggest card
and payment processor

USE TYPE
IT Operations

KEY BENEFITS
- Real-time insights into behavior of environment
- Early detection & resolution of real problems
- Higher quality services with less manual analysis

ENSURING THE RELIABILITY OF EUROPE'S BIGGEST CARD AND PAYMENT PROCESSOR

Equens SE is one of the largest payment providers in Europe, processing 9.7 billion payments and 5 billion POS and ATM transactions each year. The company's core business consists of connecting payers and payees by offering services that enable them to make and receive payments in a seamless, secure and efficient manner. Building on more than 50 years of experience in the payments industry, Equens offers modular, customizable and future-proof solutions covering the entire payments value chain. Besides traditional payments, its platforms are also geared for e-payments, m-payments, e-mandates and e-identity transactions. With offices in five countries, the company services a broad, international client base in numerous countries across Europe. The way Equens combines scale and European market coverage with local presence and expertise gives the company a unique ability to improve its clients' competitive edge.

To become a successful transaction and payment processor, building trust is critical – customers must have confidence that you run a well-built, well-maintained, secure and protected operation. To that end, Equens has been dedicated to maintaining a high level of operational monitoring, ensuring that the company is able to provide the same level of security, reliability and uptime that customers have come to expect, even in the face of rapid growth and increasing global threats.

prelert®

REMAINING VIGILANT

Equens monitors its pan operations from a Centrale Operativa Allarmi (COA), or alarms control room, in Italy. The facility houses twenty operators that monitor all systems and networks every hour of every day. The COA serves as the junction point between customers and the company – and is the part of the company that receives first word of any problems in the system or of any issues customers are having.

The COA's operators are responsible for reviewing notifications and alerts, connecting with specialists to see what the problems are, assisting in the resolution of the problem and being the direct interface with customers.

EQUENS

If something goes wrong operationally, the COA is the first to know about it – and immediately has to step into action.

SPLUNK IMPLEMENTATION

Despite the committed staff and dedicated resources, Equens wanted to improve the way that it identified and analyzed potential incidents. It wanted to be more proactive and reduce the time it took to respond following the identification of a problem – while finding ways to make data analysis easier and quicker. With those goals in mind, assisted by his business partner **Kiratech,** Equens turned to **Splunk,** maker of a software platform that enables organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices.

Although the Splunk implementation radically improved how Equens was able to monitor, identify, analyze and solve potential operational issues, the company soon found that business growth drove data volumes to a point that overwhelmed their support teams. As the company grew, so did the number of false positive alerts that needed to be reviewed and ruled out or acted upon.

Put simply, there was too much data to analyze, increasing the likelihood that an error or issue would be inadvertently missed.

ADDING NEEDED FUNCTIONALITY WITH PRELERT

Without evolving its management approach beyond rules and thresholds, the company feared it had no way to know for sure if it was dedicating its resources to the most critical potential system and network issues. Equens decided it needed an advanced analytics approach to minimize false positives and pinpoint real issues that posed a threat to its network and its customers.

Equens turned to **Prelert's** machine learning anomaly detection software to help.

A native app for Splunk, Prelert's Anomaly Detective solution uses machine learning to extend the capability of standard Splunk searches. Its advanced algorithms automatically establish normal behavior patterns and accurately identify anomalous activity, helping to quickly flag performance problems.

By extending Splunk with Prelert's machine learning-based anomaly detection technology, Equens now has a clear vision of its services and can automatically monitor for anomalies, denials, banks involved, percentages, returns and reason codes. Most importantly, Equens can more easily address rapidly growing data volumes because the machine learning technology automatically identifies anything that's amiss without the time and labor required to configure and maintain alert rules or thresholds.

Because Prelert's Anomaly Detective application also cross correlates abnormal behaviors, soon after its implementation Equens' troubleshooting and response times were slashed.

"In the past, we had no warning of any problems – the problems were reported to us by the customers themselves," said Maurizio Chiametti, team manager of Equens' COA. "Now we have a very clear vision and real-time view into what is happening. With Prelert we are able to highlight situations of lack of traffic, or strong reductions of the same, even without having direct evidence of anomalies."

The combination of Prelert and Splunk have also allowed Equens' operations team to become as agile as its development team, creating monitoring for new application components in a single day – ensuring that new services are protected from day one.

MAKING ALERTS EASY AND ACCURATE

Equens soon found that Prelert's automated anomaly detection was the key to managing the massive amounts of data and even more massive amounts of alerts received every day.

"Using Splunk we were able to strongly reduce the time it took to monitor card processing services without any application changes. By adding Prelert, we can now find anomalies in historical trends and in real-time, in core business applications," added Maurizio Chiametti. "Unstructured data has become easy to investigate and categorize – our business monitoring now sends only real alerts."

With the machine learning technology in place, the system learns and improves its decision-making with each instance, giving Equens – and its customers –the confidence needed to continue the company's tremendous growth and success.

ABOUT PRELERT

Prelert is the leading provider of machine learning anomaly detection for IT security and operations teams. By using automation and machine intelligence to eliminate manual effort and human error, the company's software finds security breaches and service disruptions that legacy tools miss. Hundreds of progressive IT organizations rely on Prelert's advanced analytics to automatically mine huge volumes of IT data in real time, enabling them to identify security threats and performance issues before they impact business. For more information, please visit **www.prelert.com** or follow **@Prelert.**

DOWNLOAD YOUR FREE TRIAL AND START REPORTING ON ANOMALIES IN MINUTES.

We know you're skeptical, but we want to show you that this works. You can download a free trial of Anomaly Detective and have it installed, baselining your data, and reporting on anomalies within minutes. Quick set up, nearly instant results, and no pressure to buy. **Try it out for yourself** and see how it can workfor YOUR data.

ANOMALY DETECTIVE
Free Download