DARKTRACE

CASE STUDY

Orio Al Serio International Airport

Orio al Serio international airport
S.A.C.B.O. S.p.A.

Overview

Industry

- Transport

Challenge

- Sophisticated cyber-attackers and rapidly-evolving threats
- Digitization of airport practices
- Limited network visibility
- Insider threat

Results

- Next-generation threat detection in real time
- Ability to carry out deeper investigation and risk-mitigation
- 100% network visibility
- 3D graphical Threat Visualizer interface

Business Background

Il Caravaggio - Orio al Serio International Airport, sometimes referred to as Milan-Bergamo International Airport, is situated just outside Bergamo city in Northern Italy and 45 miles north-east of Milan. Managed by SACBO SpA (Società per l'Aeroporto Civile di Bergamo-Orio), it is the third busiest Italian airport with over 11 million passengers each year. The international airport is the second largest Ryanair hub in Europe, after London Stansted.

> The unparalleled level of visibility and nextgeneration threat detection capability makes Darktrace's technology one of a kind.
>
> **Ettore Pizzaballa, ICT Manager, SACBO SpA**

Challenge

The latest technological advancements employed by airports in general, including Wi-Fi networks, online check-in, automated baggage systems, electronic passports and un-manned border controls, have improved efficiency and organization. However, the digitization of airport practices also creates potential vulnerabilities and possible entry-points for cyber adversaries. This is a pressing concern for airports, which are already a likely target for malicious attacks.

As part of Italy's critical national infrastructure, Orio al Serio International Airport has a profile of interest to a range of potential cyber-attackers. As such, the airport was keen to strengthen its cyber defense strategy with the latest, most innovative cyber technology available.

Moreover, the airport wanted complete network visibility in order to have a thorough understanding of its employee and user behaviors and, therefore, be better prepared to detect any potential insider threat. Given the number of devices logging onto the airport's main network everyday, the need for transparency into all activity was crucial.

Ultimately, Orio al Serio International Airport needed a cyber security technology capable of detecting potential vulnerabilities and actual threats, inside and outside its network, that may aim to target its critical assets and disrupt its vital operating systems.

Solution

After completing a 4-week Proof of Value ('POV') with Darktrace's Enterprise Immune System, Orio al Serio International Airport was impressed by the technology's ability to achieve real-time threat detection.

Powered by machine learning and mathematics developed by specialists from the University of Cambridge, the self-learning technology is inspired by the biological principals of the human immune system. It is capable of modeling the behaviors of every user, device and network as a whole to establish a 'pattern of life' specific to Orio al Serio International Airport's network.

Using its dynamic understanding of what is normal, the technology automatically detects any behavior or activity that deviates from the norm and flags it as suspicious, without using any rules or signatures, reporting the anomalies to the airport's security team. All alerts are presented via Darktrace's Threat Visualizer, a 3D graphical interface that also provides a topological representation of Orio al Serio International Airport's network and the activities within it.

> The TIRs are invaluable to us. We can easily share findings with company management so we all understand what is going on and how we are dealing with any issues.
>
> **Ettore Pizzaballa, ICT Manager, SACBO SpA**

Benefits

Thanks to Darktrace's immune system technology, Orio al Serio International Airport is now alerted to genuinely anomalous behavior, that may be indicative of cyber-threat, in real time. The Threat Visualizer functions allow the airport's security team to look back in time at how events unfolded, dig deeper into specific devices and carry out any necessary risk-mitigation to prevent serious damage.

Soon after deploying the Enterprise Immune System, the airport was notified to a number of potentially problematic incidents. For example, a flash proxy (that had gone previously unnoticed) and various weak points in the network, which were being unknowingly accessed by the public. The airport now has 100% network visibility and, therefore, a much better understanding of its employee anduser behaviors.

The airport also receives weekly Threat Intelligence Reports ('TIRs'), created by Darktrace's expert analysts, which summarize and classify the potential threats detected. "The TIRs are invaluable to us. We can easily share findings with company management so we all understand what is going on and how we are dealing with any issues," said Ettore Pizzaballa, ICT Manager, SACBO SpA. "This, on top of the unparalleled level of visibility and next-generation threat detection capability, makes Darktrace's technology one of a kind."

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010

info@darktrace.com
darktrace.com