DARKTRACE

Pizza Hut Restaurants UK

Overview

Industry

○ Hospitality

Challenge

○ Limited human security resources

○ Phishing attacks targeting workforce

○ IT security team working remotely

Results

○ Self-learning AI technology across email and network traffic

○ Malicious emails automatically held back

○ Time-to-triage dramatically reduced with Cyber AI Analyst

○ Complete visibility over network and digital activity

Business Background

The first Pizza Hut Restaurant in the UK opened in Islington over 40 years ago. The organization has since grown rapidly and now has over 7,000 employees working in over 250 restaurants across the country, serving 20 million guests a year. Embracing innovation across all areas of the business, Pizza Hut relies on Darktrace's Cyber AI Platform to protect its employees and customers from the most sophisticated and targeted cyber-attacks.

> " From a security point of view, the nature of a threat is that it's something you don't think to look for – you don't know where it's coming from. "

James Bywater, IT Infrastructure Manager

Challenges

With a lean IT security team, Pizza Hut Restaurants UK had accepted the need for the use of technology to augment its human resources and help protect the sensitive information of over one million customers.

More recently, increasing attention has turned to the email realm, where the organization is faced with a range of possible threats, from compromises in its supply chain and account takeover, to spoofing and malicious payload delivery.

During the recent and rapid transition to remote working, the security team faces an additional challenge in their inability to investigate onsite and ask employees about their activity face-to-face. Pizza Hut Restaurants UK required a unified security platform to augment its small and remote team with this array of challenges.

An Immune System Approach

The organization deployed Darktrace's self-learning technology in favor of audit or log-based solutions. James Bywater, IT Infrastructure Manager, explains: "With auditing tools that require you to set up rules, you have to know what you're looking for. From a security point of view, that's the precise nature of a threat; it's something you don't think to look for – you don't know where it's coming from."

The security team lacked sufficient resources to set up and manually configure these legacy products, and so opted for Darktrace's Cyber AI, which was set up in under an hour and effective within days. Immediately the Enterprise Immune System began learning the 'pattern of life' for every device and employee in its workforce. "It wasn't really a contest in my eyes," explains Bywater. "Having technology that is constantly learning and improving is just so much better than auditing tools."

> "
> The AI has become an additional person on our team.
> "
>
> **Mariusz Sznerch, Lead IT Infrastructure Architect**

Augmenting The Team

The security team now benefits from Darktrace's real-time analysis, and its prioritization of threats based on over 750 metrics allows the team to spend their time on only the most relevant incidents.

"If the level of threat came out at above 90%, we were jumping on it straight away," explains Mariusz Sznerch, Lead IT Infrastructure Architect at Pizza Hut Restaurants UK.

With the release of the Enterprise Immune System version 4, Darktrace's AI not only detects threats, but now automatically emulates the thought-processes of world-class analysts to investigate broader security incidents in real time, offering further time savings for Sznerch and his team in a technology called Cyber AI Analyst. "When the Cyber AI Analyst came to life, I have begun leaving the individual security events with a low anomalous score. I leave the whole security overwatch to AI at this point. The AI has become an additional person on our team."

Extending to Email

In 2019, Pizza Hut Restaurants UK expanded its Cyber AI coverage into email, after increasing concern about the frequency and sophistication of phishing emails received on a weekly basis. These emails, often attempting to spoof suppliers or colleagues, may have seemed innocuous, but contained hidden payloads hidden behind links or attachments.

In particular, the concern was around executive-level 'whaling' attacks; payloadless emails that sought to illicit confidential information from the company's senior staff members.

"We had put a lot of emphasis on training our workforce," explains Bywater. "But ultimately in an organization of our size, human beings are always going to click on something that they find interesting; you can't guarantee that won't happen."

Wanting to bring the same level of coverage to email as it had in other areas of the enterprise, Pizza Hut Restaurants UK once again turned to AI to protect its inbox. Antigena Email now absorbs the patterns of communication between employees internally and externally, using the same unsupervised machine learning techniques to detect subtle indicators of an attack.

The Cyber AI now responds to the full range of email attacks targeting the workforce, from spoofing and solicitation to supply chain account takeover.