

# REFIRST Company



## REFIRST Company Description

REFIRST is a retail company that is headquartered in the US with 12000 employees. REFIRST sells and ships consumer goods via its online service. The company has also 50 sites in EU(10) and US (40) that allows on-site purchases of goods via its retail network with POS devices. Following a recent breach from [FIN6](#) adversary, a new CISO has been appointed to improve the cyber security posture of REFIRST.

## REFIRST's Online Infrastructure

REFIRST's online infrastructure is hosted in Microsoft Azure and is Windows-based. The software stack of its website runs on IIS and Oracle DB. One of the most critical components of its online infrastructure is the customer portal that has uptime SLA 99.9%. One year ago, REFIRST fell victim to a credential stuffing attack against its online customer portal. The perpetrators have been found to sell the stolen accounts in dark web. Finally, REFIRST's external perimeter is scanned on a daily basis by the enterprise vulnerability management tool.

## REFIRST's Corporate Network

REFIRST's enterprise network is Windows-based (Windows 7, Windows 10 and Windows Server 2016). During the past 6 months, the most common AV detections that SOC analysts observe are [PUA \(Potentially Unwanted Applications\)](#) and [Emotet](#).

## REFIRST's Retail Network

REFIRST's retail network is Windows based (Windows 7 and Windows XP) and suppliers connect directly to the sites to support operations. There are two suppliers for the POS network in the US and the EU. Some admins within Retail IT Ops admins can access the retail network from REFIRST's corporate network.

## REFIRST's CTI Team

CISO tasked the Head of CyberDefence to start with a team of 2 CTI analysts. The goal is to kick off and build CTI capabilities from scratch.