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 10.0 version 1809 and Oracle DB version 19.1.0. One of the most critical components of its online infrastructure is the customer portal that has uptime SLA 99.9%. Moreover, REFIRST's external perimeter is scanned on a daily basis by the enterprise vulnerability management tool. 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.

REFIRST's Corporate Network

REFIRST's enterprise network is Windows-based (Windows 7, Windows 10 and Windows Server 2016). The enterprise network is flat and a solid Business Continuity Plan is currently being worked on. The enterprise network hosts in its data centre a dozen of business critical servers. During the past 6 months, the most common Anti-Virus detections that SOC analysts observe are PUA (Potentially Unwanted Applications) and Emotet. Finally, a dozen of backoffice servers are hosted in REFIRST's data centre that are critical for the company's sales operations.

REFIRST's Retail Network

REFIRST's retail network is Windows based (Windows 7 and Windows XP) and suppliers (PANX Global and ZZZ Electronics) remotely connect to the sites using TeamViewer to support operations. Some admins within Retail IT Ops admins have access to the retail network from REFIRST's corporate network.

REFIRST's CTI Team

CISO tasked the Head of CyberDefence to start with a team of 3 CTI analysts. The goal is to kick off and build CTI capabilities from scratch.