ACME OSINT Plan

Produced by: Marvin the Martian SOC

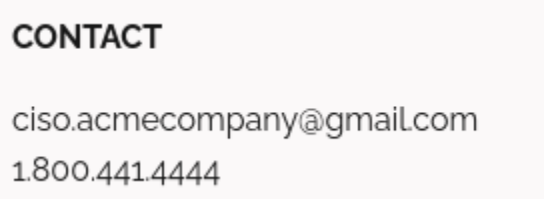
Commissioned by: WIley E. Coyote

Date: 11/04/2022

Initial OSINT findings

Open source intelligence on ACME employees and organization will consist of any recon which can be done without raising flags. This includes open web resources such as social media websites, company websites, and any established business partners. Business critical information should never be shared online, and employees should be made to understand and agree to the terms of confidentiality agreements which include social media websites such as LinkedIn, Facebook, Instagram and twitter. NDAs are to be signed by any employee with access to confidential information which could lead to system/network breaches, such as any IT admin, or vendor consultant.

Figure 1 CISO email



Cursory open sources investigation shows that the ACME website lists the CISO's personal email address, which can be used to enumerate other email addresses, social engineer or brute force access. It should also be brought to the forefront that as stated in our vulnerability scan, the company website, either through automation errors, incompetence or deliberate action, shows many if not all our information security flaws.

Figure 2 ACME assets

Hardware Assets:

Cisco Identity Services Engine
Cisco Firepower
Cisco ASA 5500
Ubiquity Wireless and Network Equipment

Software Assets:

What's Up GOLD
Splunk Enterprise
Active Directory
Windows Print Server
Adobe Connect Server

Cloud Assets
OKTA IdP
Zoho Password Management Suite
Microsoft Teams
One Drive
Office365

Information is to be scrutinized by security teams, such as the SOC, before being posted to any website, blogs or articles to see if there is any information which should not be shared or obfuscated. Social media training for the entire organization should be held, to help all understand what should and should not be shared and why. Internal information is to be immediately removed from the open web.