Review of ACME Security Events

Produced by: Marvin the Martian SOC

Commissioned by: WIley E. Coyote

Date: 11/06/2022

Review of Security Events

Late this year ACME was the victim of a large data breach, and had it's lack of security known to the media. Investigation shows that The Cyber Stooges SOC was negligent in it's due diligence, with not even basic security practices being implemented. Brocade switch logs did not show any abnormalities, despite documented brute force attempts shown in firewall and IDS logs. Bad actors managed full access to network, installed spyware on ACME networking assets, gained access to at least two users and sucessfully exfiltrated data while maintaing persistence on the network.

Recommended Metrics

Recommended metrics include: Detected intrusion attempts, Incident (rates/severity levels/ response times/ time to remediation), Vulnerability patch response times, Number of users categorized by application and access levels, and Volume of Data generated by the organization.