ACME Co.

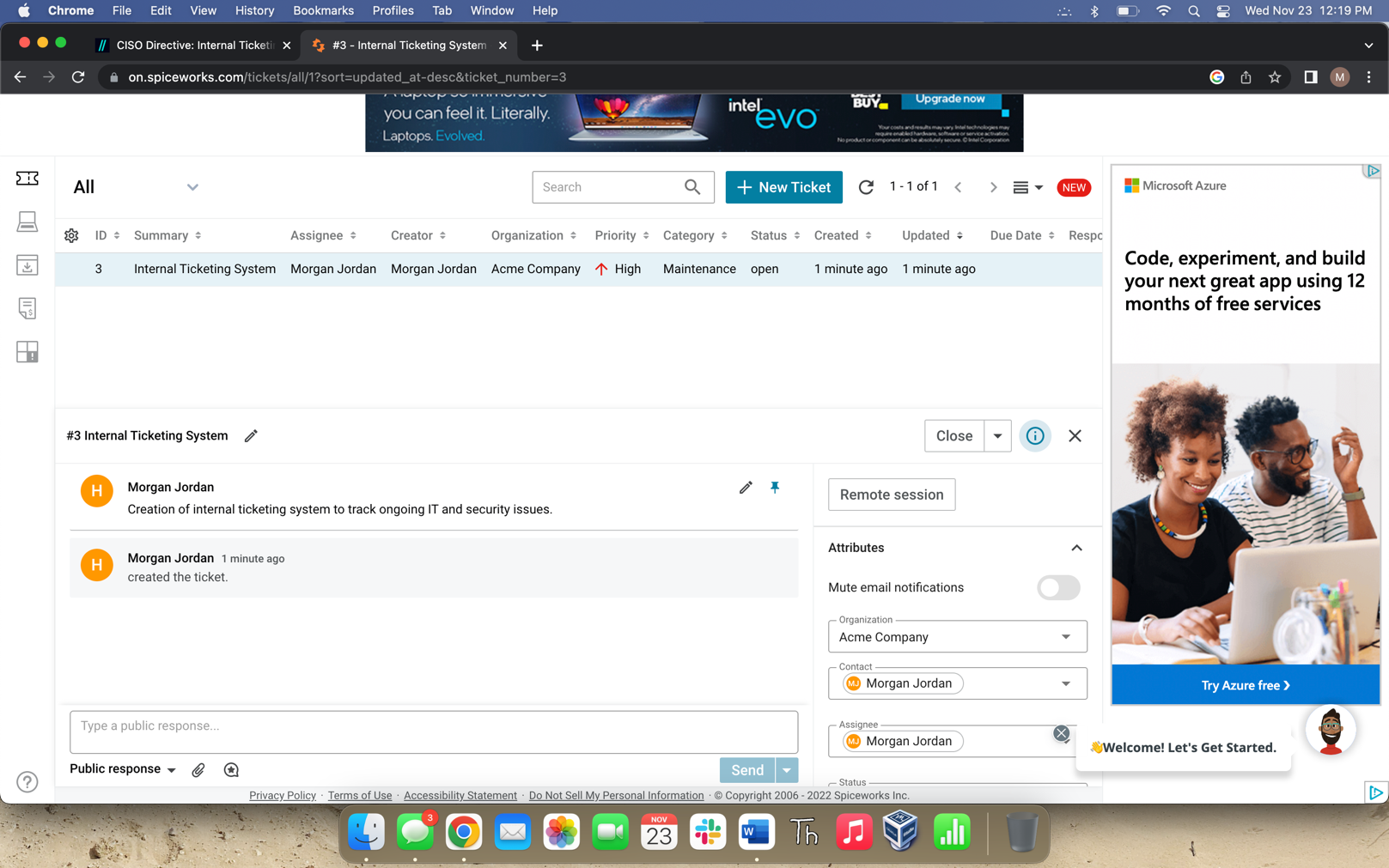
Network Evaluation Summary

Executive Summary

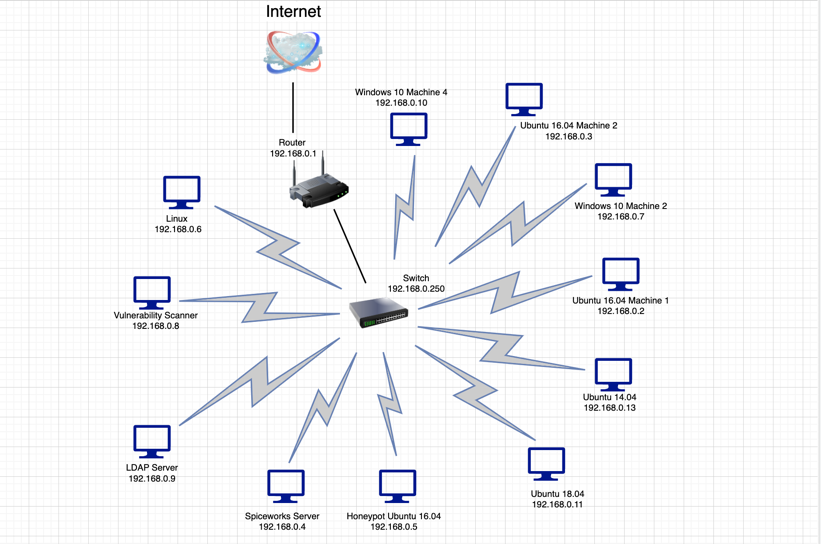
Through a multitude of scans and assessing the current network with logs, we were able to discover the magnitude of the breach along with how to proceed. In order to prevent breaches of this level from occurring in the future we developed an Internal Ticketing System to keep up on current network needs, a Risk Assessment which will be continually updated, an OSINT Remediation Plan, an Incident Response Plan, and a Security Plan with Timelines. These measures, along with implementing a SIEM and general Governance, Risk and Compliance, will not only shore up our network defenses but allow us to reduce the impact of any future attacks.

Evaluation with Solutions

The first task to complete was initiating an Internal Ticketing System via SpiceWorks which is a free online ticketing system. This will allow us to adequately track and monitor any outstanding or discovered IT and security issues.



After getting the ticketing system in place, we were then able to evaluate the network and update the pre-existing diagram to show the appropriate, current asset information. By doing so we will be completing the first portion of the NIST CSF. It is at this point that we noticed the firewall was no longer in place, thus creating a severe security and non-compliance issue. PCI DSS (Payment Card Industry Data Security Standard) states that a secure network must be maintained in which transactions are to be conducted, to include firewalls.



From here, we started developing a Risk Assessment to collect and track all security related issues in one place. Within the Risk Assessment we were able to provide cost approximations, benefits provided, timelines to implement, and a high/med/low estimate. To populate the Risk Assessment table, we performed a vulnerability scan with a free program called Nessus and examined log files by running them through a SIEM called Splunk Enterprise.

The vulnerability scan provided us with the following output:

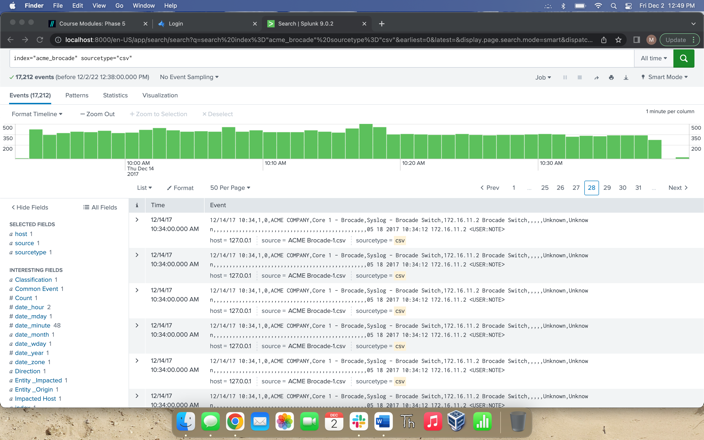
A picture containing text, screenshot, computer, indoor

Description automatically generated

When reviewing the remediation tab, we noticed the majority of the issues found were because much of the software within the network had not been updated, leaving numerous vulnerabilities that an attacker could use to their advantage. According to PCI DSS, systems should be protected against malicious attacks by having frequently updated anti-virus/spyware/malware software or programs in place. Patches offered by software and OS vendors should also be routinely installed to ensure the highest possible level of vulnerability management.

By using our SIEM, Splunk Enterprise, to evaluate the Brocade Switch, Firewall, and IDS log files, we were shown when and how the breach occurred.

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

* Unknown access to the brocade switch (172.16.11.2) on 12/14/17 from 10:33am-10:34am
* Firewall
  + Buffer overflow attacks on Thomas2 (10.7.6.13), ACME.LOC access
  + Malicious URL Directory Traversal on Jessica7 (10.0.0.15), ACME.LOC access
  + Web server enforcement violations, OpenSSL, Overly-long Heartbeat Response information disclosure (ACME.loc External Connectivity and Azure External Connectivity)
* IDS
  + Potential vulnerability exploit allowed – 1,271 (6.9%)
    - 12/18/17 0600 External – Impacted application: HTTPS, Protocol: TCP (443)
    - 12/18/17 0700 External – Impacted application: Unknown TCP Port, Protocol: TCP
    - 12/18/17 0800 Outbound – Impacted application: DNS, Protocol: UDP (53)
    - 12/18/17 0800 Outbound – Impacted application: SSH – Secure Shell Protocol: TCP (22)

From here, we created an OSINT Remediation Plan which consists of a strategy to safeguard all sensitive data that could potentially be shared publicly. This plan contains information on how to collect, analyze, and reduce OSINT breaches. PCI DSS states that cardholder information must be protected wherever it is stored, meaning it should be secure against hacking and encrypted in an effective way. Access to this information also needs to be restricted and controlled. By maintaining these standards, we will not only maintain compliance with PCI DSS, but also GDPR and NIST CSF.

External Threat Feeds, when implemented with a SIEM, can greatly reduce risks on a network along with increasing efficiency of our current appliances. They are essentially a repository of Open-Source Cyber Threat Intelligence feeds that are in STIX format and can be integrated with our SIEM (Splunk Enterprise). After getting the integration completed, we are then able to set-up conditions, actions and alert criteria so that the appropriate staff was notified if any suspicious activity were to occur.

The Security Plan with Timelines allowed us to evaluate the current security posture (low) and create a multi-year plan to improve our security maturity while continuing to reduce risk. The first year will consist of creating and maintaining an asset inventory, ranking and prioritizing risks, educating employees on security best practices, creating and maintaining an Incident Response Plan, and continuously reviewing gaps in our security controls. In the years following, after those tasks are completed, we would want to focus more on having routine reviews and training to continually mature our security posture. This would allow us to maintain compliance with PCI DSS standards.

For being prepared to handle security events in the future, we created an Incident Response Plan, as well. This is a document that helps guide any employee in how to proceed if and when they encounter a security incident. Some of the key points in the document are the current system diagram, incident response team contact information, and incident response procedures. This complies with the NIST CSF in regard to detecting and responding to security events, therefore allowing us to recover.

Internal Honeypots can be extremely helpful in early indication of malicious activity, allowing us to detect and deflect attacks within our network. The Cowrie is an open source, moderate interaction SSH and Telnet honeypot written in Twisted that is able to log brute force attacks and an attacker’s shell interaction. This allows us to gain information about the way the attacker is operating and/or distract them from other targets within our network. Included within the set-up of cowrie, are the ports by which Cowrie is accessible as well as any plug ins, such as Splunk Enterprise. Cowrie automatically outputs event data to text and JSON log files, allowing us to monitor traffic/activity via our SIEM and set-up alerts to the proper staff.

In order to properly monitor our web services, we need to integrate the website, router and firewall logs with our SIEM. The SIEM can then process the information and, with the proper notifications set-up, inform the necessary staff of any malicious activity within the network or on our website.