Initial Scenario

Scenario Description

Users in multiple departments are reporting an email from a software website claiming one of the two things: Office365/Teams needs to be updated, installation of a new Microsoft Defender. Some have also claimed to have received emails that supply links requiring them to sign in to Office365.````

Scenario Questions

1. Have any users entered credentials or downloaded files?
2. From targeted users, what data is at risk?
3. What is the source address and domain of the sender?
    a. Are any emails originating from inside the network?
4. Do you notify users on the network about recently observed security threats, particularly via email?

Escalation Point One

Scenario Description

Some users are starting to complain about not being able to get to everyday sites or websites with completely different web pages than they remember a few hours ago.

Scenario Questions

1. What sites are affected?
2. Has the user's HOSTS file been changed?
3. Are you able to access and review the default DNS server for affected clients?
4. What is the IP address hosts are resolving to (wireshark)?
5. Is it a certain network segment being affected, or maybe even a certain location?

Escalation Point Two

Scenario Description

Alerts begin to pop off for multiple MFA failures as well as some alerts for impossible logins from users originating halfway across the world.

Scenario Questions

1. Are any users actually in the regions that impossible logins are coming from?
2. Are there adequate password policies in place to prevent rouge logins?
3. Is there an active practice of principle of least privilege?

4. What access and permissions do compromised accounts have?

Final Review

Review Questions

1. How can users be better trained to prevent clicking on phishing emails?
2. How can you improve the Defense in Depth strategies applied and prevent escalation?
3. Were there any alerts on the SIEM rather than only user-based reports?