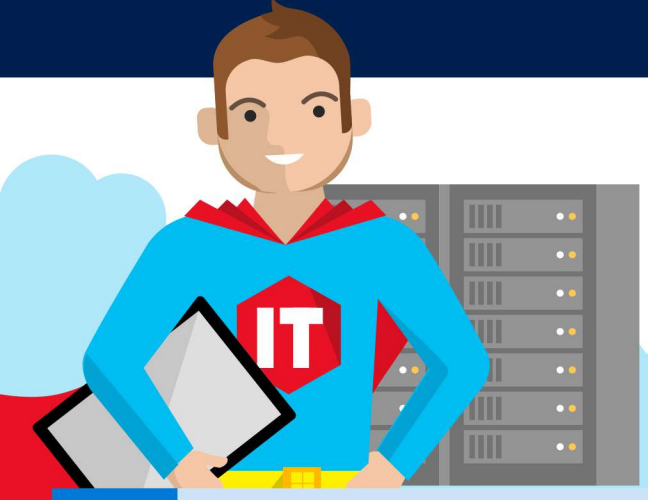


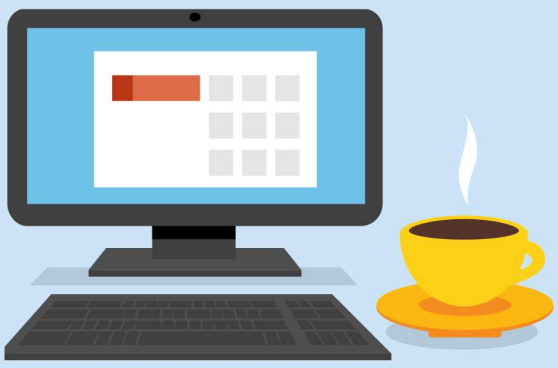
Defend, Protect, Secure

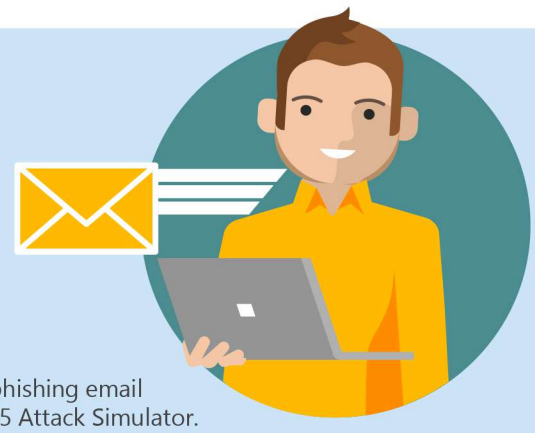
IT heroes in action

Monday

8:30 AM

Joined weekly morning security briefing to review latest attack vectors including viruses, ransomware, and new vulnerabilities.

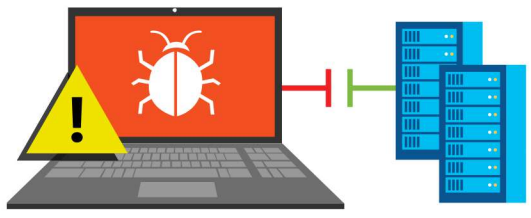




9:30 AM

Launched the quarterly anti-phishing email campaign using the Office 365 Attack Simulator. User clicks will be tracked throughout the week.

Tuesday



9:15 AM

Alert received from Windows Defender Advanced Threat Protection (WDATP) about an in-memory malware detected on a user system. System automatically quarantined by WDATP from all network resources.

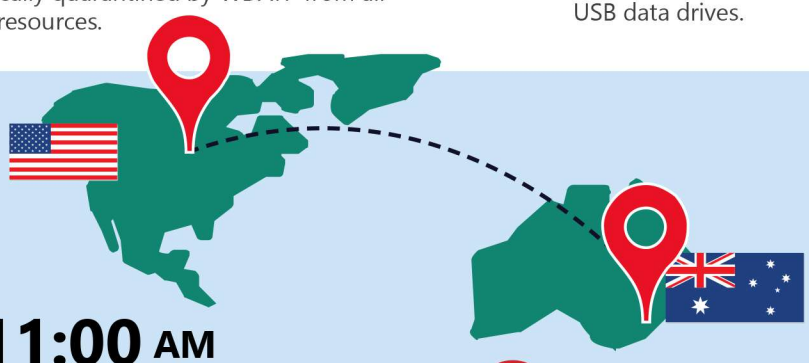
10:00 AM

WDATP dashboard indicates infection source is connected USB drive. Infection confirmed with user. WDATP client signature auto updated using the Microsoft Intelligent Security Graph, preventing further infection within minutes.

10:30 AM

Updated weekly security report with incident details. Recommendation made to prevent use of personal USB data drives.

Wednesday



11:00 AM

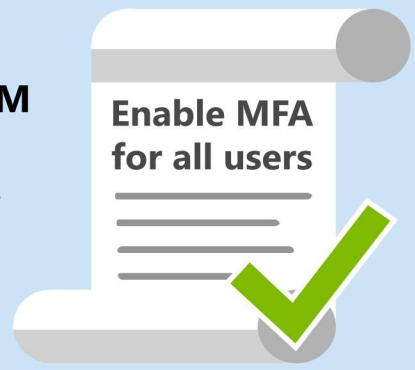
Alert received from Cloud App Security (CAS) regarding impossible logon event. US employee logged on, minutes later same credentials used for attempted Australia logon. Attempt thwarted and account locked until further review.

11:30 AM

Employee contacted, password changed, account enabled for Office 365 Multi-Factor Authentication (MFA).

12:00 PM

Updated weekly security report with incident details and recommendation to enable MFA for all users to close breach vector.



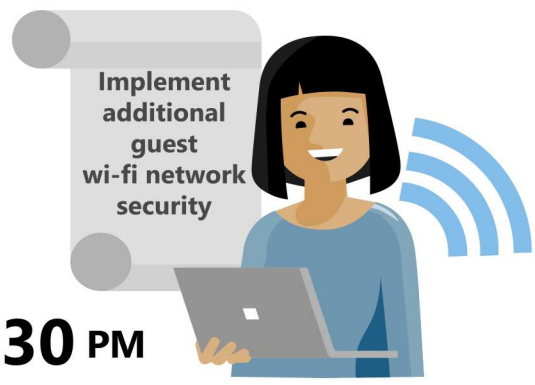
Thursday

1:30 PM

CAS triggered an alert about a network device beaconing a signal to an Internet Command and Control bot server hosted by a known bad actor. The signal was automatically blocked by CAS to prevent a potential breach.

2:00 PM

After a prompt review by the security team, the network device was found to be from a visitor's system on a guest wi-fi network.



2:30 PM

Updated weekly security report with incident details. Recommendation made to evaluate and setup additional security rules and alerts on guest wi-fi network.

Friday

2:00 PM

Quarterly anti-phishing email campaign results analyzed. Of the 1,000 email accounts targeted, over 65% of the users clicked on the simulated website links.

2:30 PM

A PowerBI dashboard was automatically generated and included in the final campaign report. A recommendation for additional user awareness training is included based on the demonstrated susceptibility of the users.

5:00 PM

Depart for the weekend confident that IT systems have been defended, protected, and secured and knowing that not all heroes wear capes.

nexus technologies, inc.

Microsoft