1500 - MS Just Gave the Blue Team Tactical Nukes (And How Red Teams Need To Adapt)

Saturday at 15:00 in 101 Track
45 minutes | Demo, Tool
Chris Thompson*Red Team Ops Lead, IBM X-Force Red*

Windows Defender Advanced Threat Protection will soon be available for all Blue Teams to utilize within Windows 10 Enterprise, which includes detection of post breach tools, tactics and techniques commonly used by Red Teams, as well as behavior analytics. Combined with Microsoft Advanced Threat Analytics for user behavior analytics across the Domain, Red Teamers will soon face a significantly more challenging time maintaining stealth while performing internal recon, lateral movement, and privilege escalation in Windows 10/Active Directory environments.

This talk highlights challenges to red teams posed by Microsoft's new tools based on common hacking tools/techniques, and covers techniques which can be used to bypass, disable, or avoid high severity alerts within Windows Defender ATP and Microsoft ATA, as well as TTP used against mature organizations that may have additional controls in place such as Event Log Forwarding and Sysmon
Chris Thompson
Chris is Red Team Operations Lead at IBM X-Force Red. He has extensive experience performing penetration testing and red teaming for clients in a wide variety of industries. He's led red teaming operations against defense contractors and some of North America's largest banks.

He's on the board for CREST USA (crest-approved.org), working to help mature the pentesting industry. Chris also teaches Network & Mobile Pentesting at one of Canada's largest technical schools.

Hacking his way through life, Chris likes to pretend he's a good drone pilot, lock picker, and mountain biker.

Twitter: @retBandit

#defcon25/by_track/101/saturday #defcon25/By_Day/_saturday