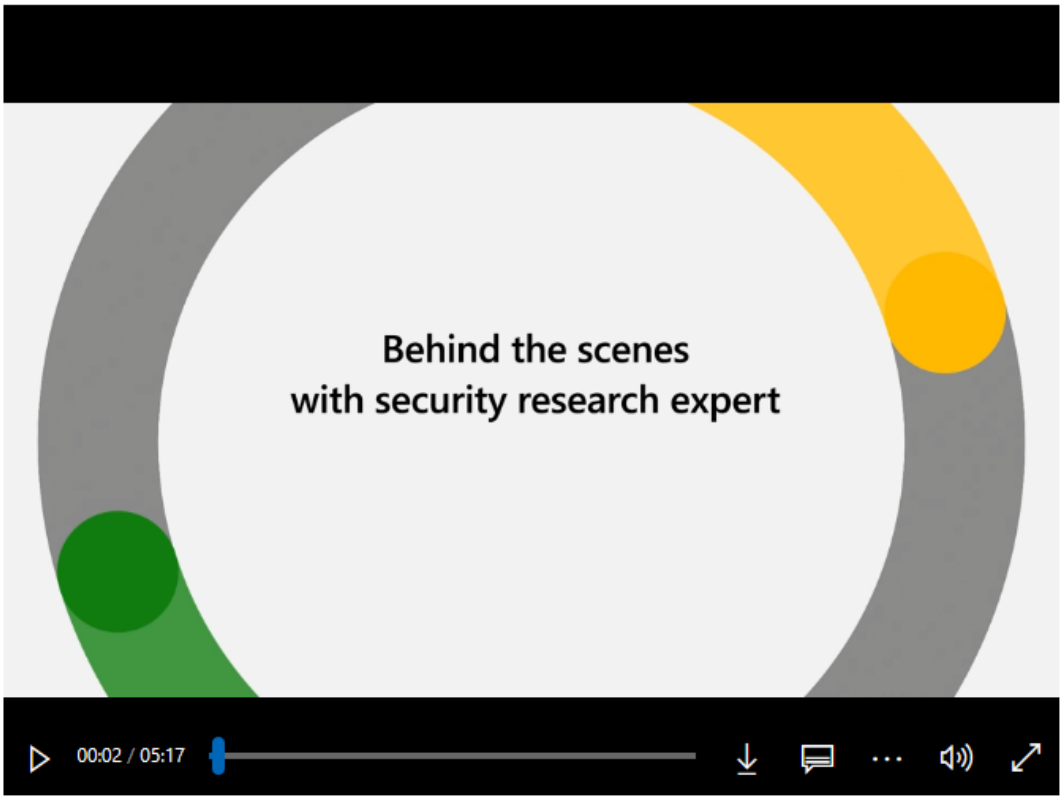
www.microsoft.com /en-us/security/business/security-insider/behind-the-scenes/expert-profile-dustin-duran/

Comment penser comme un acteur de la menace

Profil d'expert de Microsoft : Dustin Duran

WTcr-prod

- Security Insider
- Fiches sur les menaces
- Rapports
- Dans les coulisses
- Informations sur les acteurs de la menace



wus-streaming-video-rt-microsoft-com.akamaized.net/d17c46a8-43c3-4bce-ab89-ec4719d439af/9786ccf6-c806-4005-890d-19932211_6750.mp4

Comment penser comme un acteur de la menace

Mon équipe raconte l'histoire de l'attaque de bout en bout.
Nous relions les points entre les différentes phases d'une chaîne d'attaque pour mieux comprendre les causes profondes d'une attaque, en un coup d'œil, pendant qu'elle se produit.

Nous copions également les techniques et la pensée des attaquants.

Les attaquants abordent le monde en termes d'objectifs et de séquences d'activités.
Ils enchaînent différentes techniques ensemble – c'est pourquoi nous appelons ces histoires d'attaque des « chaînes de destruction » – et se déplacent à travers les voies les plus bénéfiques pour eux.
Ce n'est pas un processus linéaire.
Nous appelons cela penser en graphiques.

En tant que défenseurs, nous devons adopter le même état d'esprit.
Nous ne pouvons pas nous condamner à penser en listes, où nous essayons de réassembler tout le puzzle lorsqu'une attaque est en cours.
En un coup d'œil, nous devons savoir comment les attaquants ont obtenu l'accès, comment ils se déplacent latéralement, vers quoi ils travaillent.

Les défenseurs identifient plus précisément les activités malveillantes lorsqu'ils comprennent ensemble la séquence de ces activités, et pas seulement les techniques individuelles prises isolément.

Un bon exemple est lorsque nous avons analysé une récente série d'attaques de fraude financière et remarqué comment les attaquants utilisaient une configuration de proxy inverse pour contourner l'authentification multifacteur (MFA).
Nous avons noté les signaux de dérivation de l'AMF et attiré des communications vers d'autres cas où la technique émergente est apparue.
Ce que nous avons appris sur la collecte d'informations d'identification grâce à notre capacité à relier ces points nous permet de réagir plus tôt dans l'attaque.
Cela nous aide à être de meilleurs défenseurs.

Lorsqu'on me demande ce qui peut être fait pour mieux protéger une organisation, je réponds toujours la même chose : il est essentiel de tirer systématiquement parti de l'authentification multifacteur.
C'est l'une des recommandations les plus importantes que nous formulons.
C'est l'une des choses les plus essentielles que les entreprises peuvent faire pour mieux se défendre, en s'efforçant d'utiliser cet environnement sans mot de passe, car cela désactive toutes les techniques d'attaque émergentes.
L'utilisation correcte de l'authentification multifacteur oblige les attaquants à travailler plus dur.
Et s'ils ne peuvent pas accéder à une identité et à votre organisation, lancer une attaque devient beaucoup plus compliqué.

Ressources

supplémentaires Pour en savoir plus sur les chaînes d'élimination, la compromission des courriels professionnels et la surface d'attaque moderne, consultez les ressources Microsoft ci-dessous.

- L'anatomie d'une attaque moderne Résumé des menaces de surface
- The CISO Insider Issue 3 : La sécurité centrée sur le cloud et comment les principaux RSSI comblent les lacunes de couverture
- Le numéro 1 des cybersignaux : L'identité est le nouveau rapport sur le champ de bataille
- La sécurité est aussi bonne que votre briefing sur les menaces mettant en vedette l'expert John Lambert

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230905
"C'est ensemble qu'on avance"