Defending Assets in the ‘New Normal’

In times of rapid change, current attack detection approaches looking for needles in stacks full of needles is futile. Network traffic and user behavior during this unprecedented period will shift to a ‘new normal’ (aka #workingfromhome). Everything AI engines have ‘learned’ will be irrelevant as sudden changes in user behaviors fire as anomalies. Tools focused on identifying disruptions of baselines will soon burden SOC teams with a tsunami of false positives at a time when skilled personnel and quick triage will be necessary to combat the near certainty of an attacker landing in the network.

Against this backdrop, cyber criminals are ratcheting up efforts—be it attack of VPN security gaps in newly spun up (or legacy) infrastructure, or phishing campaigns targeting large bodies of first time work-from-home users anxious for breaking health news or internal organizational communication updates.

• How robust are your current defenses?
• How will changes to the work environment affect your attack surface?
• What can you do to immediately reduce your risk?

Gain Visibility Into Your Attack Surface

Illusive’s free Attack Risk Assessment identifies attack risks in your network—artifacts attackers need and seek to navigate the network towards high-value assets. The assessment reveals risk factors you’ll want to be aware of and the value that ongoing, end-to-end cyber hygiene provides.

Within Hours, you'll discover hidden vulnerabilities
• Cached domain admin credentials
• Exposed endpoints with direct access to critical business assets
• Phantom RDP sessions
• Ambiguous “shadow admins”

Armed with this knowledge, you’ll be better positioned to defend your organization from these opportunistic attacks
Identify Attack Risk from the Safety of Your Home Office

Illusive’s fully remote Attack Risk Assessment evaluates six different attack surface categories, with review ranging from identification of ‘crown jewel’ assets, user credentials, and local administrators to network connection pathways and shadow admins. Each category is assigned a grade from A to F along with specific details of risk findings. The report concludes with recommendations for prescriptive execution of high-impact actions for each category and the potential grade improvements gained.

The Attack Risk Assessment assigns an overall grade based on findings across several attack surface categories along with a summary of key findings, e.g., 81 Unmonitored highly privileged users / 55% of hosts have Domain Admin privileges

Risk findings are grouped by category, e.g., Crown Jewels, Pathways, Shadow Admins along with specific details. Categories are graded on an A to F scale

High impact actions are recommended by category with expected improvement to grade, e.g., Disable 321 Shadow Admin Users. Improves grade from D to B

Identify Risk and Remediate

- Illusive’s experts will guide you through the simple process of initiating the assessment and operation on a local workstation or laptop
- Illusive and your team will define rules for identification of user credentials, mission critical connections, local admin and shadow admin users
- Data collected is analyzed to identify conditions that violate these rules
- Up to 7,500 endpoints can be included in the scope of discovery

Following the exercise, Illusive and your evaluators will meet via conference call to analyze the results, answer questions, and discuss how your organization could act on the data to preemptively harden your environment. The exercise requires very few resources—no external connections or integration testing. All of your data remains solely in your possession at all times.

Web: www.illusivenetworks.com
Email us: info@illusivenetworks.com
©2020 Illusive Networks Ltd.