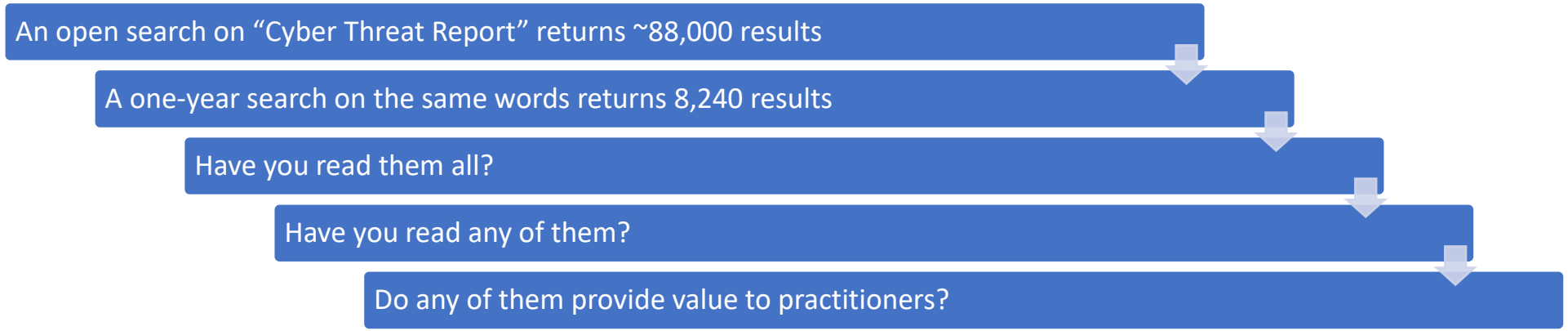
Cyber Threat Reports

Helpful or a Waste of Time?

There are at least hundreds of cyber threat reports released each year, almost all are from product or services vendors. Are they informative or just a disguise to get you interested in buying from the author's company?



ColeSec LLC
Cybersecurity & Risk Management

Microsoft Digital Defense Report 2022

Our objective with this report is twofold:

1. To illuminate the evolving digital threat landscape for our customers, partners, and stakeholders spanning the broader ecosystem, shining a light on both new cyberattacks and evolving trends in historically persistent threats.
2. To empower our customers and partners to improve their cyber resiliency and respond to these threats.

!!!

Perhaps most importantly, throughout the MDDR we offer our best advice on the steps individuals, organizations, and enterprises can take to defend against these increasing digital threats. Adopting good cyber hygiene practices is the best defense and can significantly reduce the risk of cyberattacks. -Tom Burt, Microsoft CVP, Corporate Security & Trust

!!!

!!!

!!!

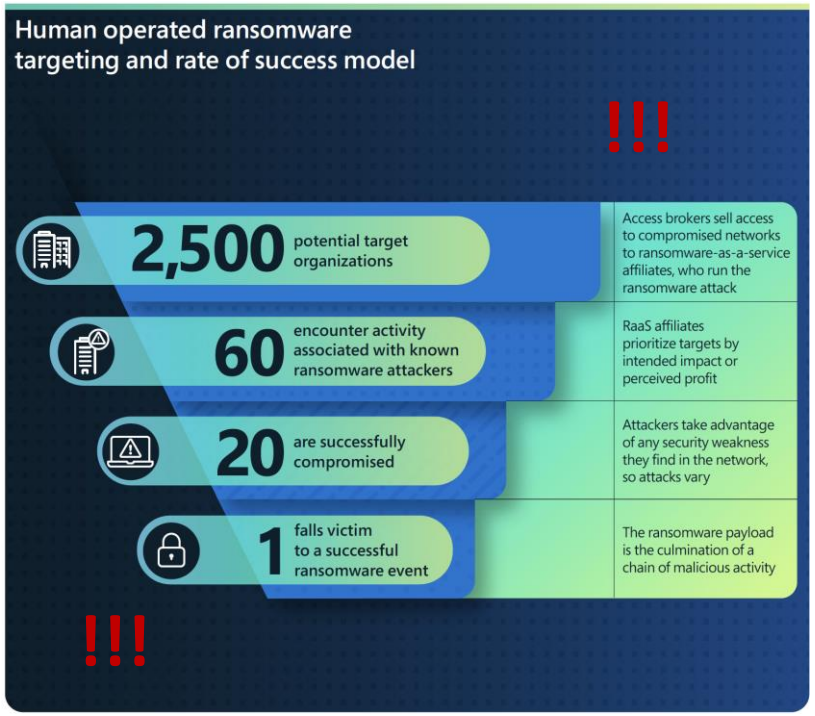
???

???

The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict. Russia has also supported its war with information influence operations, using propaganda to impact opinions in Russia, Ukraine, and globally. Outside Ukraine, nation

???

???



Actionable insights

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in disrupting the cybercriminal economy. !!!

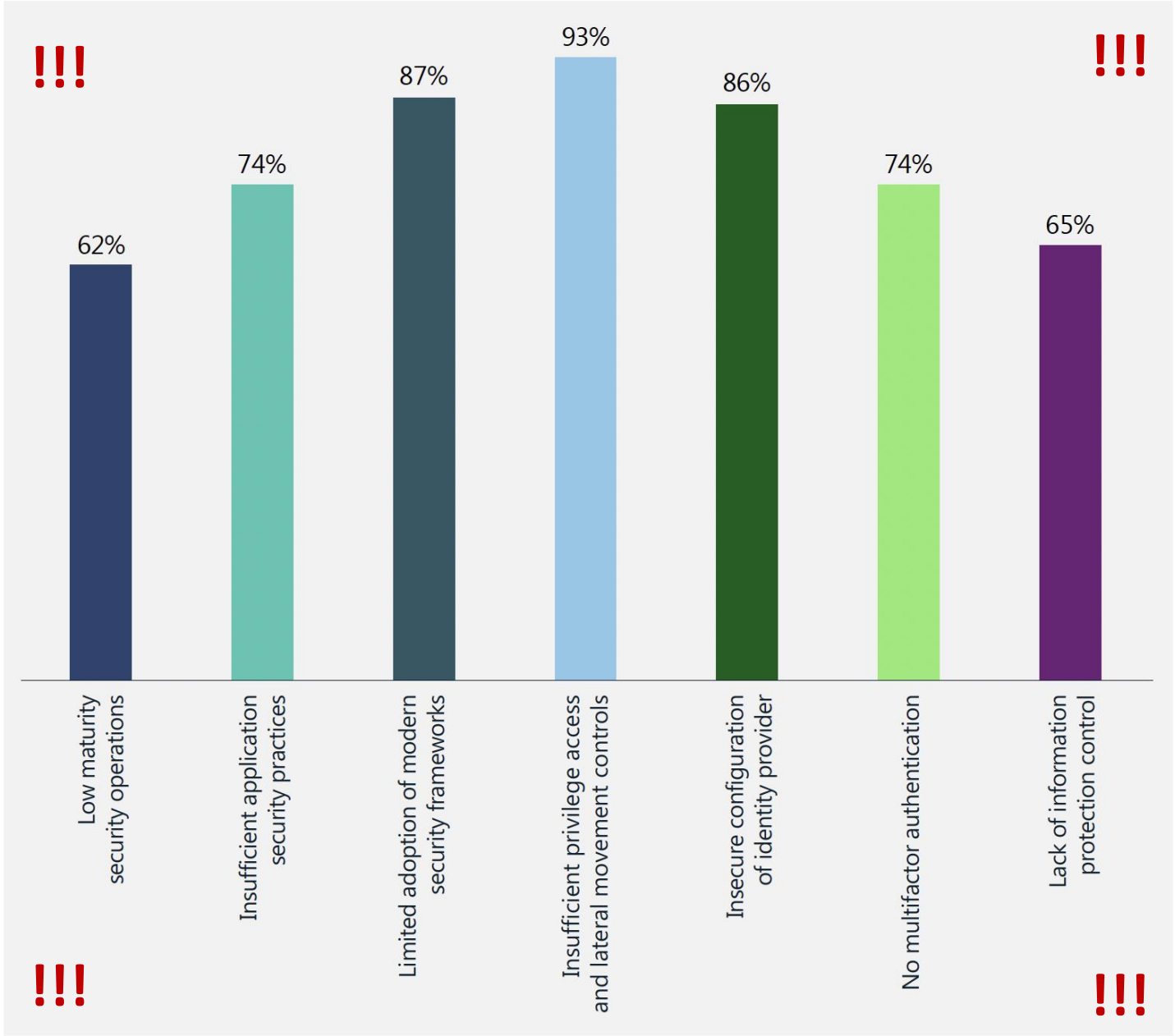
1. Build credential hygiene. More so than malware, attackers need credentials to succeed in their operations. The successful human-operated ransomware infection of an entire organization relies on access to a highly privileged account like a Domain Administrator, or abilities to edit a Group Policy.
2. Audit credential exposure.
3. Prioritize deployment of Active Directory updates.
4. Prioritize cloud hardening.
5. Reduce the attack surface.
6. Harden internet-facing assets and understand your perimeter.
7. Reduce SOC alert fatigue by hardening your network to reduce volume and preserve bandwidth for high priority incidents.

Links to further information

- RaaS: Understanding the cybercrime gig economy and how to protect yourself | Microsoft Security Blog
- Human-operated ransomware attacks: A preventable disaster | Microsoft Security Blog

!!!

Summary of most common findings in ransomware response engagements



The most common finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls.

Cyber Threat Reports Helpful? It depends

- In general, threat reports provide great value to cyber practitioners, as long as you remain aware that every company is looking to sell to you at every opportunity.
- Some vendor threat reports are blatant tools to try and sell you products or services.
- Find the reports from reliable vendor ***partners*** that fit your need and review each new iteration thoroughly for tidbits that can help you enhance your security posture.
- If a vendor can’t become your partner, time to find a new vendor.

*Some of the Better Report Links

- Microsoft Digital Defense Report 2022
  - https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022
- Mandiant M-Trends 2022: Cyber Security Metrics, Insights and Guidance From the Frontlines
  - https://www.mandiant.com/resources/blog/m-trends-2022
- CrowdStrike 2022 Global Threat Report
  - https://go.crowdstrike.com/global-threat-report-2022
- Verizon 2022 Data Breach Investigations Report
  - https://www.verizon.com/business/resources/reports/dbir/
- Ponemon/IBM Cost of a data breach 2022
  - https://www.ibm.com/reports/data-breach

*not all ~88,000 links

Tony Cole
LinkedIn: www.linkedin.com/in/wmtonycole
Twitter: https://twitter.com/NoHackn

ColeSec LLC
Cybersecurity & Risk Management