David C Frier, CISM, CISSP, etc.

Reducing the Attack Surface

A COMPREHENSIVE APPROACH TO ENHANCING ORGANIZATIONAL INFORMATION SECURITY

Agenda

- Who is this guy?
- What is this all about?
- Why does this matter?
- What was that, again?
- But I have questions!

Who is this Guy?

- David C Frier, CISM, CISSP, CRISC, CCSK
- vCISO and Senior Cybersecurity Program Manager at Sedara… *but I speak only for myself, not for Sedara!*
- I've been doing Information Security for I* years. Been in IT, from the metal on up, for 20*
- Avid player of poker… Orioles and Cubs fan… enthusiastic-if-slow rider of a Trek.

* - *base 22*

Geekosaurus

Who is this Guy?

What is this all about

- Attack Surface Definition
- What are the components of Attack Surface
- How to know your Attack Surface, "for sure"
- What to do about your Attack Surface
- What kind of tools are out there

Attack Surface Definition

- Attack Surface is: ***the total set of vulnerabilities your organization exposes to the world***
- It includes Digital and Physical aspects
- Even humans: employees can be approached, bribed or coerced, burgled or robbed
- Some non-cyber areas are beyond the scope of this talk. We'll focus mainly on the digital.

Attack Surface Components

- Digital Components include
  - Web applications
  - Mobile applications
  - Cloud – EaaS
  - APIs – visible and hidden
  - Shadow IT
  - IoT "stuff"
  - Everything remote workers connect to
- Physical components include:
  - Data centers
  - Offices
  - Portable & Mobile devices with company data
- *Do your vulnerability scans hit all of these?*

Knowing your attack surface "for sure"

- **If you don't know about it, you can't defend it!**
- Inventory everything:
  - Web applications
  - All Cloud properties:
    - SaaS accounts, PaaS/IaaS tenancies, Servers, Microservices
  - APIs – including "hidden" or "private"
  - Shadow IT
  - IoT
  - Hybrid & Remote Workers
- You may do this by hand, you may obtain a tool to help

Knowing your attack surface "for sure"

- Let's talk about... APIs
  - "Hidden" or "private" APIs can be a real danger.
  - Home-built AND 3rd party
    - 3rd party products often have undocumented APIs
    - You will have to hunt them up to test them

Knowing your attack surface "for sure"

- Let's talk about... Shadow IT
  - Not in your asset management
  - How can you find it all?
    - Check FW logs for egress
    - Try an amnesty program

Knowing your attack surface "for sure"

- Let's talk about… IoT
  - Probably found in discovery scans
  - Often without owner, unlike applications or infrastructure
  - Probably reachable via arcane pathways from Internet
  - May be phoning home.
    - P = 1.0, unless blocked
    - Now you have all the vulnerabilities of its mfr. to deal with
  - These items need to be isolated as much as possible
  - They should also be blocked from Internet access

Knowing your attack surface "for sure"

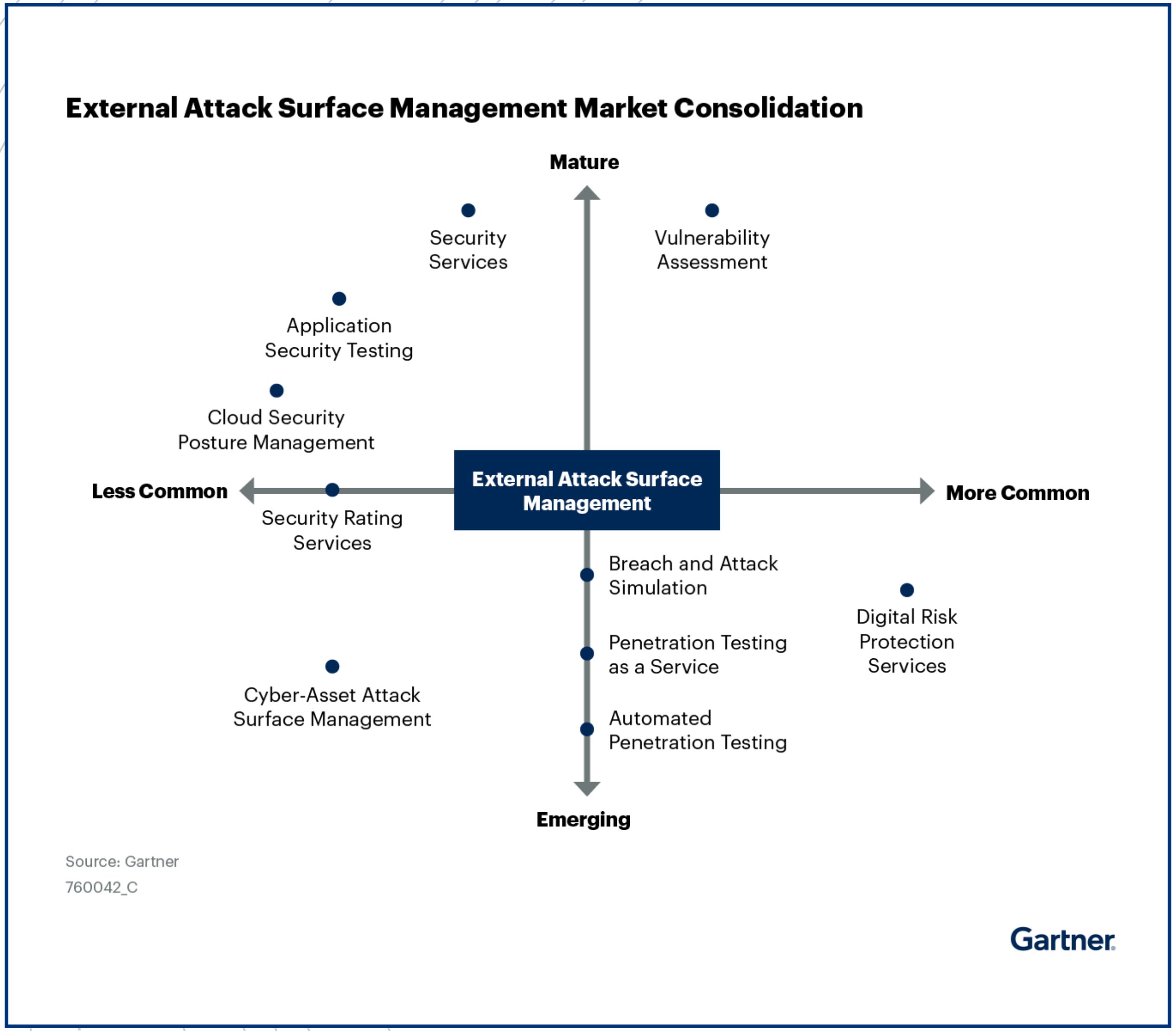
- Let's talk about… Hybrid / Remote Workers
  - Taking company computers home or to coffee shops
  - Connected via VPN and…
  - …split tunneled?
  - How do you manage not to create a bridge between corporate network and little Danny's Minecraft server

What to do about your Attack Surface

1. Find it - Asset discovery and inventory
2. Prioritize it - Threat modeling
3. Assess it - Scanning and Testing
4. Reduce it – Remediation, Code Minimization
5. Separate it – Network Segmentation to the MAX
6. Watch it - Monitoring and Reporting
7. Automate all of the above

What kind of tools are out there

- Two classes of tools
  - EASM – External Attack Surface Management
  - CAASM – Cyber Asset Attack Surface Management
- EASM – polices up your "Perimeter"
- CAASM – reaches for all digital assets
  - Most CAASM tools are a superset of EASM tools now



External Attack Surface Management Market Consolidation

Mature
Security Services
Vulnerability Assessment
Application Security Testing
Cloud Security Posture Management
Less Common
External Attack Surface Management
More Common
Security Rating Services
Breach and Attack Simulation
Digital Risk Protection Services
Penetration Testing as a Service
Cyber-Asset Attack Surface Management
Automated Penetration Testing
Emerging
Gartner

Source: Gartner
760042_C

Tools are Evolving through M&A

- Major vendors acquiring niche companies
  - Example: Tenable bought Bit Discovery to add EASM to its commodity vuln. scanning service
  - Example: IBM acquired Randori to get CAASM into its arsenal
- **This market is a moving target**

Why does this matter?

Someone once said…

- …"If you don't know about it, you can't defend it"
- *Don't I already do vulnerability scans?*
- *As long as everything is scanned, I'm OK, right?*
- Are you a Compliance or a Security?
- Third party responsibilities – do you need more?

What was that again?

I will now make everything as simple as possible but no simpler

- Find all the things
- Be sure to be searching for all the TYPES OF things
- Reduce all the things, as much as practical
- Isolate all the things, as much as practical
- *Maybe* get a tool to help with all the things
- Automate all the things

Further reading

- Paladin Cloud on CAASM
- IBM topic on Attack Surface
- Randori Report
- OWASP Cheat Sheet Series - ASM
- Hidden APIs
- CrowdStrike's Cybersecurity 101 Series
- Team Cymru Resource Library
- Gartner: EASM Competitive Landscape

But… I have questions!

How to reach me

- david.frier @ rocinfosec.com
- BlueSky
- Mastodon
- LinkedIn
- About.Me
- Twitter, Facebook, Instagram?

nope^3

If all else fails, try to find me IRL