Randori

MAN IN THE MIRROR

Upping Your Threat Hunting Game
By Seeing Yourself Like An Attacker.

July 2020

www.randori.com/DFIR

ERIC MCINTYRE

DIRECTOR OF R&D

HI, I'M ERIC.

I'm Eric McIntyre, Director of R&D at Randori. Previously, I served as a security researcher at Kyrus Tech, where I worked for six years leading teams supporting clients in the national and commercial security spaces. I love landing exploits, running, and exploring the outdoors.

Follow: @pwnpnw | @RandoriAttack

OUTLINE

01 | The Beginning and The End

02 | Flipping the Script

03 | Think Like an Attacker

04 | Take Action

Randori

OUTLINE

01 | The Beginning and The End

02 | Flipping the Script

03 | Think Like an Attacker

04 | Take Action

Randori

THE POINT

FIRST...

- I'm not a threat hunter.
- I'm not here to teach you how to threat hunt.
- I'm here to tell you how we hack companies at scale and explain the attacker's perspective.
- When I say *red* in this talk, I mean *adversary*.

AND FINALLY...

- You can't hunt what you don't detect.
- Understanding how attackers think will make you a better threat hunter.
- Better prediction leads to effective prioritization leads to optimization of resources and reduction of risk.

OUTLINE

01 | The Beginning and the End

02 | Flipping the Script

03 | Think Like an Attacker

04 | Take Action

Randori

RED HAS TO BE RIGHT ONCE. BLUE HAS TO BE RIGHT ALL THE TIME.

Randori

RED HAS TO BE RIGHT ONCE. BLUE HAS TO BE RIGHT ALL THE TIME.

WRONG.

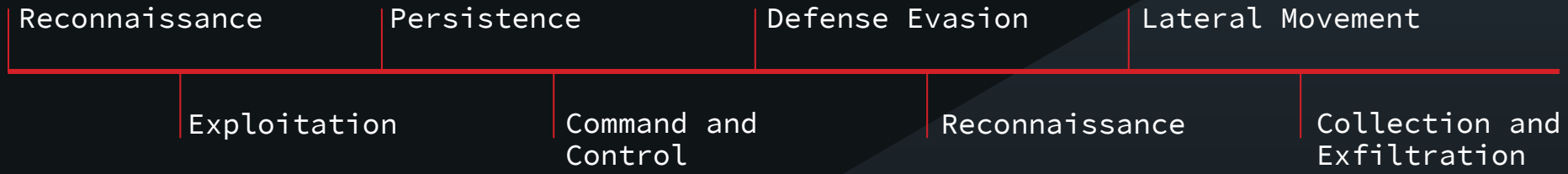
Randori

BLUE HAS TO BE RIGHT ONCE. RED HAS TO BE RIGHT ALL THE TIME.

IRL.

Randori

KILL CHAIN



Randori

ADVANTAGE BLUE

- Every action I take is a opportunity to get caught
- You know the playing field
- Getting caught is expensive

Randori

ADVANTAGE RED

- I know your tools
- You lack control
- Time is on my side

Randori

OUTLINE

01 | The Beginning and the End

02 | Flipping the Script

03 | Think Like an Attacker

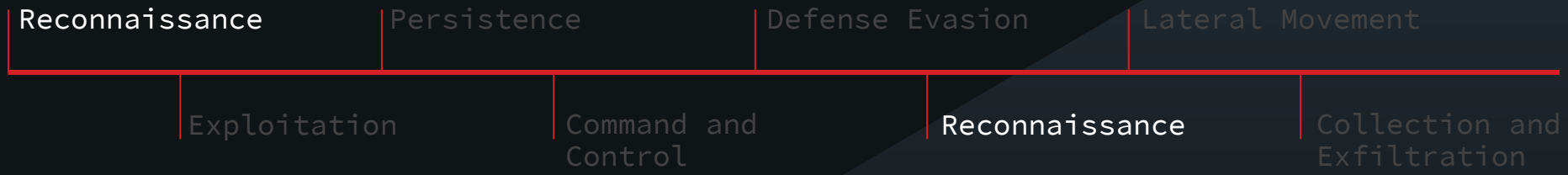
04 | Take Action

Randori

THIS TALK IS ABOUT HOW YOU CAN OPTIMIZE YOUR DEFENSES.

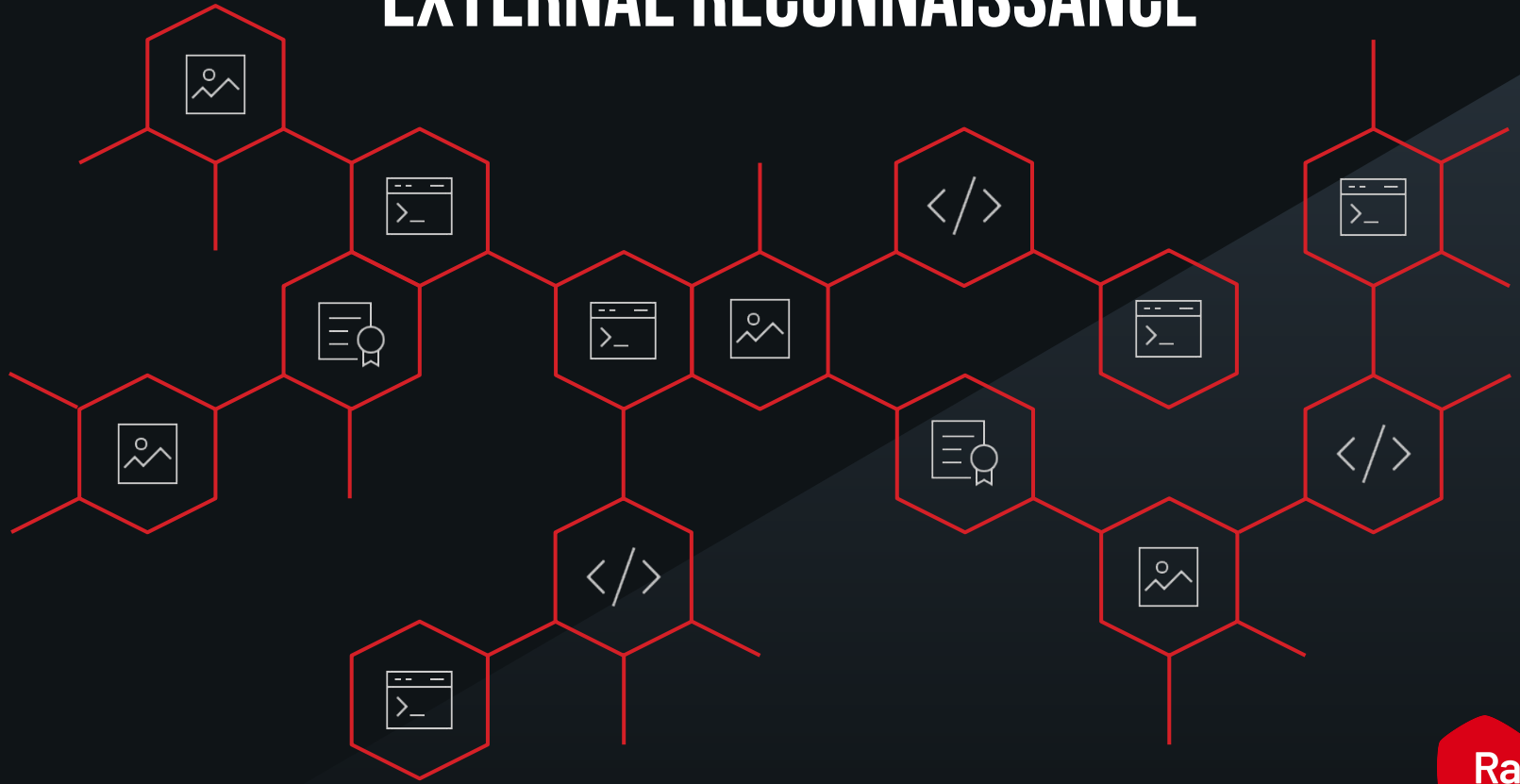
BY THINKING LIKE AN ADVERSARY.

KILL CHAIN



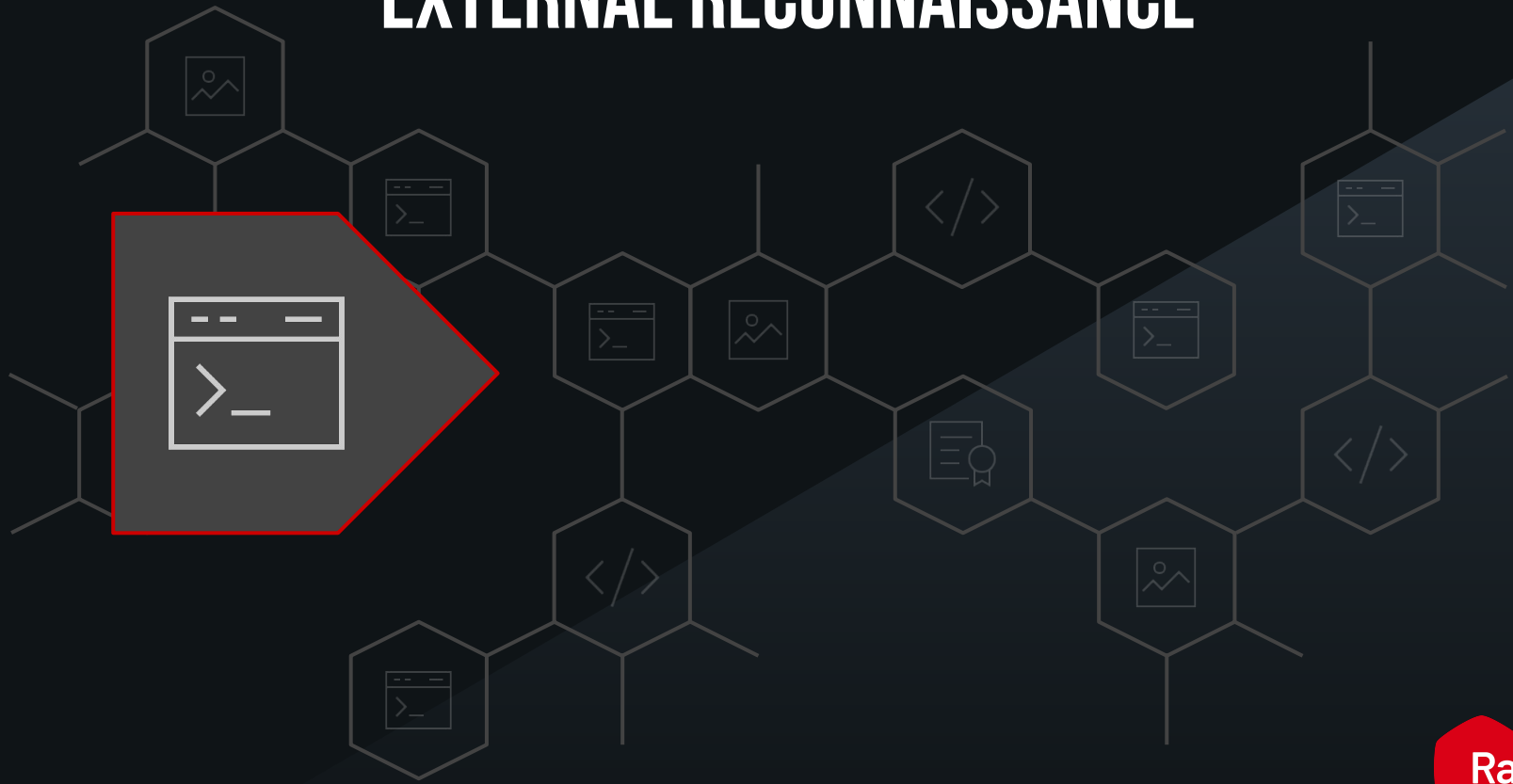
Randori

EXTERNAL RECONNAISSANCE



Randori

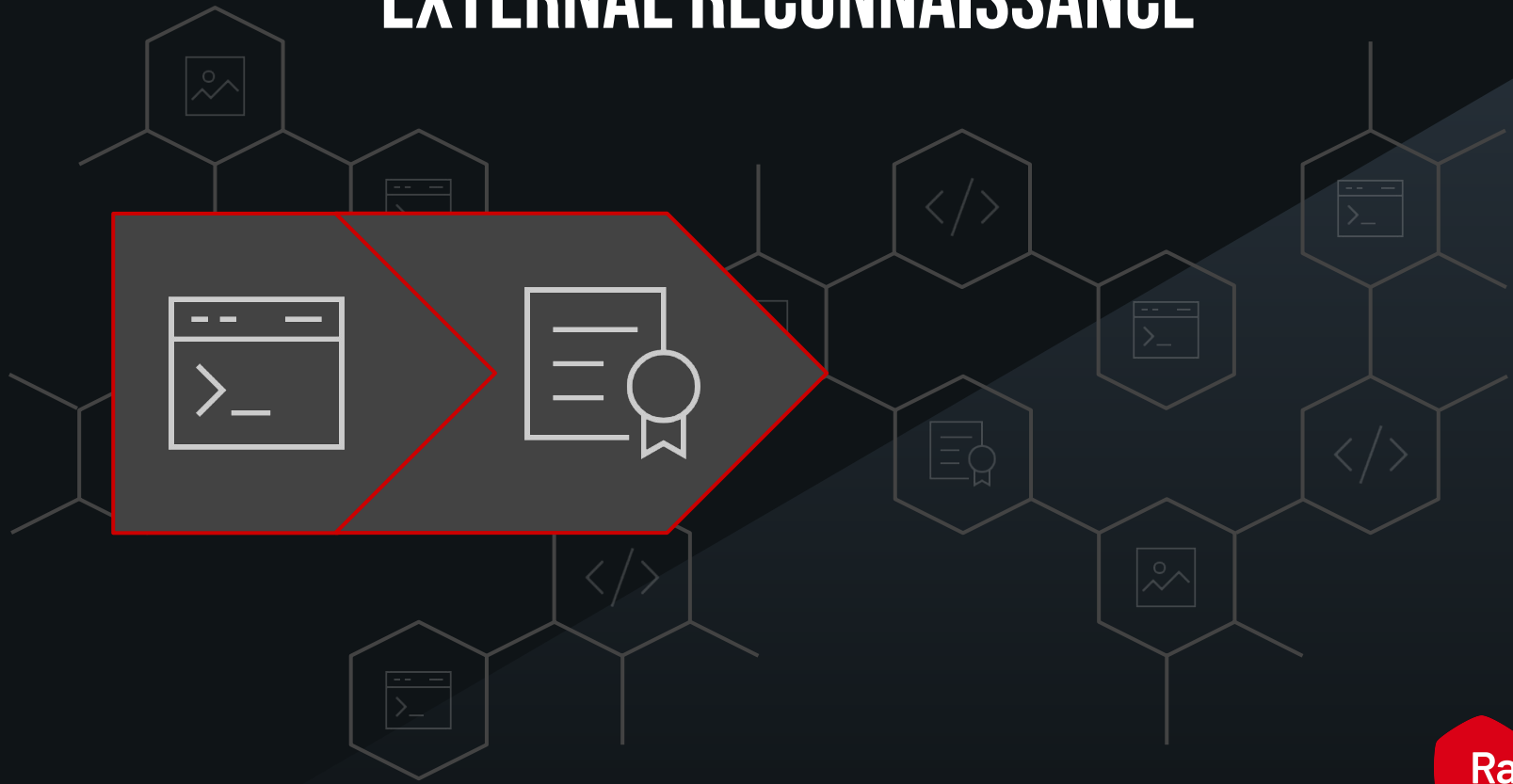
EXTERNAL RECONNAISSANCE



www.randori.com/DFIR

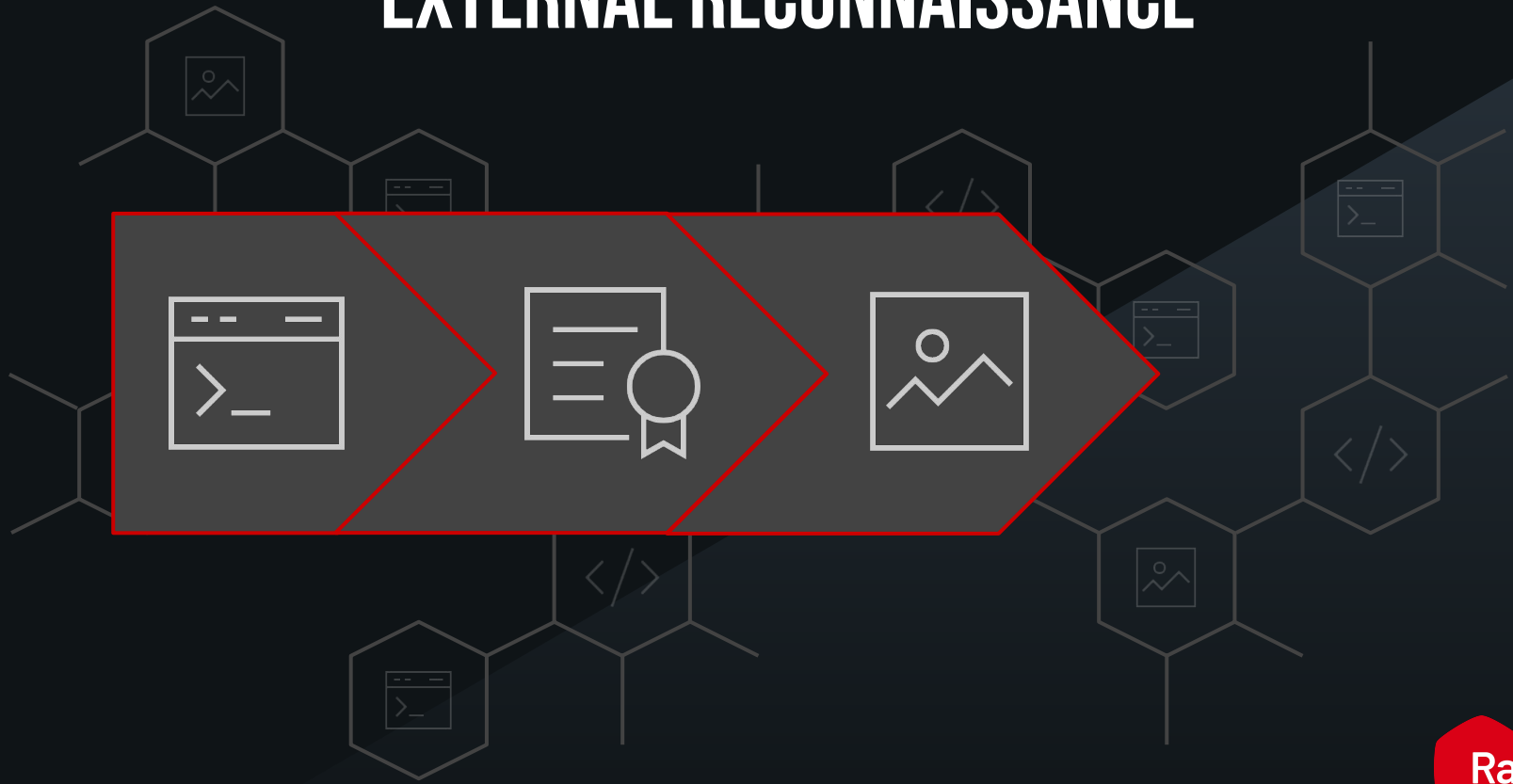
Randori

EXTERNAL RECONNAISSANCE



Randori

EXTERNAL RECONNAISSANCE



Randori

EXTERNAL RECONNAISSANCE

Randori

SIX FACTORS OF TEMPTATION

ENUMERABILITY
Precision of detection

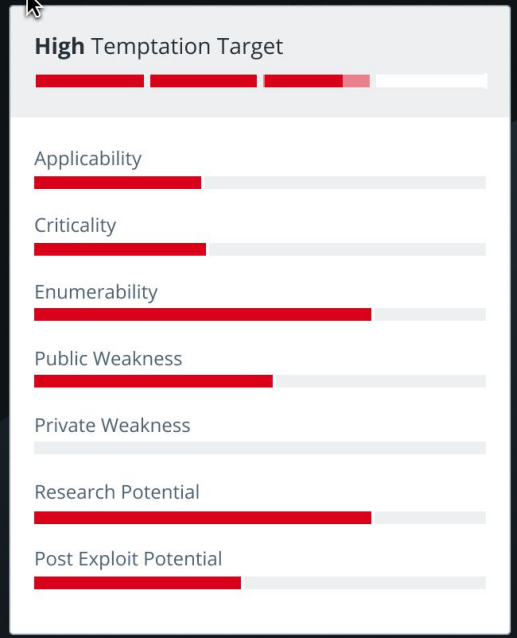
WEAKNESS
Known disclosures and exploits

CRITICALITY
Importance of function

APPLICABILITY
Level of adoption

POST-EXPLOITATION POTENTIAL
Usefulness after compromise

RESEARCH POTENTIAL
Ease of development

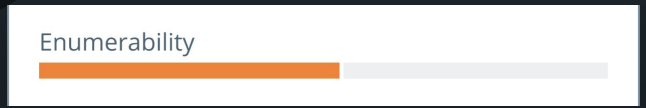


Randori

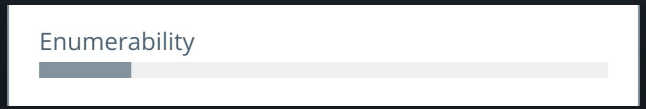
ENUMERABILITY
PRECISION OF DETECTION

Detecting an exact version, patch level, and configuration

Detecting a major and minor version



Detecting only the software name



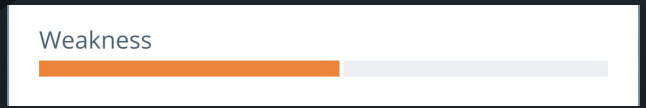
Randori

PUBLIC/PRIVATE WEAKNESS

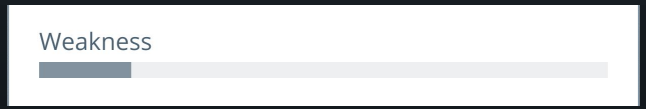
KNOWN DISCLOSURES AND EXPLOITS

Critical, reliable, unauthenticated remote code execution with PoC

Local privilege escalation, post-authentication



Possible information disclosure vulnerability



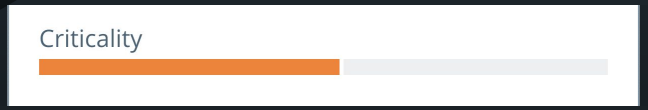
Randori

CRITICALITY

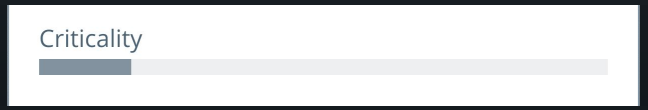
IMPORTANCE OF FUNCTION

Services that inherently define a critical security boundary

Services infrequently, but possibly on a security boundary



Services not commonly on a security boundary

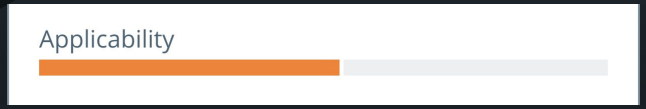


Randori

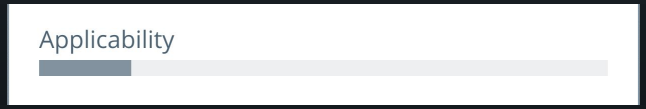
APPLICABILITY
LEVEL OF ADOPTION

A ubiquitous service found in most enterprises

A service found in limited segments



An unusual service with few users



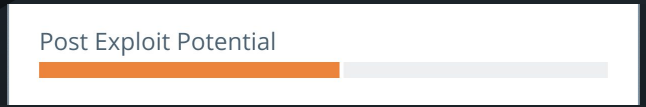
Randori

POST-EXPLOITATION POTENTIAL

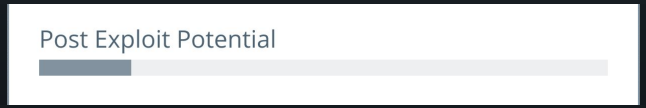
USEFULNESS AFTER COMPROMISE

Well-known environment where few defenses exist

Common environment with likely defenses



Esoteric or highly defended environment



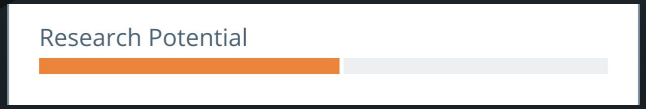
Randori

RESEARCH POTENTIAL

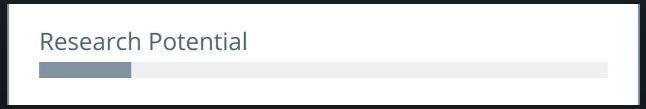
EASE OF DEVELOPMENT

Tooling, research, PoCs, and exemplars exist

Some prior research, but may lack development tools



Difficult to obtain hardware, no tools, no prior research



Randori

SIX FACTORS OF TEMPTATION

ENUMERABILITY
Precision of detection

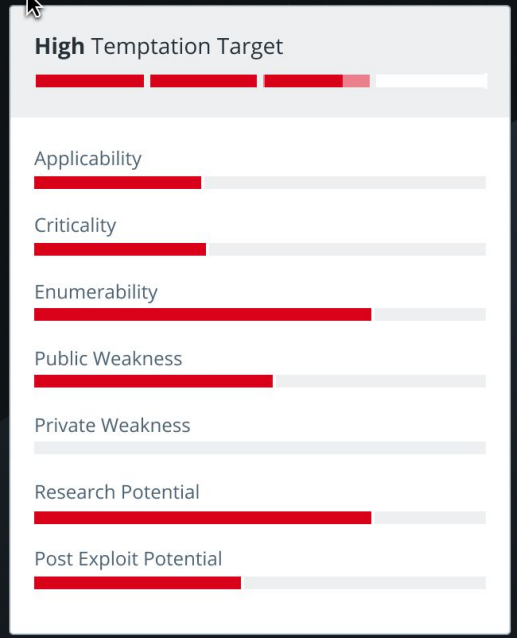
WEAKNESS
Known disclosures and exploits

CRITICALITY
Importance of function

APPLICABILITY
Level of adoption

POST-EXPLOITATION POTENTIAL
Usefulness after compromise

RESEARCH POTENTIAL
Ease of development



Randori

OUTLINE

01 | The Beginning and the End

02 | Flipping the Script

03 | Think Like an Attacker

04 | Take Action

Randori

TAKE ACTION

IF YOU BELIEVE THIS...

- ➔ You can't hunt what you don't detect.
- ➔ Understanding how attackers think will make you a better threat hunter.
- ➔ Better prediction leads to effective prioritization leads to optimization of resources and reduction of risk.

THEN DO THIS...

- ➔ Utilize black box discovery to see your attack surface like an attacker.
- ➔ Gain an attacker's perspective.
- ➔ Rank your targets and prioritize them based on risk, accounting for both temptation (likelihood) and impact.

Randori

JOIN US ON 9/3

HIDING IN THE NOISE

EVAN ANDERSON
DIRECTOR OF OFFENSE

Adding new security tools to your OSOC toolset may help alert you to your business's latest cyber threats. However, when a million unprioritized alerts hit you in a day, it's easy to quickly reach for the snooze button without understanding what is truly going on. Drowning in alerts, the best enterprises are discovering that to cut through the chaos and triage alerts accurately, operators need to undersand the attack from the adversary's perspective.

REGISTER www.randori.com/DFIR
FOLLOW US: @RandoriAttack