

A small green seedling with two leaves is growing out of a crack in a dark, textured rock surface. The background is blurred, showing more of the rock and some moss.

New Age of Penetration Testing

Persistent, Not Necessarily Advanced



WHO AM I?



- COO, PRINCIPAL AND FOUNDER AT RIVER SECURITY
- PRINCIPAL INSTRUCTOR AT SANS
- CO-AUTHOR OF SEC550 – CYBER DECEPTION, ATTACK DETECTION, DISRUPTION AND ACTIVE DEFENSE
- SHORT SUMMARY:
- I SHOW HOW CRIMINALS BREAK-IN,
AND I HELP THROW THEM BACK OUT...

GCIH GIAC Certified Incident Handler
GPEN GIAC Certified Penetration Tester
GSLC GIAC Security Leadership
GIAC Mobile Device Security Analyst
GDAT GIAC Defending Advanced Adversaries
GCTI GIAC Cyber Threat Intelligence
GCFA GIAC Certified Forensic Analyst



WHY DO WE DO PENETRATION TESTING?

WHAT IS THE GOAL OF PENETRATION TESTING?
(LEGIT QUESTION)

Common problems with penetration testing

I have been lucky enough to be on both sides of the table:

- Several years as CISO
- Procurer and receiver pentest

I have Built, trained and managed several penetration testing teams.



A group of business professionals in an office setting. A woman in a grey blazer is pointing at a tablet held by another person. A man in a dark suit and striped tie is visible on the left. The scene is brightly lit, likely from a window in the background. The text "Do Attackers Care About Scope?" is overlaid in the center in a white, bold, sans-serif font.

Do Attackers Care About Scope?

Digital Footprint Assessment



Mapping Attack Surface First

- Immediate **value** by just having hackers LOOK at you
- Smaller investment up front
- Easier to guarantee that the entire (or just some) of the scope has been tested
 - Customer and Provider knows what has been left out of scope
- Find shadow IT, unmanaged data
- Bottom-up approach!



Digital Attack Surface Report



Might lead into



Penetration Test Report

Digital Footprint Report

Focus Points and Summary

Overview of Applications, status and attractiveness

Lists of leaks, vulnerabilities and everything else a customer may find useful.


Value, value, value!

SERVICES

This section shows the different assets we have found to be potentially included in scope, or that needs to govern under security management of the client.

Legend

Purple	Assets with a high business value and high chance of vulnerabilities are present.
Red	Assets with a medium impact to the organization. Consider in-scope for testing.
Yellow	Assets that will likely not be targeted or contains a third-party logon. We should try compromised passwords against these.
Green	Probably safe assets with little or no attack surface or avenues for attack.
Grey	Assets that we have consider out of scope. See Appendix.

HOSTNAME	ATTACK SURFACE COMMENT
http [REDACTED]	<p>[REDACTED]</p> <p>Refreshes stats from power station every 5 seconds.</p> <p>/tags expose available tags which has much more information that is shown on the website.</p> <p>These tags may be retrieved via the /tagbatch endpoint.</p> <p>Equipment looks to be a [REDACTED] panel from [REDACTED] This API supports updating values as well as reading them. (not tested to avoid operational issues).</p> <p>This was reported and removed during assignment. It now just redirects to the [REDACTED]</p> 



WHAT IS ATTACK SURFACE MANAGEMENT?



HIGH LEVEL PENTEST METHODOLOGY



The Digital Footprint Dilemma

- Businesses want an increased digital footprint and presence
- From a Cyber Security point of view, we want a small footprint
- Continuous Attack Surface Management helps mitigate the problem



Cyber Security Team



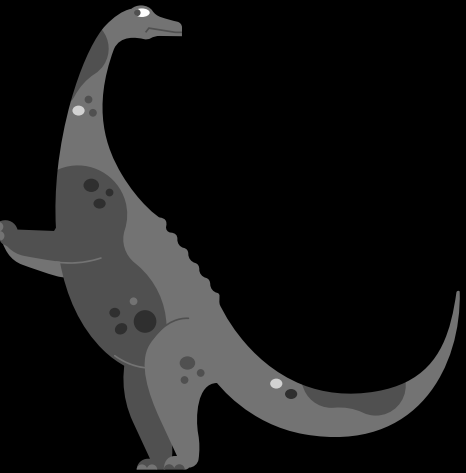
Organizations Direction

WHAT IS ALWAYS-ON PENTESTING & OFFENSIVE SOC?





With Traditional
PenTesting -
Are we playing
the same game
as attackers?



HIGH LEVEL PENTEST METHODOLOGY



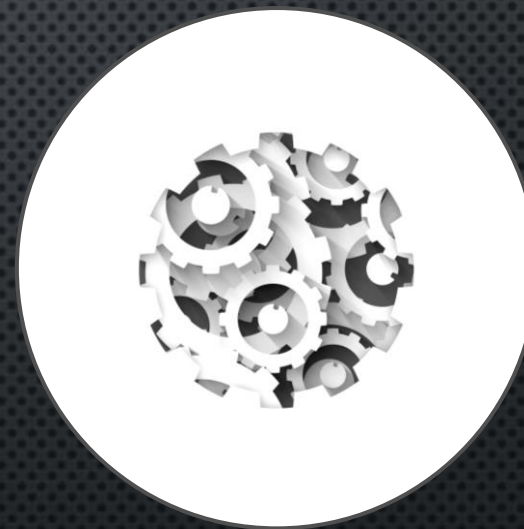
ALWAYS-ON PENTESTING

NEW ATTACK SURFACE (DELTA)



- Recon, Discover and Scan continuously
- Pentest and assess ASAP

EXISTING ATTACK SURFACE



- Hunt on existing targets
- Use new CTI to assess ASAP



OBSERVE change to Attack Surface

DECIDE to develop working exploit and notify customer

OODA LOOPS

Beating Attackers At Their Own Game

ORIENT
ourselves

Customer ACT based
on recommendation

Examples Impact



Confluence Support Documentation Knowledge base Resources ▼

Atlassian Support / Conflue... / Docume... / ... / ... / Confluence Security Overview...

Confluence Security Advisory 2022-06-02

Confluence Server and Data Center - CVE-2022-26134 -
Critical severity unauthenticated remote code execution
vulnerability

Examples Impact

[9136119374](#)

Leaf certificate

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2023-04-11 15:14:44 UTC	946730466	Google	https://ct.googleapis.com/logs/argon2023
2023-04-11 15:14:44 UTC	1087671115	Google	https://ct.googleapis.com/logs/xenon2023

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2023-04-30 17:02:00 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

SHA-256 [3C83AE9615000A17FB74B7184BAC079CA697DF84BED49CF0F60CE0087C93AB61](#) **SHA-1** [B73190DD96729212CFBB509F343B6A8FB65BEB59](#)

[Certificate:](#)

Data:

Version: 3 (0x2)

[Serial Number:](#)
03:a7:0a:c7:37:24:55:80:a2:43:54:cb:6b:d2:46:fb:a0:df

Signature Algorithm: ecdsa-with-SHA384

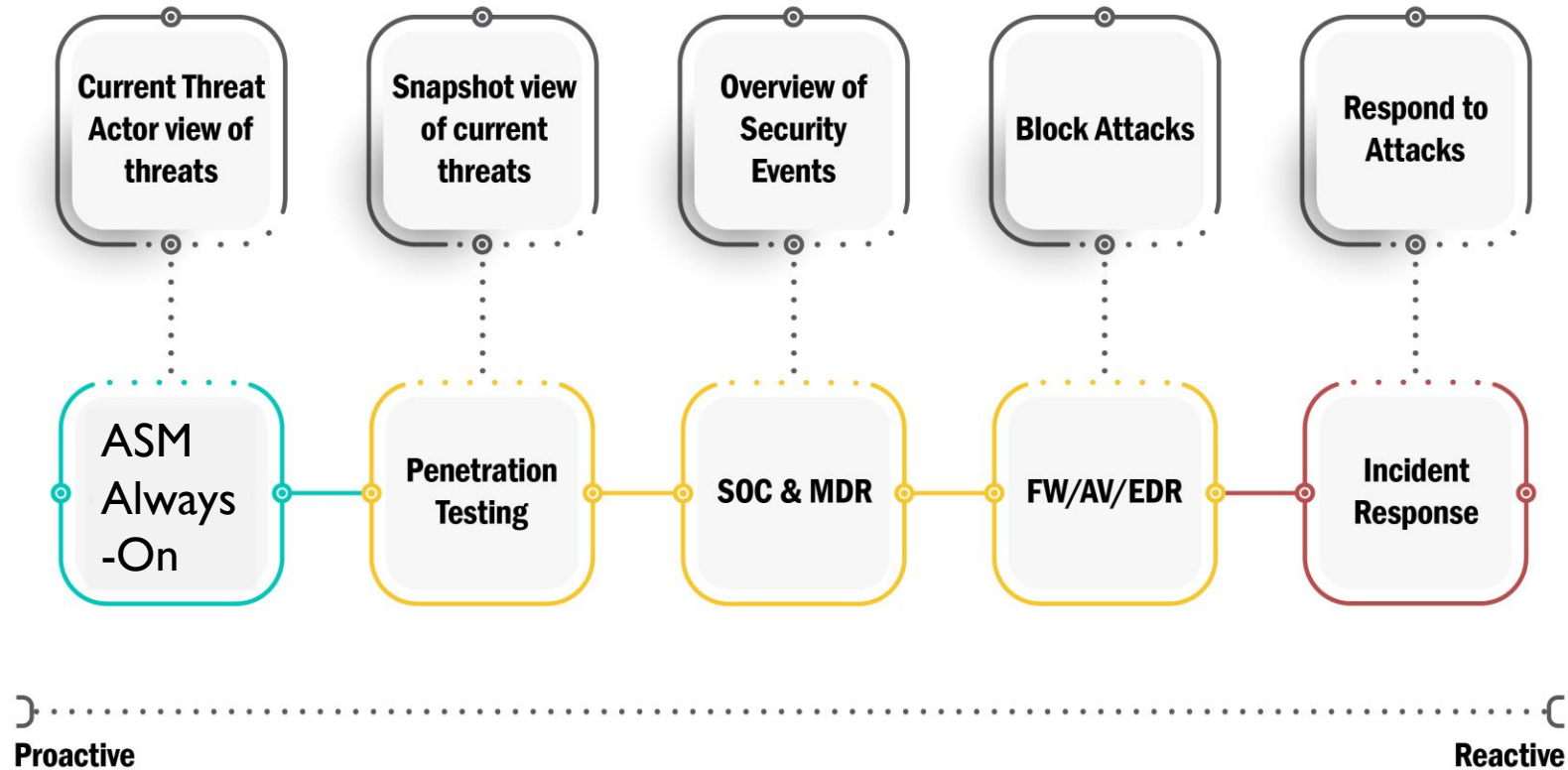
[Issuer:](#) (CA ID: 183283)
commonName = E1
organizationName = Let's Encrypt
countryName = US

Validity
Not Before: Apr 11 14:14:44 2023 GMT
Not After : Jul 10 14:14:43 2023 GMT

Subject:
commonName = *.af.riversecurity.eu

[Subject Public Key Info:](#)
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)

Proactive vs. Reactive





Defend Forward





Cyber Warfare vs. Traditional Warfare

“Know yourself, know your enemy, you will not fear the result of a hundred battles”
Sun Tzu, The Art of War

1. KNOW YOURSELF

The task once dubbed asset inventory remained neglected

Until OFFENSIVE SOC

2. KNOW ATTACKERS

Pentesting was deemed annual or solely for compliance by the industry

Until OFFENSIVE SOC

3. ADVANCED PERSISTENT THREAT

Pentesting has lacked agility and sustained impact

Until OFFENSIVE SOC



<https://into.bio/chrisdale> & <https://into.bio/rivsec>

🔼 Download slides here!



Twitter – <https://twitter.com/ChrisADale>



LinkedIn – <https://www.linkedin.com/in/chrisad/>



Fighting Cyber Crime – <https://riversecurity.eu>

Work with us! We ARE hiring by **attitude**, and train for **talents** 🧠