



Offensive Services as **Preventive** Security Measures

Penetration Testing is changing, are you?



WHO AM I?



COO, PRINCIPAL AND FOUNDER AT RIVER SECURITY

PRINCIPAL INSTRUCTOR AT SANS

- 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 a meeting, looking at a tablet. The text "Do Attackers Care About Scope?" is overlaid in the center.

**Do Attackers Care
About Scope?**

Digital Footprint Assessment



Map Attack Surface First

- Immediate **value** by just having hackers LOOK at you
- Bottom-up approach!
- Smaller investment up front
- Find shadow IT, unmanaged data
- Scope is suddenly defined
 - Customer and Provider knows what has been left out of scope

Attack Surface Overview

The following table shows an overview of your attack surface.

Domains	Total
Apex	151
Subdomains	1474
Out Of Scope	283
False Positive	1598
Suspicious	1

Applications	Total
Apps	862
Shadow	509
Out Of Scope	86
False Positive	3

IP-Addresses	Total
IP-Addresses	624

Legend	Explanation
Apex	Registered domain names eg: riversecurity.eu
Subdomains	FQDN that is not the registered domain
Out Of Scope	Usually, domains pointing to 3rd party service, that is out of scope. These are excluded from automatic scanning and testing from pen-testers
False Positive	False positives found by our tools, but not belonging to or related to the customer.
Shadow	Entities that has an attack surface but is represented by another entity. Most common example would be a http service, that also have the same service served over https.

- Dashboard
- Reports
- Issues
- Entities

- Staging
- chris@riversecurity.no
- Log out
- Report a problem

Reported issues ▾

All Categories ▾

Sort by: Date C

← Go Back

↓ Download PDF

Issues identified

The following issue have been found or is still open on the attack surface.

Several Power Plants Available Online with No Authentication or Authorization - Possible Kinetic Damages

ID: 64ebb5e7653e6a29398400c6

Severity: Critical | Category: Vulnerability | Status: Reported

Description:

Two websites presenting various metrics from two power plants were discovered. One of these exposed an API from an XXXXX XXX xxx device which is used to connect to operational technology devices such as PLCs, servos, and drives. The websites show some summary metrics as can be seen in the image below:



Proof of concept:

Light testing showed that we could extract much more detailed information by sending system-specific requests than we could find by looking at the documentation for this system. This could be used to retrieve and even alter data from the system. The finding was reported, and the site was promptly fixed. A similar page was found for XXXXXX. This site was very similar in layout, but the page became unavailable shortly after the first site was reported. Since the page was removed we were not able to verify if it also exposed some OT functionality.

/XXXXXXX expose available tags which has much more information that is shown on the website. These tags may be retrieved via the /XXXXXXXX endpoint. Equipment looks to be a XXXXXXXXXX panel from XXXXXXXXXX (at least it seems to be API compatible). This API supports updating values as well as reading them. (not tested to avoid operational issues).

Recommendations:

This was reported and removed during assignment. It now just redirects to the XxxXXXXX appliance at port 443.

These risks seem to have been mitigated, but we recommend reviewing why these sites were placed online in the first place to prevent them re-appearing without a proper security review.

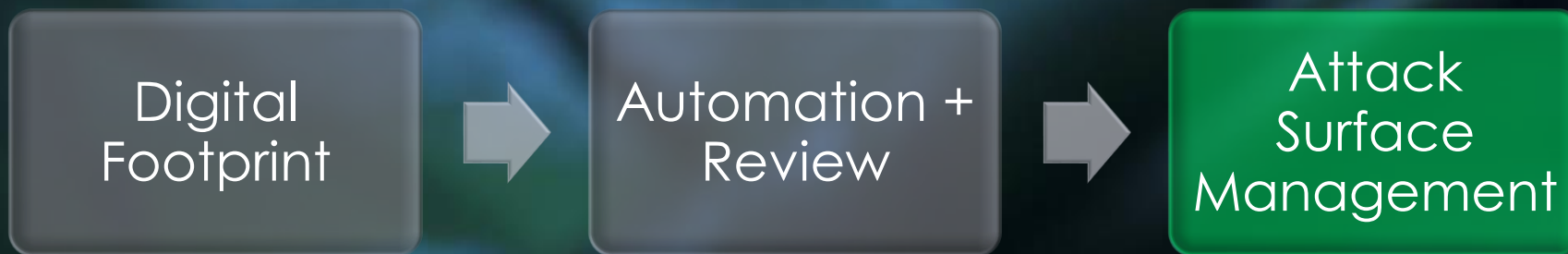
A proper strategy and necessary tactics should be built and reviewed when planning and deploying new IT solutions, especially critical ones like these. The strategy and tactics employed should be reviewed on a continuous basis to ensure that we are conforming.

Affected assets: (1)

[REDACTED]



WHAT IS ATTACK SURFACE MANAGEMENT?



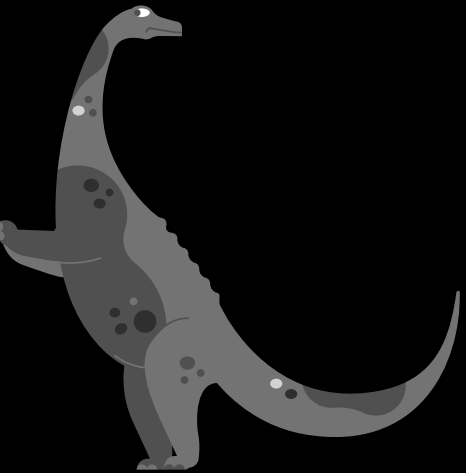
HIGH LEVEL PENTEST METHODOLOGY



WHAT IS ALWAYS-ON PENTESTING & OFFENSIVE SOC?



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

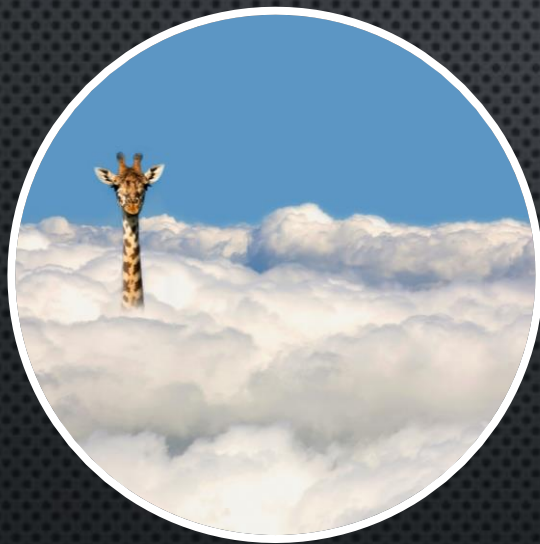


HIGH LEVEL PENTEST METHODOLOGY



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

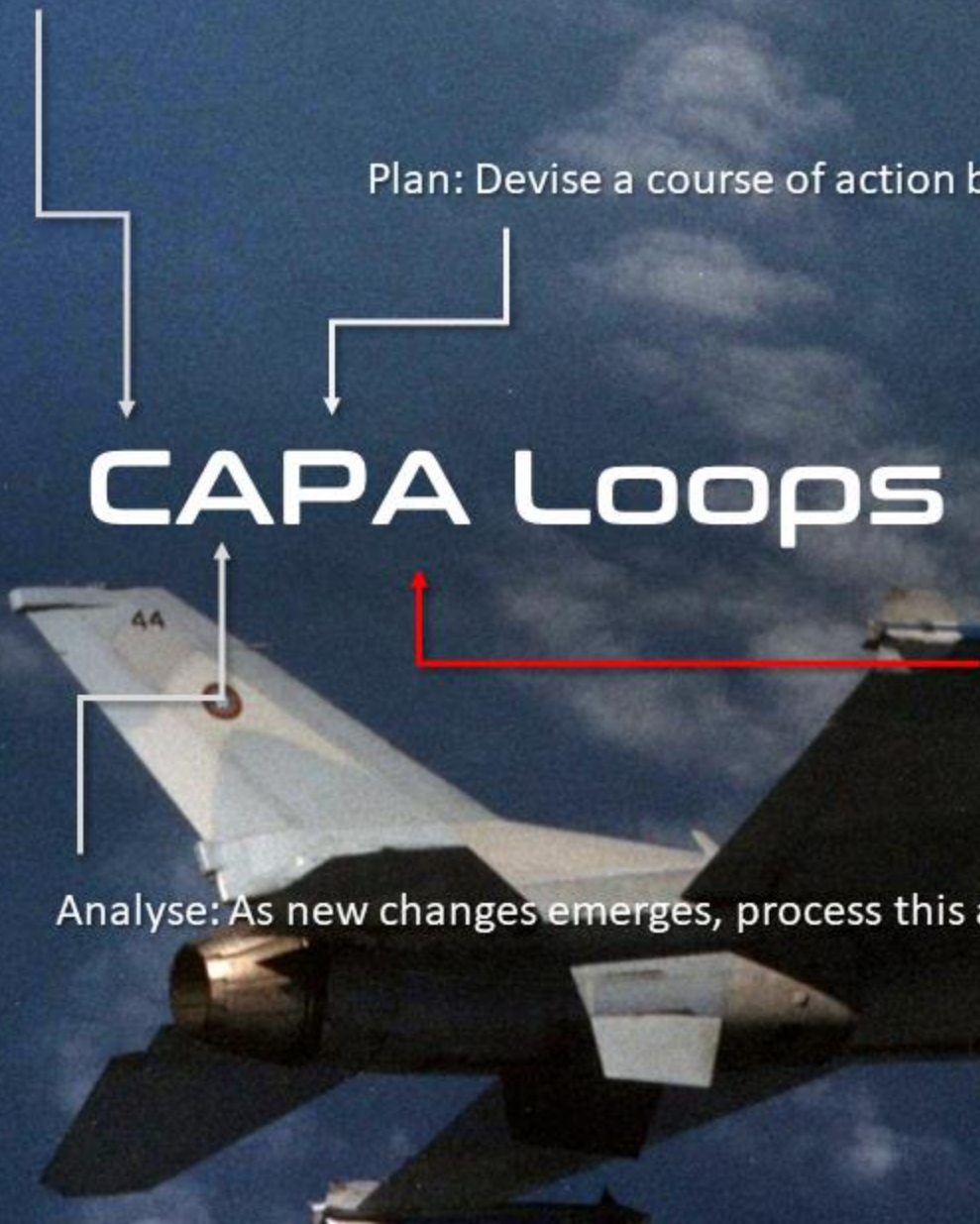
Capture: Discover changes to target attack surface or new CTI which enables attacks.

Plan: Devise a course of action based on information: exploit, pre-emptively alert and conclude risk

CAPA Loops

Act: Act before Threat Actors can complete the same loop!

Analyse: As new changes emerges, process this as opportunities to apply penetration testing efforts





Wait, isn't this a Red Team Exercise?

- It's in the word "exercise"
- Offensive SOC is not an exercise, it's a continuous operation
- Companies have a hard time training and retaining pentest talents
 - It is important to still have this competency "at hand".

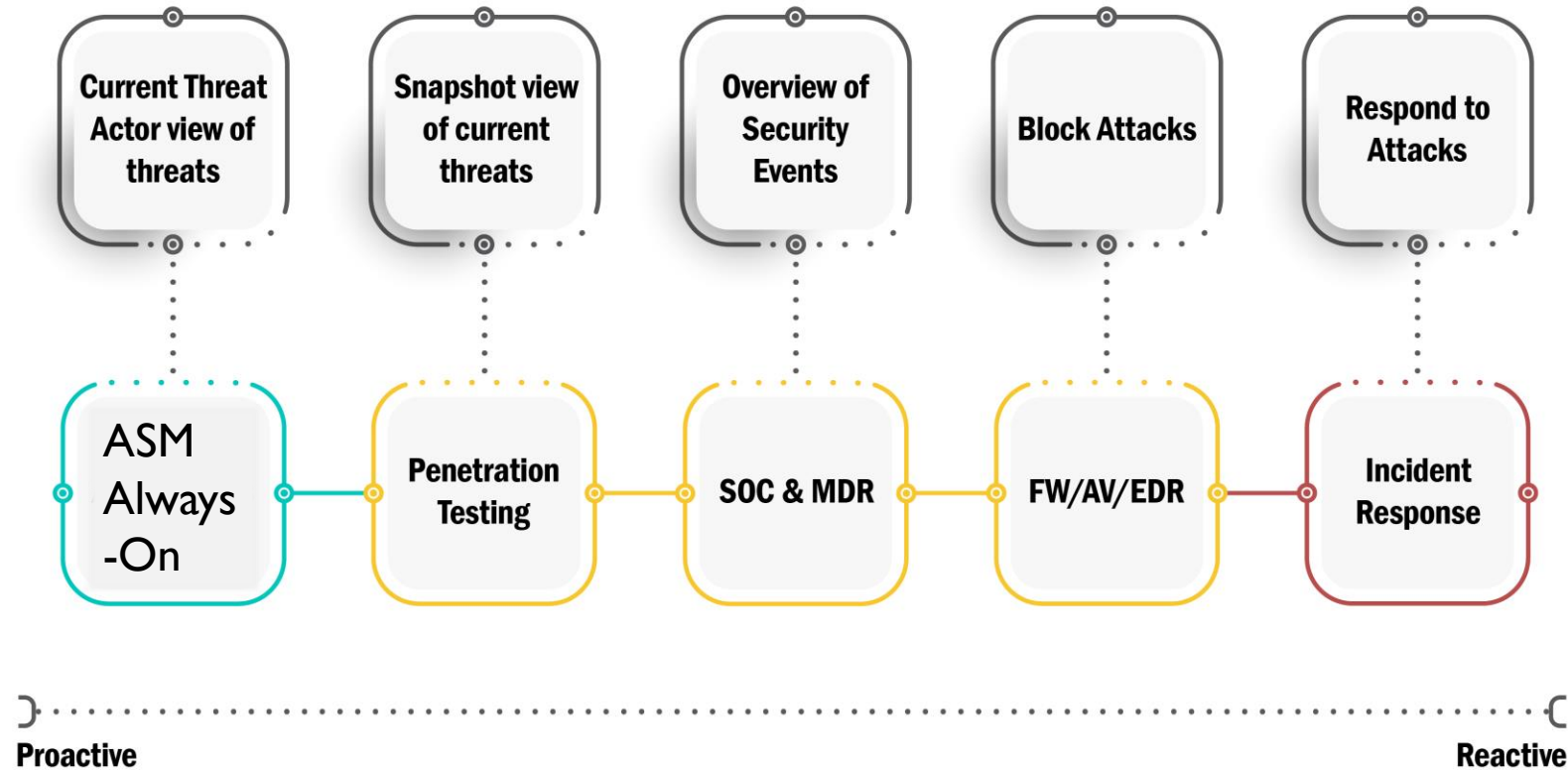
<u>Concern</u>	<u>Offensive SOC</u>	<u>Red Team Exercise</u>
Stealth	No	Yes
Physical	Not typically ¹	Yes
People In-Scope	Not typically ¹	Yes
Utilizes Stolen Credentials	Yes	Yes
Prioritization	Speed	Target value compromise
Blue Team Cooperation	Yes	No ²
Scope	Wide	Wide first, then narrow
Duration	Continuous	Exercise
Change Management ³	Prioritized	Often ignored as recon is done
Goal	Report and Remediate ASAP	Breach

1. It will always work. If not today, then tomorrow.
2. Most Red Teams will try to determine the effectiveness of the Blue Team, while O-SOC will report continuously with full transparency, typically via API's for Blue Team to pay attention to.
3. Change Management implying changes to customer, but also CTI, hacking techniques, CVE's and more.

Defend Forward



Proactive vs. Reactive



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)



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>