Offensive Security Operations

Penetration Testing of the Future

Chris Dale

- CHO, Principal and Founder at River Security
- Principal Instructor at SANS
- Co-Author – Cyber Deception, Attack Detection, Disruption and Active Defense

- Short summary:

I show how criminals break-in, and I help throw them back out…

CERTS

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

Exclusively in Offensive Security Space

- And a touch of Incident Response

- 20 employees
- Boot strapped
- 4 years in business
- 41+ public customer testimonials
- 8+ customer cases

Exclusively in Offensive Security Space

- And a touch of Incident Response

- 20 employees
- Boot strapped
- 4 years in business
- 41+ public customer testimonials
- 8+ customer cases

Team River Security @ Hacker Space 2024

WHY DO WE DO PENETRATION TESTING?

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

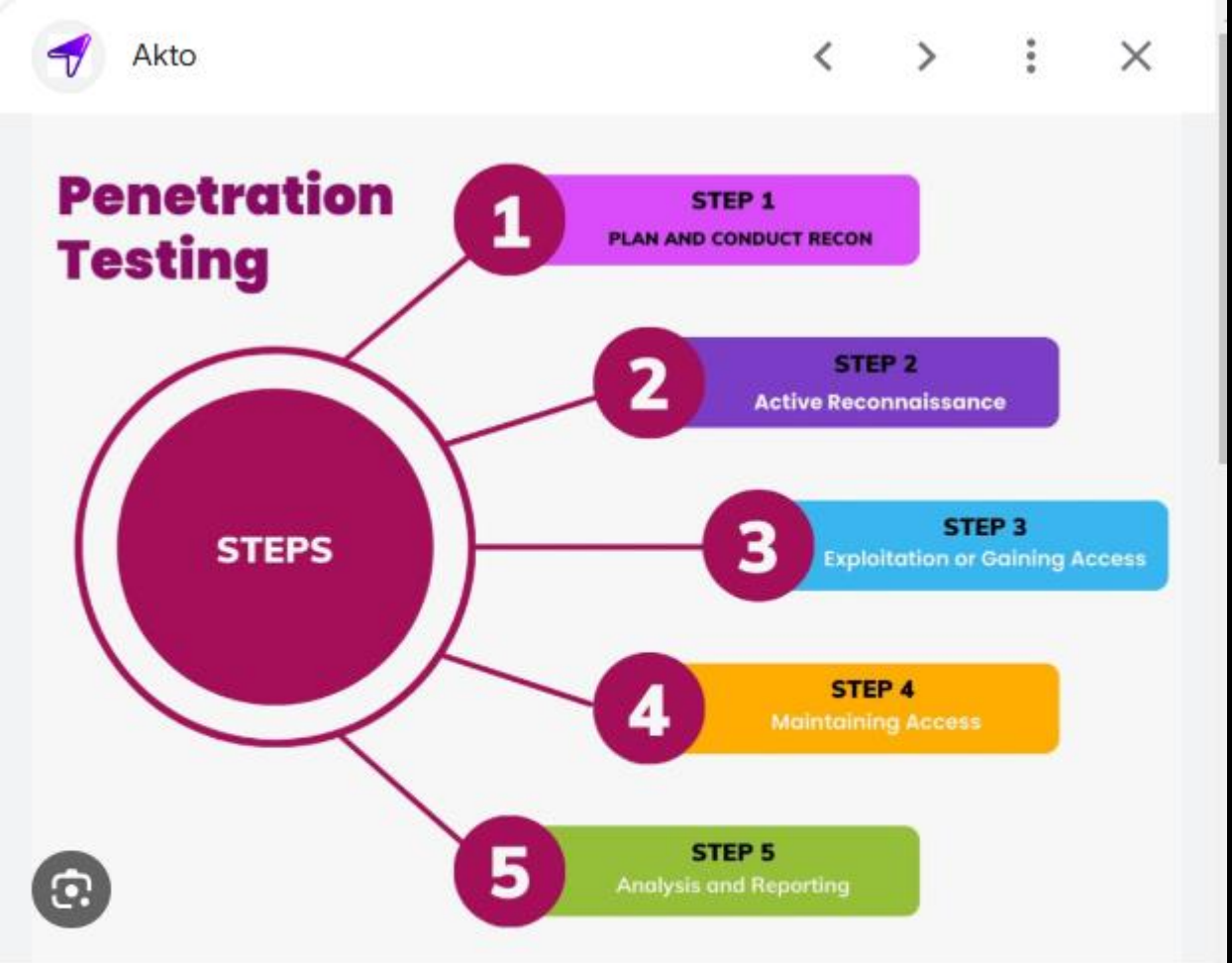
COMMON PROBLEMS WITH PENETRATION TESTING

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.

Do Attackers Care About Scope?



Penetration Testing | Pen Testing | Automated Penetration Testing - Devsecops

Visit ›

Sprinto

Top 5 Penetration Testing Methodol...

esting? Definition ...

Sprinto

Top 5 Penetration Testing Methodology to Follow in 2025

Visit ›

Images may be subject to copyright. **Learn More**

Share

Save

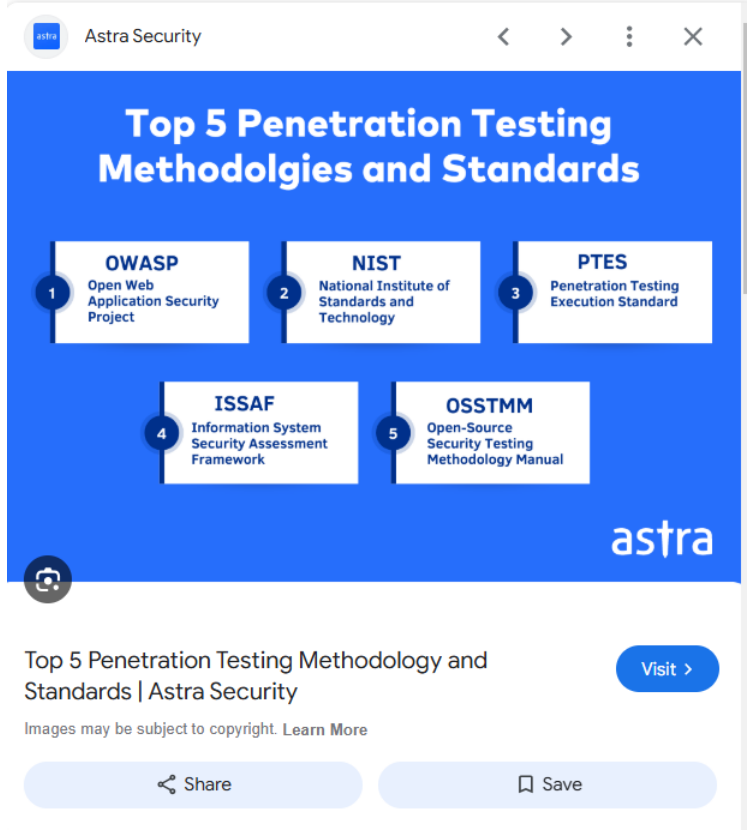
Penetration Testing Execution Standard (PTES)

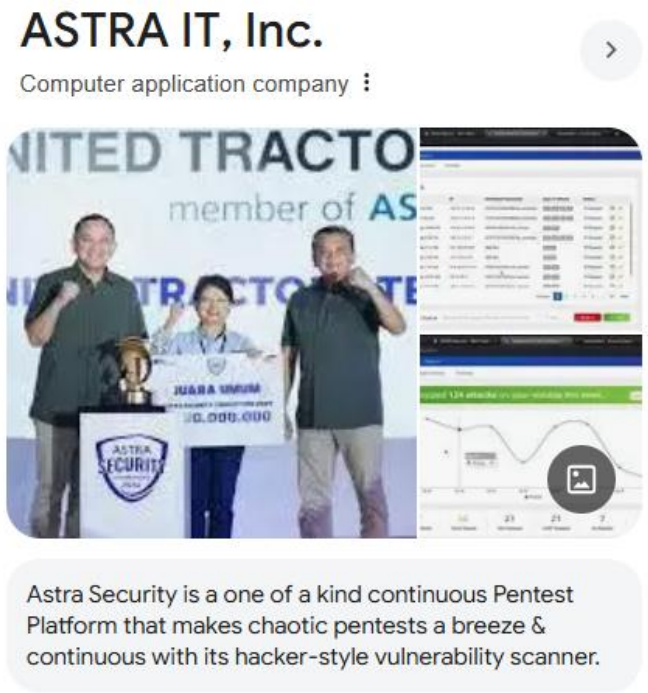
PTES, or the Penetration Testing Execution Standard, is a penetration testing framework tailored to serve as a standard for conducting penetration testing. It was developed by a group of security experts to offer a consistent and repeatable methodology for testing.

Different penetration testing methods can be implemented for different types of ng to secure system and network infrastructure. These include multiple o penetration testing, such as application penetration testing, web-based sting, static analysis, dynamic analysis, and social engineering tests, s to prevent hacker attacks and ensure infrastructure security.

ures of PTES include:

RIVER SECURITY





Find and fix every single security loophole with our hacker-style pentest.

- **Get the industry's deepest & broadest vulnerability coverage**
  Test for 9300+ vulnerabilities including industry standard OWASP & SANS tests.
- **Upgrade your DevOps to DevSecOps**
- **Ensure continuous ISO, SOC 2, GDPR or HIPAA Compliance**
- **Triage & address business-critical threats instantly**
- **Rest easy with the lowest false positives rate**

OSSTMM 3 – The Open Source Security Testing Methodology Manual

Version Information

The current version of the Open Source Security Testing Methodology Manual (OSSTMM) is 3.02. This version of the OSSTMM ends the 2.x series. All OSSTMM versions prior to 3.0 including 3.0 release candidates (RC versions) are now obsolete.

The original version was published on Monday, December 18, 2000. This current version is published on Tuesday, December 14, 2010.

what is the latest version os OSSTMM

The latest version of the Open Source Security Testing Methodology Manual (OSSTMM) is version 3.02, published on December 14, 2010. ISECOM This version marked a significant evolution from the 2.x series, introducing a unified methodology applicable across all channels: Human, Physical,

WSTG - Latest

Penetration Testing Methodologies

Summary

- OWASP Testing Guides
  - Web Security Testing Guide (WSTG)
  - Mobile Security Testing Guide (MSTG)
  - Firmware Security Testing Methodology
- Penetration Testing Execution Standard
- PCI Penetration Testing Guide
  - PCI DSS Penetration Testing Guidance
  - PCI DSS Penetration Testing Requirements
- Penetration Testing Framework
- Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual
- References

OWASP Testing Guides

In terms of technical security testing execution, the OWASP testing guides are highly recommended. Depending on the types of the applications, the testing guides are listed below for the web/cloud services, Mobile app (Android/iOS), or IoT firmware

WSTG Contents

Main page
PTES Technical Guideline
In the Media
FAQ

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Main Page

High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "road tested" for over a year through the industry. A v2.0 is in the works soon, and will provide more granular work in terms of "levels" - as in intensity levels at which each of the elements of a penetration test can be performed at. As no pentest is like another, and testing will range from the more mundane web application or network test, to a full-on red team engagement, said levels will enable an organization to define how much sophistication they expect their adversary to exhibit, and enable the tester to step up the intensity on those areas where the organization needs them the most. Some of the initial work on "levels" can be seen in the intelligence gathering section.

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we have also created a technical guide to accompany the standard itself. The technical gude can be reached via the link below:

- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

SQL Injection (SQLi)

According to OWASP (https://www.owasp.org/index.php/SQL_Injection) SQL Injection, or as it is more commonly known SQLi, consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases is commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

SQL (Structured Query Language) is an interpretted programming language for interfacing with a database. It is sometimes also lazily used to refer to the database management system. Applications utilize a database to store/retrieve and process informatio database is usually a relational database, where data is stored in one more tables, each table has values in one or more columns (data types/attributes) and rows (element/tuple). There are several implementations of SQL and each has their own commands few common commands are: select - retrieve data union - combine results of two or more selects insert - add new data update - modify existing data delete - delete data

What is injection? Simply stated, SQL injection exploits a vulnerability that allows data sent to an application to be interpreted and run as SQL commands.

According to OWASP (https://www.owasp.org/index.php/SQL_Injection) SQL Injection, also known as SQLi, consists of insertion or "injection" of a SQL query via the input data from the client to the application.

A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands. SQL injection discovered in the Vulnerability Analysis phase (and maybe hinted at in the intelligence gathering phase) of the engagement.

One possible way to test for sql injection is to enter a ' into input fields then compare the application response to a well formed request. If the web application is vulnerable to SQLi, a ' may return different results when the SQL statement attempts to execute. message returned, different results, web page a different size, are different HTTP codes returned. Don't forget to look at the source, not just what is displayed in the browser. Depending on the reaction, it may be necessary to use other tests for injection, for or) or '+"=' or %27%20or%201=1. It may also be necessary to encode the characters to bypass filters. If the access to the source code of the application is available, review for any variables where input can be manipulated as part of the application usage. this will be readily apparent, for instance php $sql = "SELECT * from [table] WHERE tuple = '$_GET("input")']"; c# $sql = "SELECT * from [table] WHERE tuple = '" + request.getParameter("input") + "'";

Several tools are available for the identification and exploitation of SQLi

Several tools are available for the identification and exploitation of SQLi. SQLi Tools

- Havij (http://itsecteam.com/en/projects/project1.htm)
- SQLmap (http://sqlmap.sourceforge.net)
- The Mole (http://sourceforge.net/projects/themole)
- Pangolin (http://nosec.org/en/productservice/pangolin)

XSS

<Contribution Needed>

CSRF

<Contribution Needed>

Ad-Hoc Networks

<Contribution Needed>

- Information Leakage

WSTG - Latest

PTES Technical Guidelines

PCI Penetration Testing Guide

Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3 defines the penetration testing. PCI also defines Penetration Testing Guidance.

PCI DSS Penetration Testing Guidance

The PCI DSS Penetration testing guideline provides guidance on the following:

- Penetration Testing Components
- Qualifications of a Penetration Tester
- Penetration Testing Methodologies
- Penetration Testing Reporting Guidelines

PCI DSS Penetration Testing Requirements

The PCI DSS requirement refer to Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3

- Based on industry-accepted approaches
- Coverage for CDE and critical systems
- Includes external and internal testing
- Test to validate scope reduction
- Application-layer testing
- Network-layer tests for network and OS

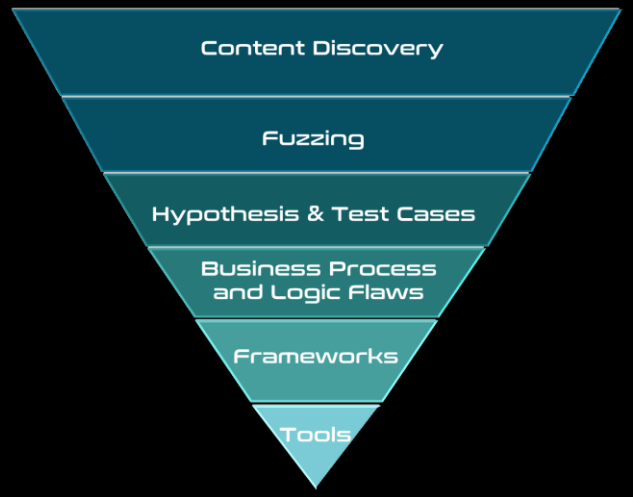
PCI DSS Penetration Test Guidance

Penetration Testing Framework

The Penetration Testing Framework (PTF) provides comprehensive hands-on penetration testing guide. It also lists usages of the security testing tools in each testing category. The major area of penetration testing includes:

- Network Footprinting (Reconnaissance)
- Discovery & Probing
- Enumeration
- Password cracking
- Vulnerability Assessment
- AS/400 Auditing

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



THE KING IS DEAD

LONG LIVE THE KING

https://riversecurity.eu/penetration-testing-methodology/

Defend Forward

Digital Footprint Assessment

RIVER SECURITY

Map Out Attack Surface – Get Hackers Opinions

- Immediate **value**
- 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
- Know what you have, before procuring pentest

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.

RIVER SECURITY

Navelgazing: NavelGazing 20c9a2ce-daa6-4f00-935b-6a8e5238e381

Available tags

Add Assets | Reports | Issues | Observables | Entities | Observables | Domains | Applications | IP Addresses | Users | More

ip-address | application | domain | company | subdomain

http://ab57f10b-24a9-4f2b-8d99-7ace97852104.rivsec.eu:80/
ab57f10b-24a9-4f2b-8d99-7ace97852104.rivsec.eu
af.rivsec.no
178.62.222.97
_wildcard.wa.rivsec.eu
_wildcard.aws.rivsec.eu
_wildcard.bs.rivsec.eu
rscb.no
tcp://rscb.no:5101/
tcp://rscb.no:1723/
tcp://rscb.no:5631/
tcp://rscb.no:1027/
tcp://rscb.no:5900/
tcp://rscb.no:110/
tcp://rscb.no:1110/
tcp://rscb.no:8000/
http://_wildcard.wa.rivsec.eu:80/
https://_wildcard.wa.rivsec.eu:443/
https://_wildcard.aws.rivsec.eu:443/
http://_wildcard.aws.rivsec.eu:80/
https://_wildcard.bs.rivsec.eu:443/
http://_wildcard.bs.rivsec.eu:80/
172.67.194.232
2606:4700:3033::6815:c8e
104.21.12.142
2606:4700:3030::ac43:c2e8
gtm.riversecurity.eu
http://gtm.riversecurity.eu:80/
https://gtm.riversecurity.eu:443/
www.riversecurity.eu
ctfd.rsxc.no
http://rsxc.no:9010/
http://www.riversecurity.eu:80/
http://rsxc.no:9001/
http://rsxc.no:9009/
https://www.riversecurity.eu:443/
rsxc.no
autodiscover.riversecurity.eu
tcp://rsxc.no:5060/
http://rsxc.no:9006/
ssl.rsxc.no
http://rsxc.no:9002/
http://rsxc.no:80/
https://autodiscover.riversecurity.eu:8443/
https://rsxc.no:443/
http://autodiscover.riversecurity.eu:80/
https://autodiscover.riversecurity.eu:443/
river security as
k0ngsbergams.com
kongsbergdigital.com
easeee.cloud
mt-link.ongsbergams.com
fe80::1
home.appexivo.com
kinderegg.appexivo.com
appexivo.com
1.1.1.1
10.1.1.80
google.appexivo.com
2a00:1450:40
rivsec.no
riversec.eu
http://www.riversec.eu:80/
www.riversec.eu
faktivo.com
2a01:5b40:0:bc03::1
http://faktivo.com:80/
www.rivsec.no
riversec.no
www.riversec.no
www.faktivo.com
http://www.faktivo.com:80/
167.71.76.111
pt.riversec.no
riversecurity.no
http://riversecurity.no:80/
https://riversecurity.no:443/
2603:1027:1:28::19
2603:1027:1:28::14
2603:1027:1:28::17
40.126.53.5
2603:1027:1:28::2
40.126.53.1
enterpriseregistration.riversecurity.no
40.126.53.0
40.126.53.3
40.126.53.4
2603:1027:1:28::3
2603:1027:1:28::15

Dashboard

Reports

Issues

Entities

Staging

chris@riverse

Log out

Report a prob

Home > Issues

Search...

Reported issues

All Categories

Sort by: Date Cr

Go Back

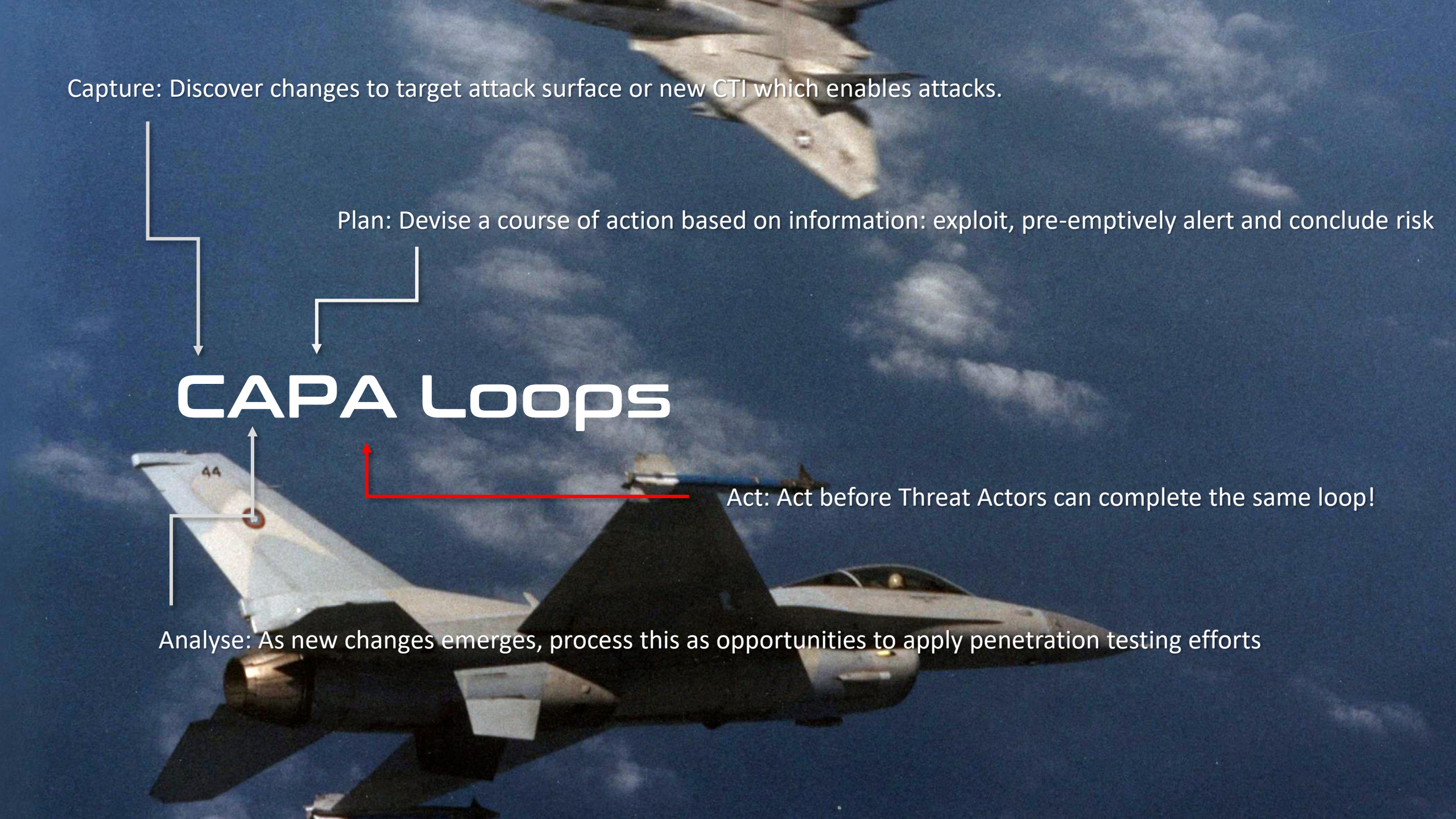
Download PDF

Not secure | [redacted] iew

AXIS COMMUNICATIONS

AXIS P5514-E PTZ Dome Network Camera

[redacted]


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

RIVER SECURITY

Enter Attack Surface Management

Digital Footprint

Automation + Review

Attack Surface Management

PENTEST METHODOLOGY

Reconnaissance

Discovery & Scanning

Exploitation & Verification

RIVER SECURITY

REDEFINING PENETERATION TESTING WITH OFFENSIVE SOC

Attack Surface Management

Test All Changes

PENTEST METHODOLOGY

Reconnaissance

Discovery & Scanning

Exploitation & Verification

11:46 / 34:55

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers

USENIX Enigma Conference
7.45K subscribers

Subscribe

1.7K | Share | Download | Clip | Save

All | For you

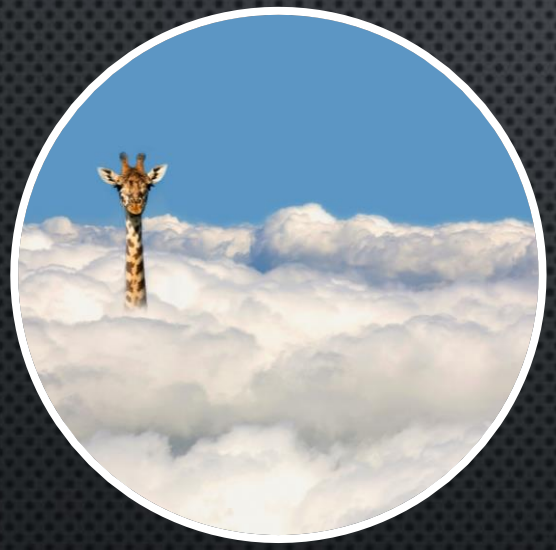
USENIX Enigma 2016 - Building

AGILE

PENETRATION TESTING

OFFENSIVE SOC OPERATIONS

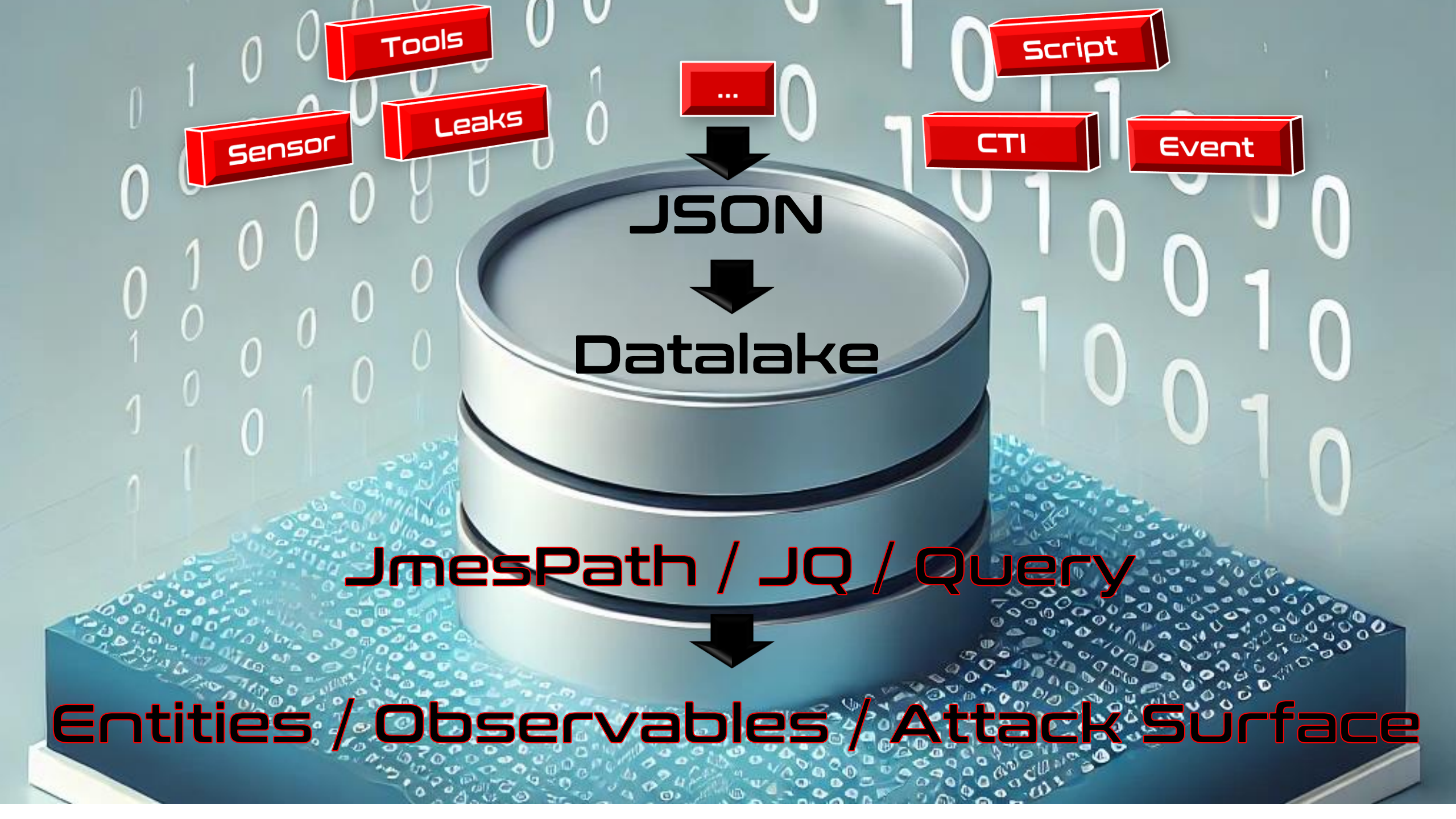
NEW ATTACK SURFACE (DELTA)



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

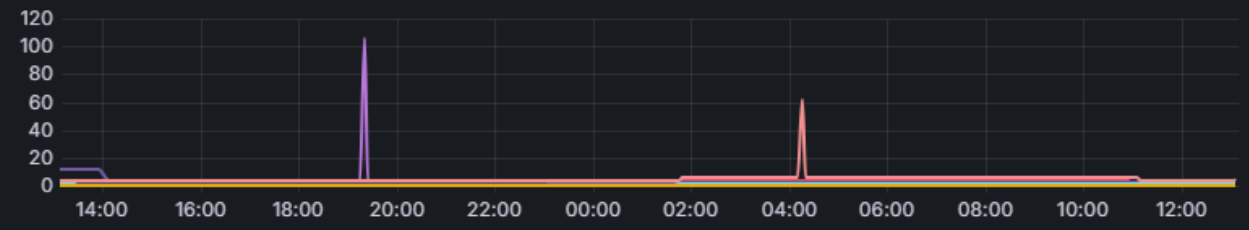
EXISTING ATTACK SURFACE

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

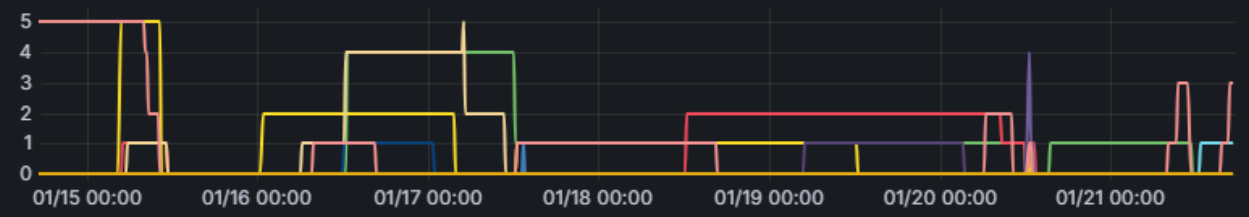

Tools
Sensor
Leaks
...
Script
CTI
Event
JSON
Datalake
JmesPath / JQ / Query
Entities / Observables / Attack Surface

RIVER

Unprocessed Applications



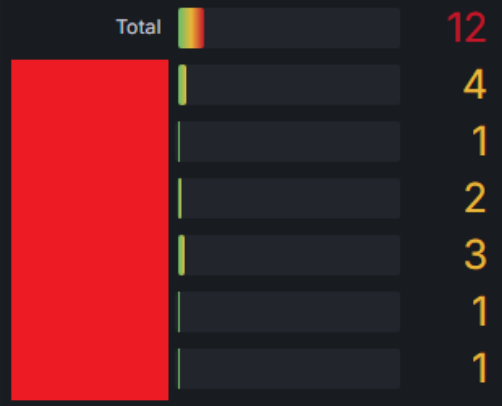
Delta Applications



Unverified Observables

Backlog Applications

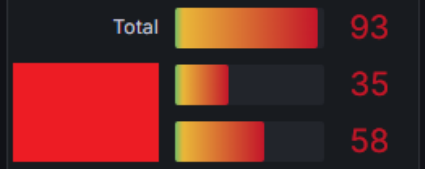
Unprocessed applications



Unprocessed Security Obsevables

Delta Application

Backlog



Escalated applications

ALL DONE

STORED - in scope

https://riversecurity.eu:443/

river security as > riversecurity.eu > https://riversecurity.eu:443/

Domains (1)

http_response_code	200
http_title	River Security – We Fight Cyber Crime
http_server_header	cloudflare
screenshot	0000ffffff0000ff
transport	tcp
ssl_info	
ssl_info.version	TLSv1.3
ssl_info.cert_browser_limit_exceeded	
ssl_info.expired	
ssl_info.mismatch	
ssl_info.CN	sni.cloudflaressl.com

Tags

login × service-wordpress × +

Attractiveness

0 1 2 3 4 5 6 7 8 9 10

Internal Status

Edit

View graph

Choose file

Customer Status

pentester 07.10.2022, 20:45

Edit

RIVER

RIVER SECURITY

GENERAL

- Dashboard
- Reports
- Issues
- Compliance
- Diagram Beta

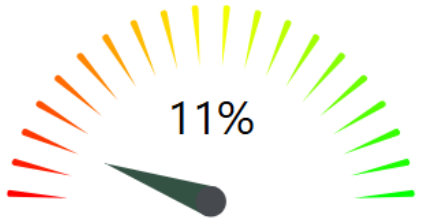
OVERVIEWS

- Certificates
- Vulnerabilities
- Authentication
- Technology
- Credentials Beta
- Web Practices Beta
- Mail Security Beta
- DNS Health

Home > WebBestPractices

Web Best Practices

The goal of these dashboards is to provide users with an overview of missing web security best practices, security hygiene, and other relevant aspects related to web applications.



HTTP Server Headers

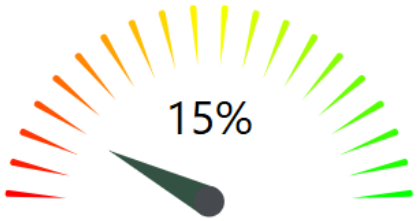
The percentage of servers that does not expose their HTTP server header is displayed in the gauge. Not exposing server headers is considered best practice because it makes it harder for attackers to profile the technology running on the server. Exposing the HTTP server header is a security risk as it provides attackers with insights into the server software, potentially helping them exploit known vulnerabilities.

5 42

HTTP Strict Transport Security (HSTS)

Strict Transport Security instructs the browser to only communicate with the server using secure HTTPS connections, even if the user attempts to access the site via HTTP. This policy is enforced through a special HTTP header (Strict-Transport-Security) that specifies how long the browser should remember to only use HTTPS for that site. The gauge shows the percentage HTTP/HTTPS servers which have this security control turned on.

18 29



Referrer Policy

Referrer Policy prevents leaking sensitive information in URLs when navigating between different sites, e.g. a link is clicked, preserving the privacy of users. It also reduces the risk of referrer header leaking information that can be exploited in attacks. The gauge shows percentage of sites with a clearly defined referrer policy.

7 40

Example

ATLASSIAN
Confluence

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

Example

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)
```

INFORMATION TECHNOLOGY

IS A MOVING TARGET

1. KNOW YOURSELF

The task once dubbed asset inventory remained neglected

1. KNOW YOURSELF

The task once dubbed asset inventory remained neglected

OFFENSIVE SOC

2. KNOW ATTACKERS

Pentesting was deemed annual or solely for compliance by the industry

OFFENSIVE SOC

3. ADVANCED PERSISTENT THREAT

Penetration testing has lacked agility and sustained impact

OFFENSIVE SOC

RED VERSUS BLUE

IT IS TIME WE "STOP FIGHTING" AND FORM PURPLE TEAM

RIVER SECURITY

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

Twitter – https://twitter.com/ChrisADale

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

Fighting Cyber Crime – https://riversecurity.eu