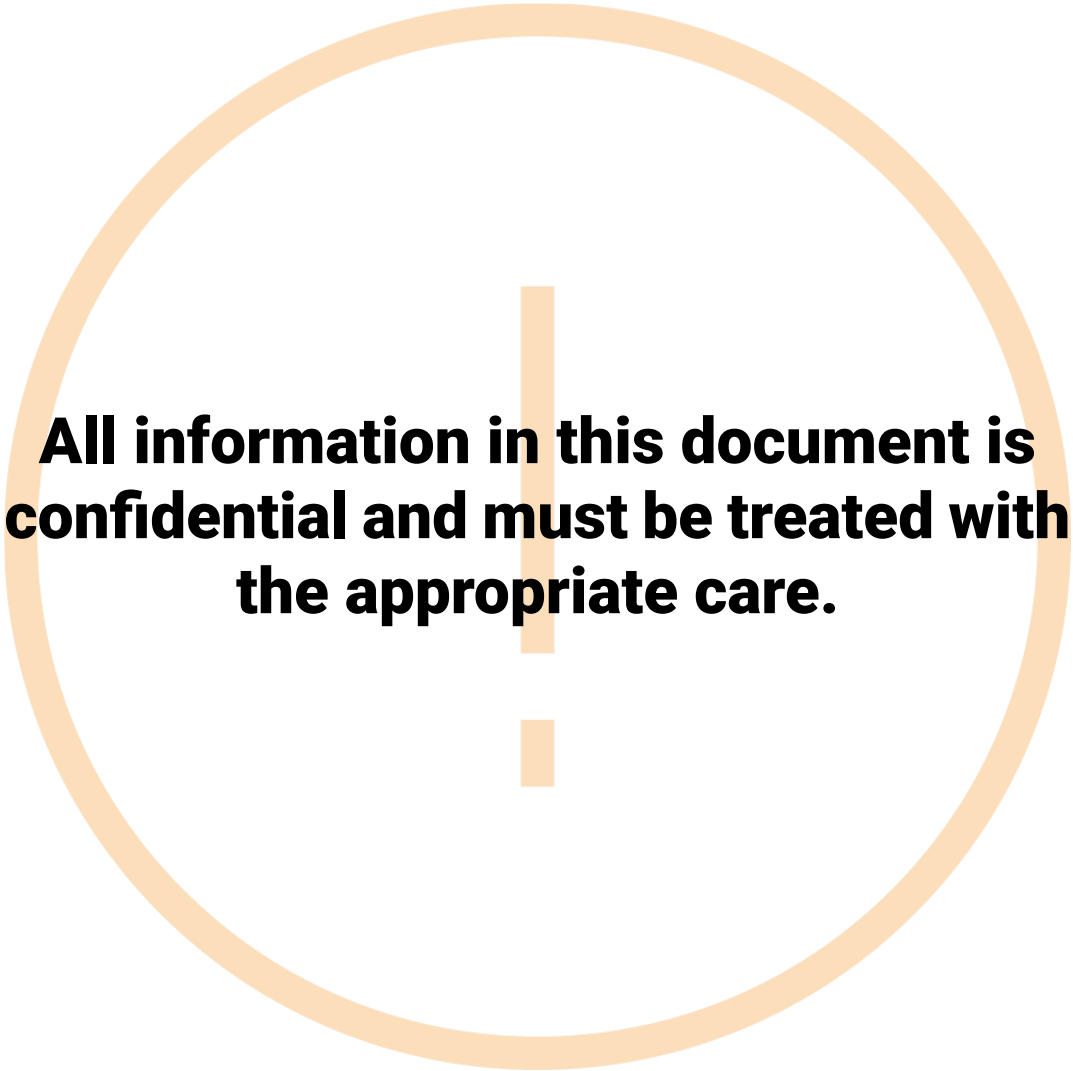
Vulnerability Report

Confidential to

THE CUSTOMER

Insight Demo - CM

Table of Contents



All information in this document is confidential and must be treated with the appropriate care.

Introduction

Dear Remy Adrian,

Silversky Insight has been running on your scan surface since 31st May 2023, 08:04 AM. Your current cyber-security risk level is**: 4.82% critical.**

Our Customer Vulnerability Report (CVR) provides you with crucial perspectives on cyber security threats that Insight Demo - CM is currently facing. The CVR is built on real-world data from 5 assets, 3 webapps and covers 1743 distinct CVEs in 2640 total CVEs, out of which 416 are weaponized (have public exploits available that can be used by attackers). Your scan surface is covering 4 internal assets , 2 external assets and 1 agents which have been scanned starting 31st May 2023, 08:04 AM until today.

The CVR Executive Summary will be covering the key metrics of your organization's cyber security risk presented from a high-level perspective which should be easy to understand by executives.

The Security Insights Analytics section of this report drills down into the cyber security field results of our analysis. You can thus identify your most critical and urgent vulnerabilities and see behind our interpretation straight to the root cause.

Technical Reports, Scan Surface and Methodology are designed for your security professionals and accelerating remediation efforts. These sections are intended to be shared with your blue team and your auditors.

The "threat landscape" is a moving, shifting form that will look different to different organizations — it all depends on where you are standing. Some people may be staring at a wide open grassland where the landscape is understood and the threats are easy to identify (though no less deadly), and others may be facing a dense jungle of hidden threats.

If you need any support in accelerating your remediation activities, please feel free to engage with Silversky's representative, **Silversky Contact**, at supportdb@silversky.com.

Note: The report contains information only on assets which have findings. Secure assets will not be taken into account when generating this report.

Data collected since
31st May 2023, 08:04 AM

Latest data refresh
13th July 2023, 12:40 PM

Scanned assets
5

Agents
1

Assets with findings
5

Distinct CVEs
1743

Total CVEs
2640

Weaponized CVEs
416

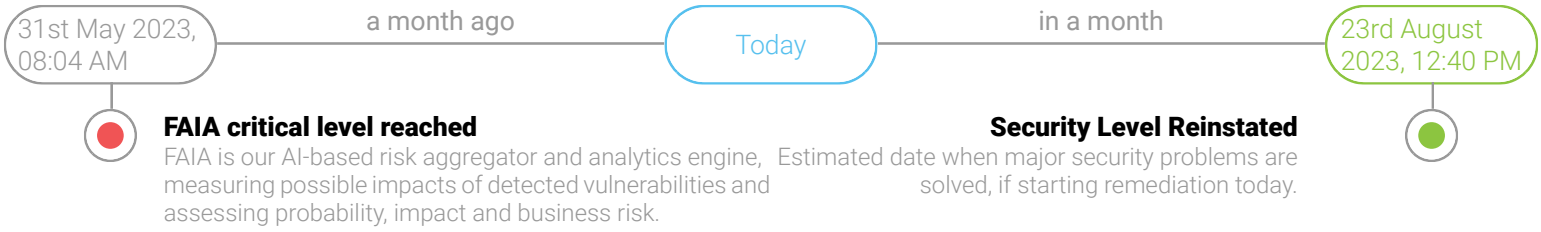
Generated by
Silversky

Executive Summary

We have selected the most important highlights regarding your organization's security. The reasoning and methodology behind these numbers are explained further in this report.

Critical Risk Exposure Timeline

Timeline of your critical risk exposure status

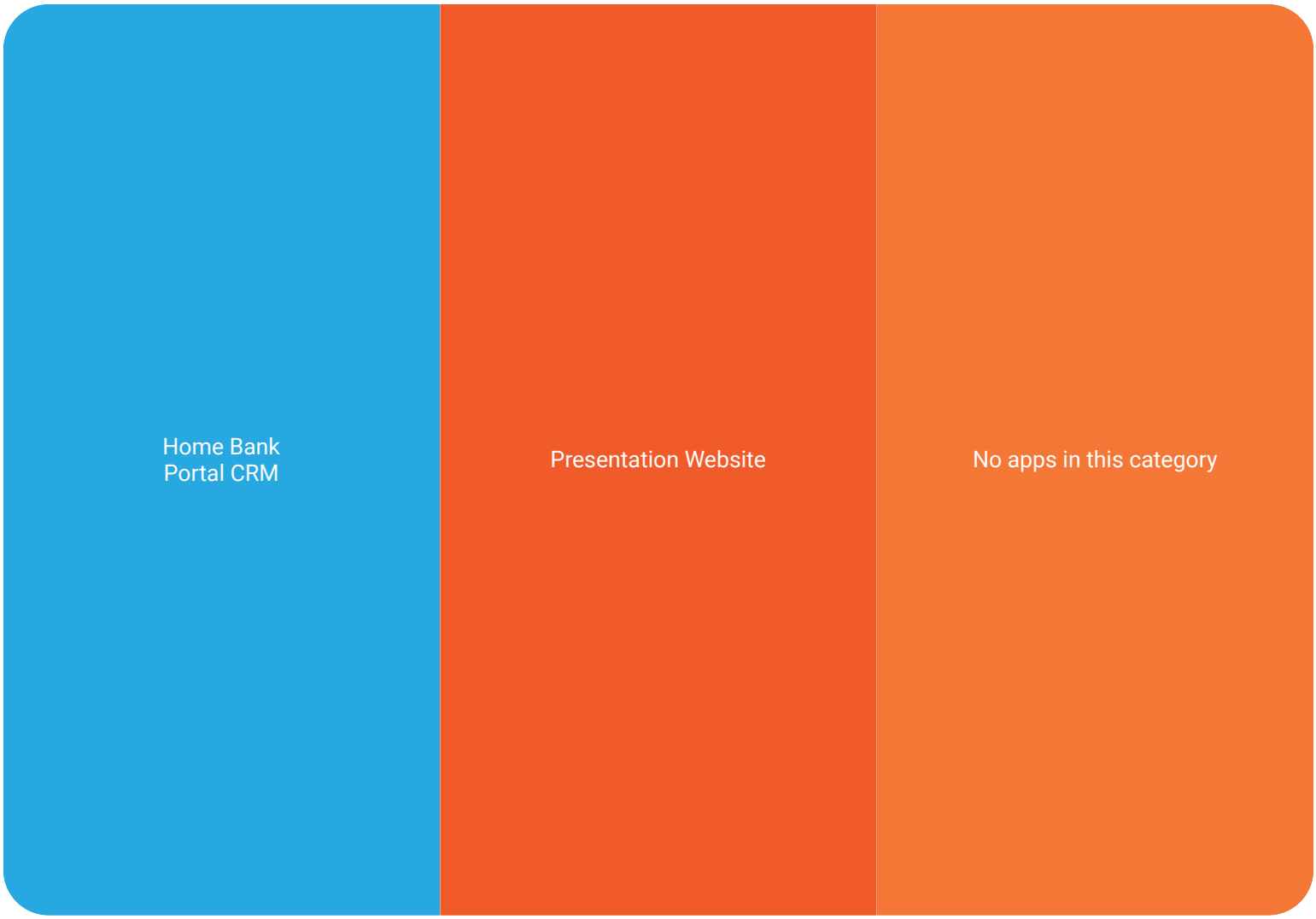


FAIA critical level reached
FAIA is our AI-based risk aggregator and analytics engine, measuring possible impacts of detected vulnerabilities and assessing probability, impact and business risk.

Security Level Reinstated
Estimated date when major security problems are solved, if starting remediation today.

Top risky web applications

An overview of your most important and vulnerable applications

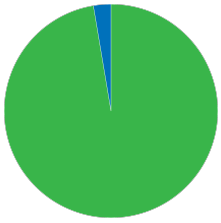


Internal and external risk

It is important to have visibility regarding all existing vulnerabilities, and to see if they are externally weaponized or just internal.

Key takeaways
Highlights of your exposure area risk level

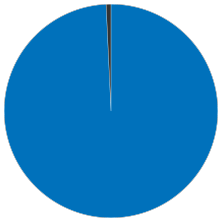
- 24 internal vulnerable applications
- 6 external vulnerable applications
- 5 unknown applications



- 97.36% Internal
- 2.64% External

Internal applications represent applications running in your company's network, usually separated from the internet.

External applications are those that are accessible over the internet, such as web servers and e-mail servers.



- 0.73% Unknown
- 99.27% Complete

Unknown applications represent a blind spot in your security analysis.

Get more information on unknown applications by installing Footprint Agent on the devices running them.

Regulation Checks

Checks against NIST CSF 1.1 - Protection - Data Security compliance issues

We have found possible compliance issues

We have identified vulnerabilities that might put you at legal risk in relation to NIST CSF 1.1 - Protection - Data Security

Caused by the following items:

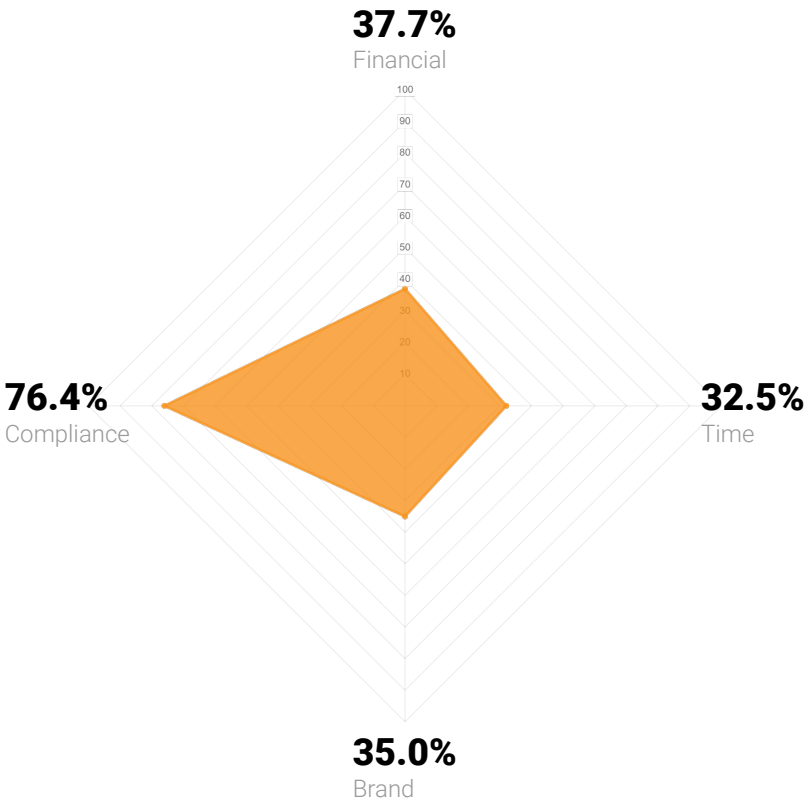
- Presentation Website
- Organizational Footprint
- File Sharing

Vulnerabilities that triggered compliance issues:

- CVE-2015-4599
- CVE-2015-4599
- CVE-2019-0232

Organization Exposure

Organization's financial, time, compliance and brand exposure



Top 5 risk scenarios

We have analyzed the top 5 applications with problems that will reduce your exposure the most

- Presentation Website
- Organizational Footprint
- File Sharing
- SAP Business Objects BI
- Agent Based Footprint

Fixing these applications will reduce your FAIA indicators to the following values:

37.7%	11.6%	7.1%	32.5%
Financial	Brand	Compliance	Time

Top impacts per exposure

We have selected the top applications that affect you in each category

File Sharing	**37.7%**
SAP Business Objects BI	**37.7%**
Agent Based Footprint	**37.7%**
Organizational Footprint	**37.7%**
Presentation Website	**35.0%**

File Sharing	**32.5%**
SAP Business Objects BI	**32.5%**
Agent Based Footprint	**32.5%**
Organizational Footprint	**32.5%**
Presentation Website	**22.5%**

Presentation Website	**76.4%**
Organizational Footprint	**76.4%**
File Sharing	**7.1%**
SAP Business Objects BI	**7.1%**
Agent Based Footprint	**7.1%**

Presentation Website	**35.0%**
Organizational Footprint	**35.0%**
File Sharing	**11.6%**
SAP Business Objects BI	**11.6%**
Agent Based Footprint	**11.6%**

Remediation Tracking

This section presents an overview on your organization's CVE management lifecycle, current status and progress across its entire scan surface since you started using Footprint.

293 Fixes Confirmed
Average score: 5.74

0 Fixes Not Confirmed
Fixed CVEs waiting for confirmation from the scanner service.

0 Fixes Pending Confirmation
After marking a CVE as fixed, Footprint needs to confirm it before not taking it into account.

0 False Positives
False positives are CVEs marked by the user as wrongly identified by Footprint.

0 Added to Review
The review is a to-do list of CVEs that are in the process of fixing.

724 Active
Average score: 5.98

0 Accepted Risk
Accepted risk CVEs are ignored based on a motivation that the user provided.

Security Insights Analytics

A more detailed look into the findings affecting your organization.

Top vulnerable devices

hermes.codacloud.net
Findings: 3 Low 65 Medium 131 High 82 Critical

AD-PC2
Findings: 9 Low 287 Medium 401 High 30 Critical

hefaistos.codacloud.net
Findings: 2 Low 56 Medium 24 High 13 Critical

ad-dc
Findings: 2 Low 186 Medium 559 High 32 Critical

TOMCATPOC
Findings: 2 Low 195 Medium 536 High 25 Critical

Top vulnerable applications

php
Max. CVSS Score: 10
Running on 35.231.129.40:8080

Mozilla Firefox (x64 en-US)
Max. CVSS Score: 9.3
Running on 192.168.12.15

Adobe Acrobat Reader DC MUI
Max. CVSS Score: 9.3
Running on 192.168.12.15

WordPress
Max. CVSS Score: 7.5
Running on 34.148.182.155:80

Apache httpd
Max. CVSS Score: 7.8
Running on 35.231.129.40:8080

Findings Insights

50 Weaponized Findings

10 Top Findings

20 Most Common Findings

Business Report

Here you can see an overview on each business context configured

Home Bank

37.50% **Critical**
Critical applications that require immediate attention

0.00% **Vulnerable**
Vulnerable application that do not pose an immediate risk

25.00% **Invisible**
Applications on which Footprint could not gather complete information

37.50% **Secure**
Applications on which Footprint did not find any notable issues

Business Impact: 50% Applications: 8

Uptime: 100% Created by: Footprint

Presentation Website

44.45% **Critical**
Critical applications that require immediate attention

11.11% **Vulnerable**
Vulnerable application that do not pose an immediate risk

11.11% **Invisible**
Applications on which Footprint could not gather complete information

33.33% **Secure**
Applications on which Footprint did not find any notable issues

Business Impact: 50% Applications: 9

Uptime: 99.565% Created by: Footprint

Portal CRM

14.28% **Critical**
Critical applications that require immediate attention

0.00% **Vulnerable**
Vulnerable application that do not pose an immediate risk

42.86% **Invisible**
Applications on which Footprint could not gather complete information

42.86% **Secure**
Applications on which Footprint did not find any notable issues

Business Impact: 50% Applications: 7

Uptime: 100% Created by: Footprint

File Sharing

3.48% **Critical**
Critical applications that require immediate attention

0.15% **Vulnerable**
Vulnerable application that do not pose an immediate risk

0.00% **Invisible**
Applications on which Footprint could not gather complete information

96.37% **Secure**
Applications on which Footprint did not find any notable issues

Business Impact: 50% Applications: 662

Uptime: 100% Created by: Footprint

SAP Business Objects BI

5.15%	**Critical** Critical applications that require immediate attention
0.00%	**Vulnerable** Vulnerable application that do not pose an immediate risk
0.00%	**Invisible** Applications on which Footprint could not gather complete information
94.85%	**Secure** Applications on which Footprint did not find any notable issues

Business Impact: 50%
Applications: 135
Uptime: 100%
Created by: Footprint

Agent Based Footprint

3.91%	**Critical** Critical applications that require immediate attention
0.15%	**Vulnerable** Vulnerable application that do not pose an immediate risk
0.00%	**Invisible** Applications on which Footprint could not gather complete information
95.94%	**Secure** Applications on which Footprint did not find any notable issues

Business Impact: 50%
Applications: 662
Uptime: 100%
Created by: Footprint

Organizational Footprint

4.82%	**Critical** Critical applications that require immediate attention
0.29%	**Vulnerable** Vulnerable application that do not pose an immediate risk
0.73%	**Invisible** Applications on which Footprint could not gather complete information
94.16%	**Secure** Applications on which Footprint did not find any notable issues

Business Impact: 50%
Applications: 680
Uptime: 99.891%
Created by: Footprint

Perimeter Definition

Top vulnerable Agent-based and Agentless devices.

Top most vulnerable Agent-based scanned devices (3)

Hostname	IP Address	Discovered on	Applications Count	Low Findings.	Medium Findings.	High Findings.	Critical Findings.
ad-dc	192.168.12.4	31.05.2023	233	2	186	559	32
AD-PC2	192.168.12.15	31.05.2023	296	9	287	401	30
TOMCATPOC	192.168.12.6	31.05.2023	135	2	195	536	25
Total			664	13	668	1496	87

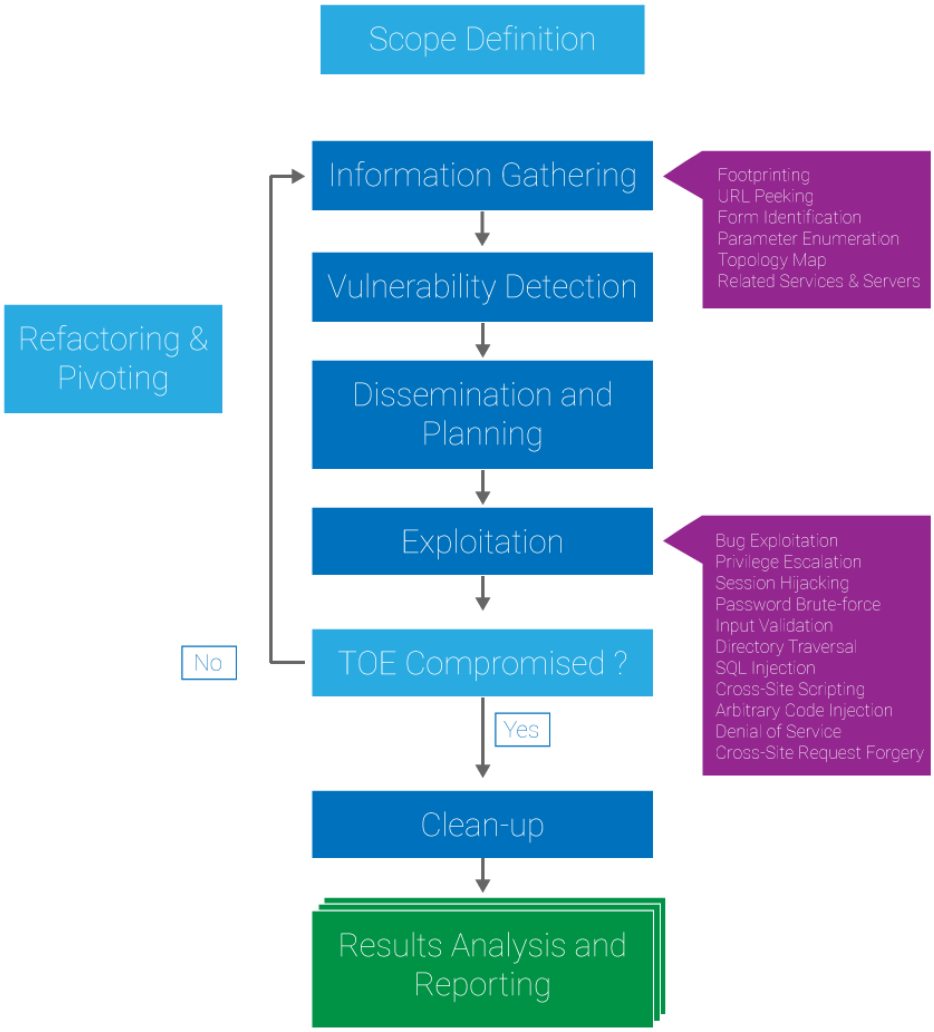
Top most vulnerable Agentless scanned devices (2)

Hostname	IP Address	Discovered on	Applications Count	Low Findings.	Medium Findings.	High Findings.	Critical Findings.
hermes.codacloud.net	35.231.129.40	31.05.2023	11	3	65	131	82
hefaistos.coda-cloud.net	34.148.182.155	31.05.2023	7	2	56	24	13
Total			18	5	121	155	95

Methodology

Detailed explanation of the methods and heuristics used to generate the data this report is based on.

The assessment methodology employed throughout the course of the security assessment can summarized in the following diagram:



Scope Definition:The initial stage is focused on defining the target of evaluation and its dependencies as well as establishing the success factors that will confirm the evaluation of a particular system's security posture.

Information Gathering:The evaluation method is based on a thorough analysis of the underlining system components that entail but are not limited to the following elements:

System Profiling: collecting data that a potential attacker might use to compromise the system that might include: DNS data, company public business data, registered public IP addresses, key business owners gathered using social networks, search engine hacking, domain registrars and internal records

System Mapping: obtaining running service ports by using automated scanners and obtaining an accurate depiction of external web resources using spidering tools

Vulnerability Detection:This stage is focused on identifying the vulnerabilities associated with the target of evaluation based on the system map created in the preceding stage. This faze employs both automated testing using enterprise grade and open source applications as well as manual analysis for eliminating false positives.

Dissemination and Planning:Based on the information collected in the preceding phases: active systems, open ports, services, web resources and operating systems along with the attack surfaces exposed by their corresponding vulnerabilities in order to formulate an exploitation strategy

Exploitation:In accordance with the previously outlined strategy the feasibility of exploiting the discovered vulnerabilities will be assessed in order to extend the reach inside the system and gather further information on it.

Refactoring and Pivoting:Based on the successful exploitation scenarios a refactoring process will take place in order to define the best possible cause of action in order to pivot and further compromise the system with maximum impact.

Clean-up:All operations carried out during the assessment are intended to be non-intrusive and are run exclusively with the permission of company management. At no point during the penetration tests will service continuity or data integrity be affected and the majority of exploits are only proof of concept.

Results analysis and reporting:All the data collected in the previous phases is aggregated and structured in a comprehensive format focusing on business impact. All the identified vulnerabilities have also been supplied with valid recommendations in accordance with security best practices. The executive summary will contain system wide observations the view the architecture as whole

Vulnerability classifications
Critical Risk

The vulnerability represents a grave problem which requires immediate attention. It constitutes a major risk that can lead to serious security breaches, financial and image losses as well as prolonged service interruptions.

Medium Risk

Represents moderate risk, and requires problem remediation in a reasonable amount of time. Impact is limited but insufficient security controls may lead a more serious breach

Low Risk

Low risk and priority usually referring to a routine operations. No major impact on security.

Informational Risk

Represents an observation whose impact could not be determined for the moment but which must be brought to the attention of the company