Payatu

November 2022

Cyber Threat Intelligence Report

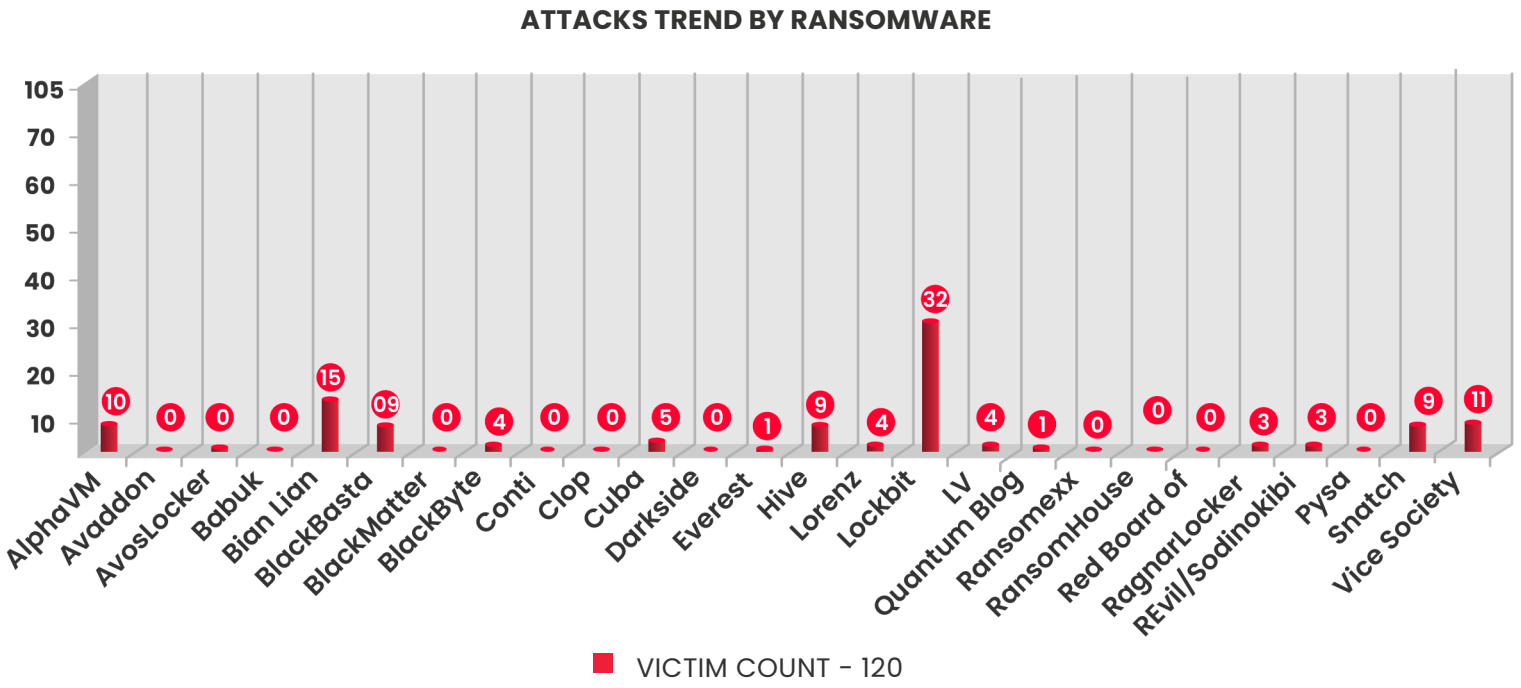
Payatu Security Consulting Pvt. Ltd.

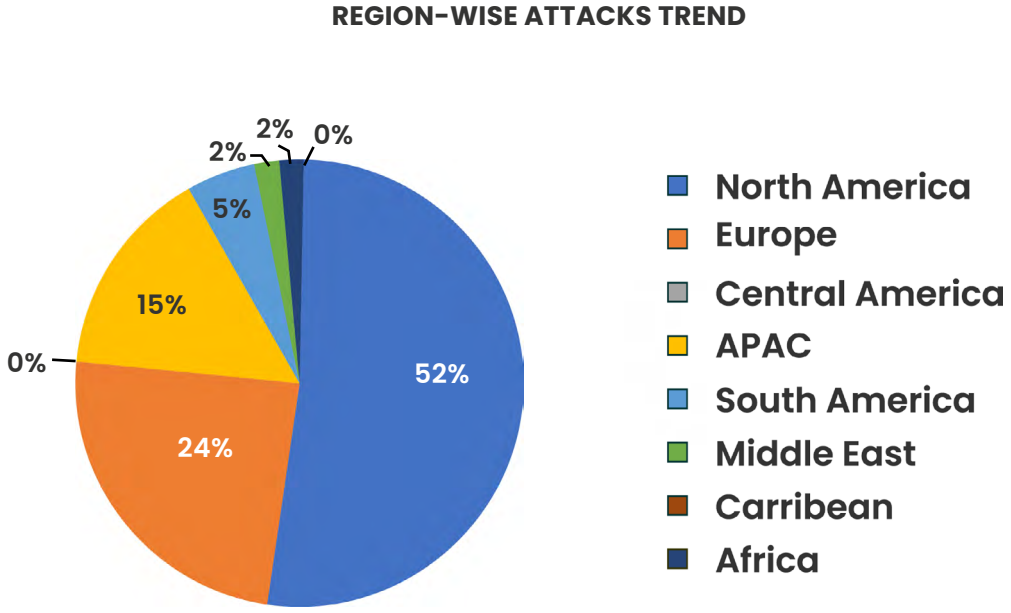
Table of Contents

01

Ransomware Statistics

- AIIMS Delhi under alleged ransomware attack.
- Ransomware attacks in India increase by 42%.





Country-wise Attacks Trend - 175

 Australia - 3

 Austria - 1

 Belgium - 1

 Brazil - 5

 Canada - 7

 China - 1

 Czech Republic - 1

 France - 1

 Germany - 7

 Hong Kong - 1

 India - 7

 Italy - 2

 Japan - 2

 Mexico - 2

 Morocco - 1

 Netherlands - 2

 Philippines - 1

 Poland - 1

 Saudi Arabia - 1

 South Africa - 1

 Spain - 2

 Switzerland - 1

 Taiwan - 1

 Thailand - 2

 United Arab Emirates- 1

 United Kingdom- 10

 United States- 55

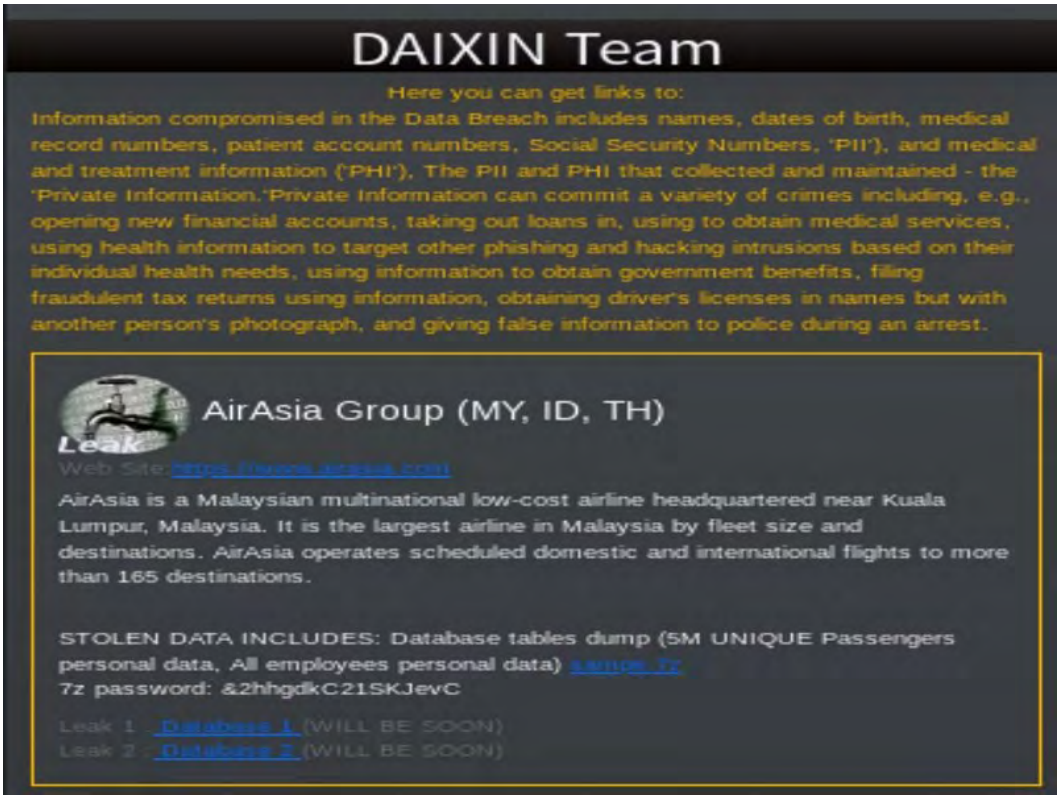
Payatu

02

Air Asia - A Victim of Ransomware Attack by Daixin Ransomware

Tags: Air Asia, Ransomware, Daixin

Daixin Team, recently highlighted by CISA-USA, where it shared an advisory on the ransomware group, has now targeted Malaysian aviation giant Air Asia group. Sharing samples and other details on its data leak website on November 19th, 2022, **the group updated that the leak involved 5 million unique passengers related to PII (Personal Identifiable Information) and data related to all employees.**



Source: 7ukmkdtyxdkdivtjad57klqnd3kdsmq6tp45rrsxqnu76zzv3jvitlqd[.]onion

Currently sharing two sample files (namely sample_1.xls and sample_2.xls) with 10,000 passenger details and 1000 employee details respectively. The data contained PassengerID, Name, Booking ID, Cost etc. And for the employee details include some interesting data like a secret question and answer for tense situations, CrewPortalUserID, apart from PII.

The Daixin team interacted with a breach intelligence website and shared

that the Air Asia group has not negotiated for the data. The impact of this data leak on Indian flyers is not major, as the data leaked does not include highly sensitive data. However, the impact on employees is major as the data leaked can be used for blackmailing and phishing to security breach in case of terror attacks.

IOCs for Daixin shared in Appendix 1A.

03

Australian Health Insurance Giant Suffers a Cyber Attack

Tags: Medibank, Insurance, Data breach

Medibank Private Limited, one of the largest Australian private health insurance providers, informed its customers about the data leak that occurred in the month of October. The company clearly denied any payments of ransom and informed its customers that PII (Personal Identifiable Information) data consisting of name, DOB, phone number, and email address for around 9.7 million customers, former customers, and authorized representatives were leaked on the dark web.

The figure represents 5.1 million Medibank customers, around 2.8 million AHM customers and around 1.8 million international customers. The data for AHM customers also includes Medicare numbers, while critical details like passport numbers and visa details have been leaked for a few international student customers. Other critical information includes health provider details, location diagnostic codes and procedures administered for certain patients. No financial details have been accessed.

On its part, the insurance provider has set up dedicated Cyber Response Support Program, cybercrime emergency response numbers where trained support is established to manage various crimes and issues related to sensitive health information. **In past two months, this is the third major data leak targeting an Australian company after Optus and Telstra.**

Source: blogxxu75w63ujqarv476otld7cyjkq4yoswzt4ijadkjwvg3vrvd5yd[.]onion

IOCs for Revil ransomware are shared in Appendix 1B.

04

Critical Vulnerabilities in OpenSSL, Patches Deployed

Tags: OpenSSL, CVE-20220-3786, CVE-2022-3602

Two high-severity bugs have been identified and released by OpenSSL on November 1st,2022, that have been fixed in the OpenSSL 3.0.7 version.

CVE-2022-3786 and CVE-2022-3602 are buffer overrun vulnerabilities, after certificate chain signature verification is complete, an overflow is triggered during X.509 certificate verification, specifically in name constraint checking. A pre-requirement to these attacks is that either a CA (Certificate Authority) has signed a malicious certificate, or the application that is verifying the certificate continues the process despite failure to construct a path to a trusted issuer.

An attacker in the case of 1st vulnerability can craft a malicious email address in a certificate to overflow an arbitrary number of bytes, containing a decimal character (.) on the stack. In a TLS client it can be triggered by connecting to a malicious server, and in the case of a TLS server, triggered if the server requests client authentication and the malicious client connects.

In the case of 2nd vulnerability, an attacker can similarly craft a malicious email address, with the difference of overflowing through four attacker-controlled bytes on the stack. This overflow could result in Denial-of-Service (DoS) or potentially Remote Code Execution (RCE). The attacking techniques on TLS client and TLS server are like those seen in the above vulnerabilities.

Originally marked as critical severity, however, due to certain mitigating factors that are applied by various platforms, like stack overflow protections, the severity was reduced to High. **OpenSSL still urges people to upgrade to the new version.**

05

Pakistan Based Threat Actors Target Indian Governmental Organizations

Tags: Kavach, APT-36, Government

The research team at Zscaler has identified a campaign from APT-36 targeting Indian government and its users in 2022 by abusing Google advertisements. These malicious ads distribute backdoored versions of Kavach MFA applications. Kavach is an initiative by Government of India to add security to smartphone devices that create an MFA (multi-factor authentication) system. The app is mainly used by government employees and army personnel.

Dubbing the tool used for data exfiltration as "Limepad", the researchers shared that the campaign uses Google ads paid search feature to push the malicious domains to the top of Google search results in India, these domains masquerade as official Kavach download portals. The attack techniques also include credential harvesting attacks through these fake websites.

This suggests that organizations and individuals need to be extra careful while accessing Google ads and be cautious before downloading mobile applications from third party websites which, by the way, is not the preferred method of installation. In addition to APT-36 another group using Google ads for the campaign is Royal ransomware.

IOCs shared in Appendix 1C.

06

CISA Updates on ICS Systems Vulnerabilities

Tags: ICS, Vulnerabilities

On November 3rd,2022, CISA-USA shared an advisory relevant to ICS (Industrial Control Systems) with reference to critical vulnerabilities in ETIC Telecoms servers, Nokia 5G system module and DIALink respectively.

ETIC Telecom Remote Access Server (RAS):
CISA updated the security community about three vulnerabilities in ETIC's Remote Access Server 4.5.0 and previous versions, affecting its Web portal and API. CVE-2022-3703 is a vulnerability that could provide backdoors to an attacker through malicious firmware packages, leading to privilege escalation.

CVE-2022-41607 is a directory traversal vulnerability in RAS's API allowing an attacker to read sensitive files from the server.

The third vulnerability CVE-2022-40981 makes it possible for an attacker to upload malicious files on the server.

Nokia ASIK AirScale System Module:
The vulnerabilities in the Airscale System Module affect the versions 474021A.101 and 474021A.102 allowing arbitrary code execution through uploaded script through CVE-2022-2482, vulnerability in signature check that can be bypassed to run a malicious firmware through CVE-2022-2484, and disabling secure boot permanently by modifying flash content to corrupt public keys, which are used by bootloader for firmware verification signature through CVE-2022-2483.

Delta Industrial Automation DIALink:
DIALink is a tool used to collect onsite data from industrial equipment.
The vulnerability identified in this tool is CVE-2022-2969, which allows unrestricted path traversal due to improper limitation of a pathname to a restricted directory.

07

Aurora, A New Botnet and Stealer To Lookout For

Tags: Botnet, Aurora, Malware

Researchers at Sekoia have discovered a new botnet Aurora, advertised on underground forums as an infostealer with multiple other capabilities. Developed in Golang, the malware was originally used as a botnet as part of MaaS (Malware as a Service). However, recent developments show that the malware is now publishing its stealer capabilities. It is capable of data collection, exfiltration to its C2 server and loading the next stage payload.

The stealer uses WMIC (Windows Management Instrumentation Command) and like all other stealers, takes screenshots. It collects information from multiple web browsers that are listed in its code. The malware is also capable of grabbing interesting files from directories listed. Infection chains used by the stealer include phishing websites, masquerading legitimate websites, YouTube videos, and fake software catalogue websites.

08

Emotet Returns With New Updates and Affiliations

Tags: Emotet, TA542

Active since 2017, malware Emotet aka TA542 has been once again launched through various phishing campaigns since early November 2022.

In their blog, researchers at Proofpoint have shared a comprehensive look of malware's recent activities through which, it has been luring individuals using excel and attachments with visual rules.

The malware has been observed targeting individuals through IRS-themed and quarterly tax requirements-based campaigns along with generic lures. The geographical locations being targeted include the USA, UK, Japan, Germany, Italy, France, Mexico, Brazil, and many others. Attachments that are macro-laden with excel if stored in administration-based folders, execute without any warnings during interactions, and in other cases require administrative permissions.

Possessing new commands, implementations and packers, the malware has updated commands for its bot, loading module, and is delivering in addition to its old pal IceID and XMRig.

For IOCs, refer to Appendix 1-D

09

CISA Warns on Increasing Attacks from Hive Ransomware

Tags: Hive Ransomware, Microsoft Exchange Server

In another advisory as part of the #StopRansomware initiative, CISA released a joint advisory on attack trends and analysis of Hive ransomware. Hive ransomware, which has been following a RaaS (Ransomware-as-a-Service) model, has been actively targeting Government facilities, Communications, Critical Manufacturing, Information Technology, and Healthcare facilities.

This ransomware uses different initial access techniques like Phishing, External Remote Services by exploiting RDP, VPN and other similar services. Hive bypasses multi-factor authentication (MFA) through FortiOS CVE-2020-12812 vulnerability. In Phishing attempts, the hive exploits vulnerabilities in Microsoft Exchange Servers, namely CVE-2021-31207, CVE-2021-34473, CVE-2021-34523. Exfiltration takes place with the help of cloud storage service mega.nz, which is followed by encryption of files and a ransom note along with a file named *.key in root directory.

In case of public disclosure of files, the group has been known to leak files through several anonymous services such as anon files, mega, ufile, privatlab.

For IOCs, refer to Appendix 1E

10

AIIMS New Delhi Hit by Alleged Ransomware Attack

Tags: AIIMS, India, Cyber Attack, Healthcare

On November 23rd, 2022, all online operations ceased at AIIMS Delhi due to a cyber incident affecting their servers. The attackers managed to erase patients data from the main and backup servers, and affected its digital services such as report generation from all departments and smart billing.

The motivation originally thought to be financial, as seen in the case of most ransomware, remains unclear as the MO (modus operandi) followed by the hackers in this case is slightly different, as after gaining access the attackers have erased the data instead of encrypting it and later sending a ransom mail to AIIMS. There is no official confirmation of any such mail by AIIMS authorities. As the services remain down for seven days till 30th November, it is still unclear why and by whom the attack was devised.

On investigating chatter over the dark web, no notable updates have been found as seen in case of ransomware attacks on the DLS (Data Leak Site) site and blogs. Though there happens to be some conversations going on, a chat over Telegram channel named KindEvils has been actively updated on any status pertaining to the news.

The drastic effect on the patients because of delays in services is one of the issues; however, AIIMS being a reputed hospital with VIP patients also raises concerns of National security as the health-related data can be actively exploited by the attackers.

10

Appendix

Appendix 1A – Daixin Team Ransomware

SHA256
9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238
19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD
54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939
EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574BAB987515AA40CBF
475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28

Appendix 1B – Revil Ransomware

SHA256
9f58b1fed5eef303f06e23f48c9359d2a74f51235677ae880bce67d76f5c827c
e281347d6faf8fa17e9bcd79d0f815187506c89e8bca9ffae78170e31ff07438
7c7ad08931468eecb7a250a9108936976ce8b2eaa9489f2a802580851b9f32
a89591555b9acb65353c2b854e582bc41db2fbc0e2210b89a877d1862084df
9fa3a004576f357b5174dd1c29ef7d13005d996d5f9fb4b86d6d978d1a4a8ae
1501f261a66eefce47dc47cb8a426107c4b694a41b5b9f000d0ad2ea76d8e34
7bafd5de1b6724962ab920f71031978a101055f061ae3cc21db8bb9fa64c5829
d0e9cd5dbdf59931d69e28c313931fac6bef83ec9f75bd84f6cb65c43f1646e7
36fa3f72afc2dd6f206a295fc618038fef5e241bc48bd5451ac9bab9128734dd
dd05b24610d5f9513e68201a88cdb05391bfd061346a7274062d1416e8322ff6
861bc212241bcac9f8095c8de1b180b398057cbb2d37c9220086ffaf24ba9e08
90c9b6460c240177644d028458874167fedf7ca459381dde17d44446b9ba50
6efd9aae5e112418bd43ab48ec4a1fce191c7503fcd11fdb95e89ad0217adb7a
a389e24bf0af9bc81b8133a600a2b6c875d32aa0885964d0b9f3ac65fee762
1937098609fbbda1b470811a7ffe5fa044058655722d84bd029050d54f2b1496

9aec4ab2c722c0ce0a01fcb5ac05b3f3d014b3f233f4b96d8f5e0f7826011a9c
89d80016ff4c6600e8dd8cfad1fa6912af4d21c5457b4e9866d1796939b48dc4
c9b04ec734151245774b54df09fc77011d703f4c93c277dbd26b998e7b6db29c
10071748cab19d1d637f24bbbb1e9fb677da5110d1cf91988436064b4694165c
6727edbb5d6abee908851a8c5fd7b4aca6d664634fdcdfc1504502b960abc5
17d153a225ea04a229862875795eeec0adb8c32769ba005073baaf8685046
c4a7f8b8046a6623cd7909bacb1cbef13471a4efd8adb4aedbf7c1377ab502d
a3f077a4c29c522d9d70e3b22778c5a07239b6949562b376175ac913843076
aad3f0a2dfc2bfce8da3523cc4a4a302d44415eb14da85861009752b249c39

Appendix 1C – APT36

Domains
ncloudup[.]com
gcloudsvc[.]com
nic-updates[.]in
kavachmail-govin[.]rf[.]gd
kavach-app[.]com
kavachguide[.]com
kavach-app[.]in
get-kavach[.]in
getkavach[.]com
kavachsupport[.]com
kavachdownload[.]in
kavachauthentication.blogspot[.]com
139.59.79[.]86
wzxdao[.]com

MD5
123b180ed44531bfbac27c6eb0bbe01d
3817590cf8bec4a768bb84405590272f
0ed6451ffe34217e44355706f4900ecc
94daa776792429d1cb65edc1d525e2fc
c195d6bb06c93b94d39e5c1a2dfc6792
889c5c98e88c4889220617f57f5480f7
ac3f2c8563846134bb42cb050813eac8

Appendix 1-D

SHA256
05a3a84096bcdc2a5cf87d07ede96aff7fd5037679f9585fee9a227c0d9cbf51
99580385a4fef0ebba70134a3d0cb143ebe0946df148d84f9e43334ec506e301

Domain
Bayernbadabum[.]com

Payatu's Security Capabilities

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared. As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

More Services Offered by Payatu -

- IoT Security Testing
- AI/ML Security Audit
- DevSecOps Consulting
- Critical Infrastructure
- Trainings