Payatu

May 2023

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

Table of Contents

A.
Ransomware Statistics 03

B.
OWASP Launches a New Project and Privacy Guide for AI Security 05

C.
MacOS Users Targeted Using Cobalt Strike Payloads Written in Go 06

D.
Google Comes Up with .zip Domains, Threat Actors Try New Exploitation Techniques 07

E.
Researchers in South Korea Develop a Mobile Network Sniffer 08

F.
CISA Issues Advisory Against Chinese State-sponsored Threat Actor, Volt Typhoon 09

G.
DarkBert - The AI Model for Understanding Dark Web Activities 10

H.
Mandiant Identifies a New OT Malware - Cosmicenergy 11

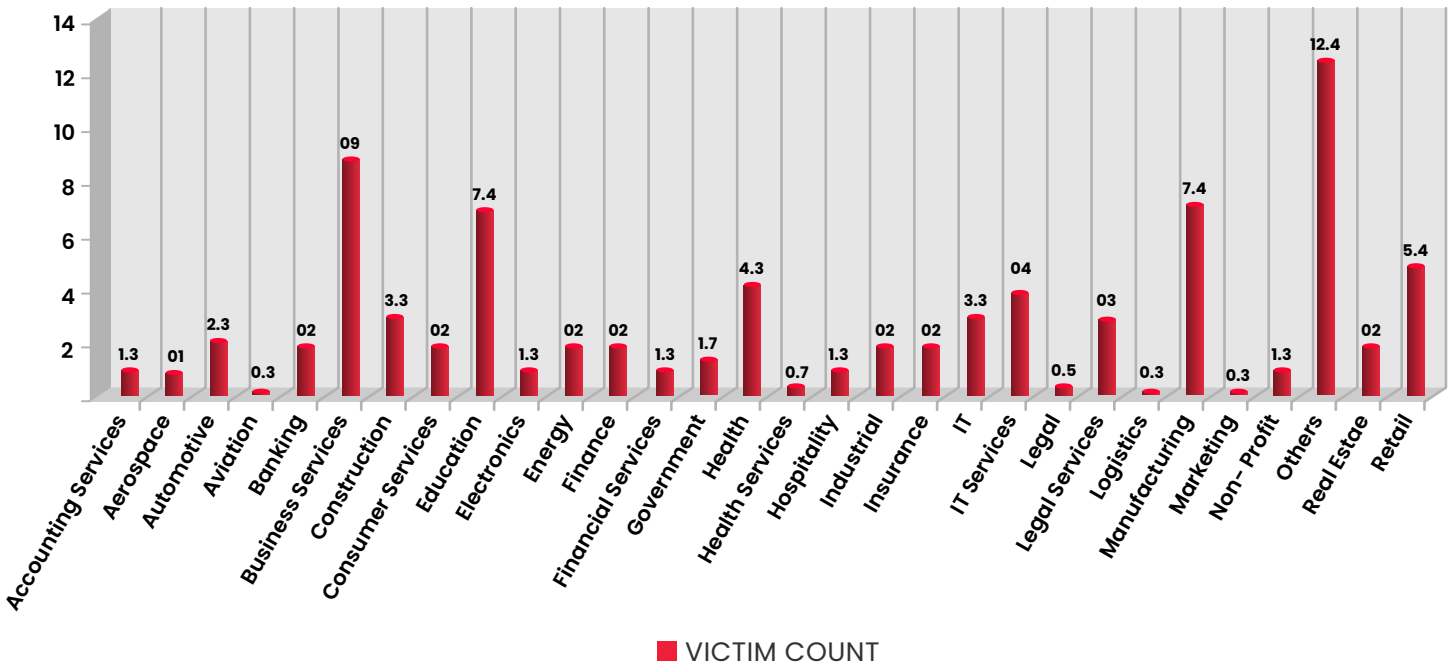
I.
Appendix 12

01

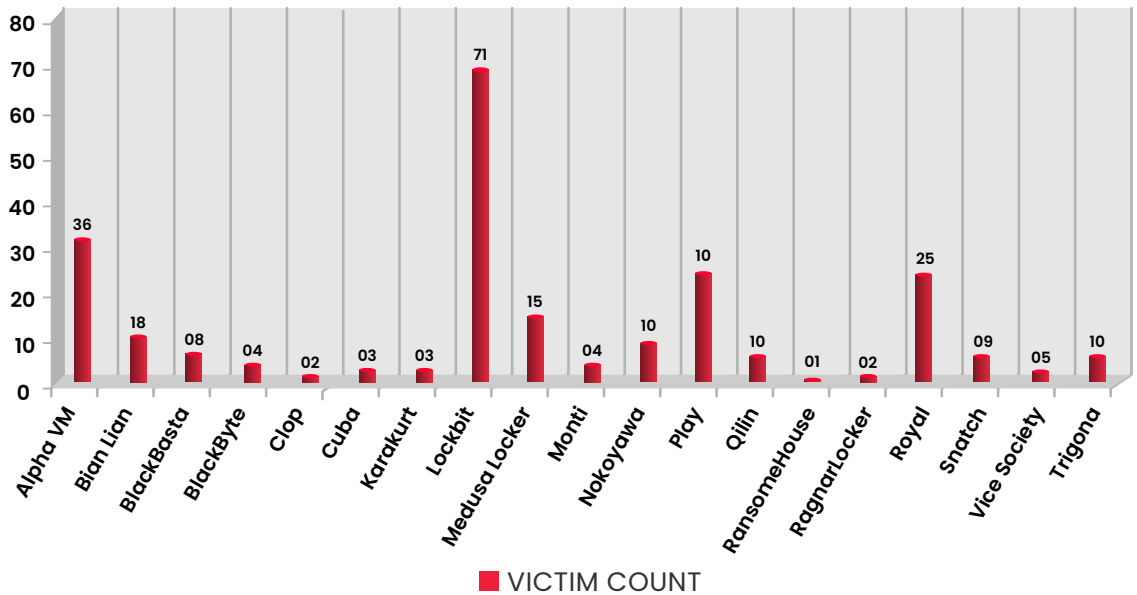
Ransomware Statistics

- FRESCA, a world-renowned beverage company hit by Snatch ransomware.
- IT Works Global hit by AlphVM ransomware.
- Increased attacks on business services sector, healthcare sector and education sector

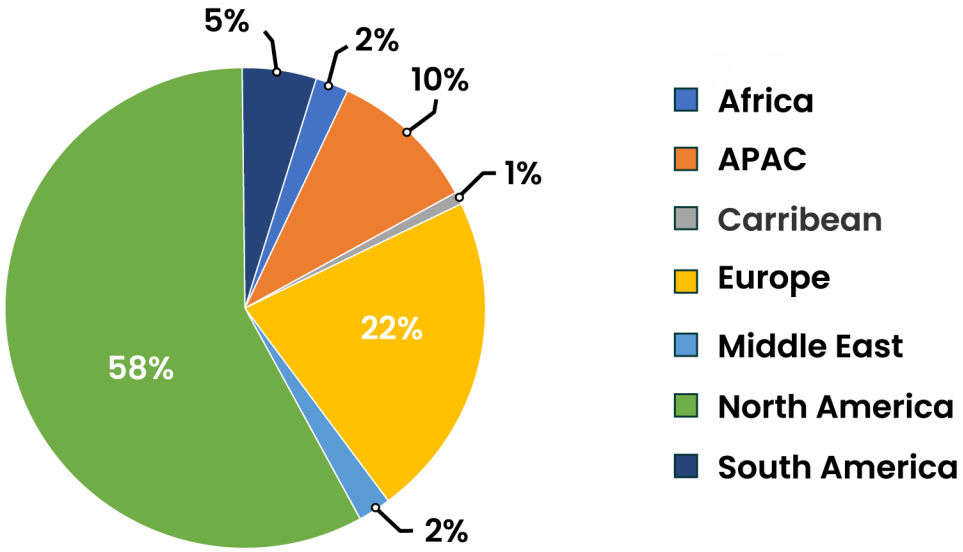
SECTOR-WISE ATTACK TREND



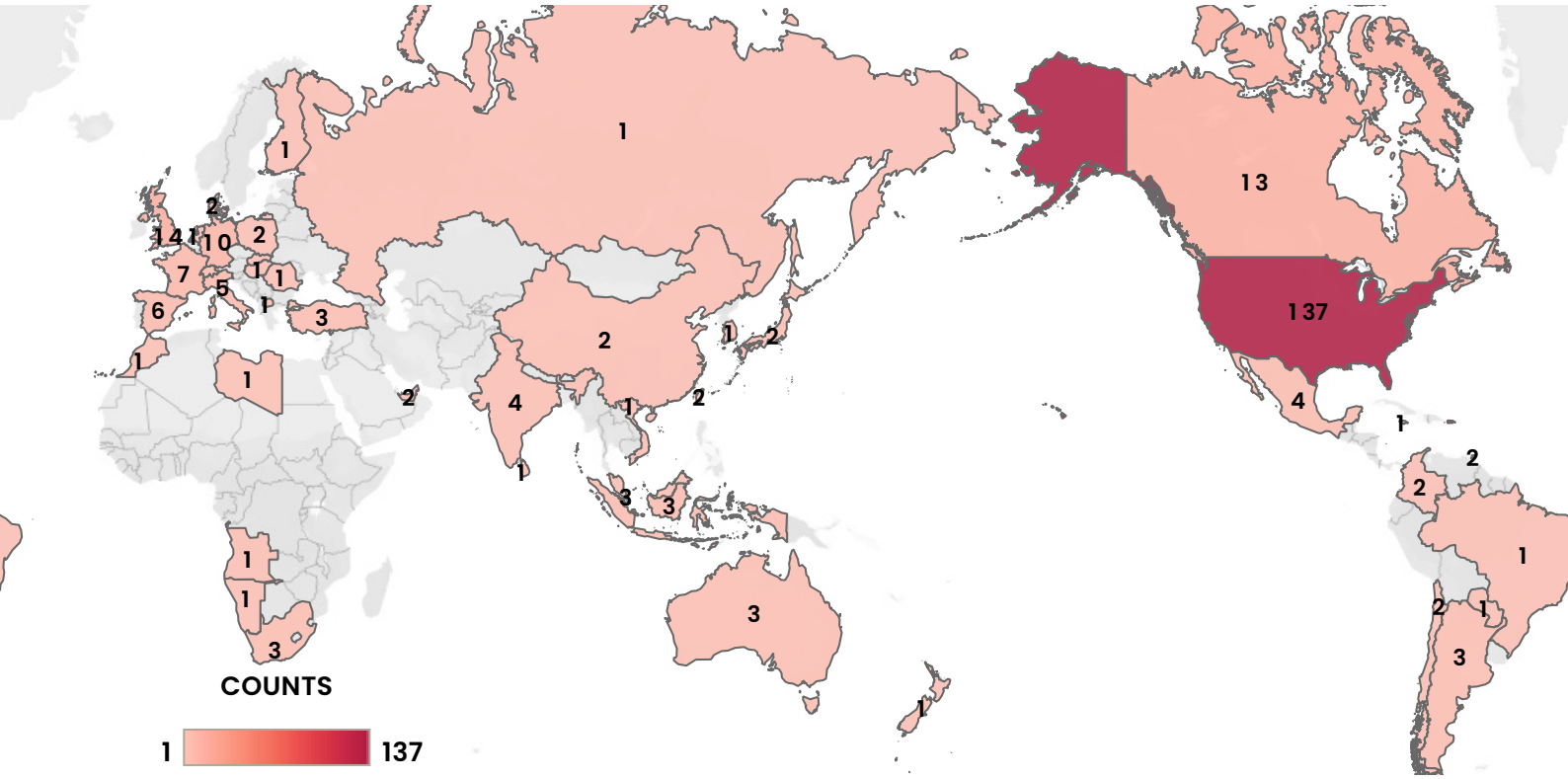
ATTACKS TREND BY RANSOMWARE



REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 262



02

OWASP Launches a New Project and Privacy Guide for AI Security

Tags: AI, OWASP

Members of the OWASP foundation recently have been developing an AI security and privacy guide to assist security professionals in securing the Artificial Intelligence landscape given the sudden increase in its demand and availability.

Suggesting professionals to understand the AI lifecycle discussed in detail on ISO's website, the guide discusses AI risks like identifying data attack surface, collecting real and authentic data, poisoning data models, input manipulation, data reconstruction, model supply chain attack, and many other possible scenarios. It also talks about privacy standards and requirements as per different regions and nations, while understanding the need to limit specifications and the limitations of storage that come with collecting data in real time for analysis and processing.

03

MacOS Users Targeted Using Cobalt Strike Payloads Written in Go

Tags: MacOS, Cobalt Strike

Cobalt Strike has been the ideal method used by most threat actors for exploiting Windows systems frequently. However, given its limitation of being unable to compromise macOS devices, until now, a Go-based setup of Cobalt Strike beacon called "Geacon" is being used to target macOS devices. Researchers at SentinelOne have identified active samples used by Chinese threat actors.

Spread as [.]app files – extension for Applescript Applet, the file faking as a resume .pdf file, calls back C2 domains. The decoy PDF file is a resume of a Chinese individual, with the capability to target both Apple silicon and Intel architectures. It is capable of communicating over network, encrypting, and further downloading files for exfiltrating data.

Another payload posing as securlink[.]app, an enterprise level application for remote connection, is trojanized to target only Intel devices. Malicious application targeting OS X 10.9 Mavericks and above, with user permissions can access device camera, contacts, databases, microphones, etc.

For IOCs, refer to **Appendix 1A.**

04

Google Comes Up with .zip Domains, Threat Actors Try New Exploitation Techniques

Tags: Google, .ZIP domains

This week, Google launched a new TLD (Top Level Domain) of .zip, meaning you can now purchase a .zip domain, similar to a .com or .org domain. The security community immediately raised flags about the potential dangers of this TLD. The TLD can be leveraged by an attacker to craft extremely convincing phishing links which will redirect you to a completely different domain altogether.

Among other domains announced by Google that include - ".dad, .phd, .prof, .esq, .foo, .mov, and .nexus", the .mov domain along with .zip domain is seen by the security community as a critical threat. Exploiting the .ZIP extension for files used as part of malicious email attachments, these domains can shorten the attack-chain exploited by threat actors.

In combination with other domain name exploiting techniques like using homoglyphs, threat actors can create URLs with look-alike domain and subdomain names with .zip as TLD. This can lead users to assume the extension into being a file. A detailed explanation of the same has been shared on medium by a security researcher.

By the end of the month, more than 8000 domains with .zip TLD have been registered.

05

Researchers in South Korea Develop a Mobile Network Sniffer

Tags: Telecom, Mobile Network, LTE, South Korea

Researchers in South Korea have developed an LTESniffer to analyze wireless traffic in LTE networks. The traffic between a cell tower and a smartphone is connected to it, but it cannot analyze encrypted data. The open-source eavesdropper first decodes the Physical Downlink Control Channel to obtain Downlink Control Information (DCIs) and Radio Network Temporary Identifiers. In simple language, a threat actor can wiretap and intercept all traffic between the base station and the target cell phone with 4G LTE in passive mode.

It is also capable of organizing an interception through APIs which can then be used in other third-party applications. Though the process and sniffer are available to use openly, the interception requires additional equipment like a programmable transceiver, antennas, and a whole lot of time and dedication to sniff relevant data from a large amout of information.

06

CISA Issues Advisory Against Chinese State-sponsored Threat Actor, Volt Typhoon

Tags: China, Evasion Techniques, Living-Off-the-Land

The United States and other international cyber security authorities together issued an advisory that highlights recent activities of a Chinese state-sponsored threat actor named "Volt Typhoon". The threat actor who primarily focuses on espionage and information gathering seems to be in the process of acquiring data and techniques for disrupting critical communications infrastructure. It has previously targeted other industries such as manufacturing, transport, IT, and education.

Recent activities suggest that the threat actor mainly focuses on post-compromise activities such as credential access and network discovery for the industries mentioned above. Active since mid-2021, the group has relied on living-off-the-land techniques and hands-on keyboard activities for issuing commands via the command line for collecting, archiving, and exfiltrating data. The data includes credentials from local and network systems using LOL techniques like credential dumping through LSASS, utilizing NtdsUtil, WMIC etc., which are later used for maintaining persistence.

To evade detections, the group tries to normalize its activities by routing its traffic through SOHO networks (Small Office Home Office networks), using customized versions of open-source tools to establish Command & Control channels.

For IOCs refer to **Appendix 1B.**

07

DarkBert - The AI Model for Understanding Dark Web Activities

Tags: AI, Language Model, Dark Web

Though the Artificial Intelligence hype has grown after the launch of ChatGPT and Bard, some researchers in South Korea have been working on developing a Large Language Model (LLM) that understands and analyses dark web communications and activities. The language model called Darkbert is based on the architecture of a previously developed AI approach – Roberta.

For those who work regularly on the dark web, it is easy to differentiate it from the surface web, not just based on the architecture, but also the language. The language model pre-trained on dark web data, can understand extremely complex and diverse structures of the dark web and gain evidence-based IOCs to mitigate emerging threats as part of CTI.

Different use case scenarios evaluated through the model include classification of different activities on dark web like selling stolen data, logs, drugs etc., ransomware leak site detection and processing, and monitoring sensitive threads and conversations on different forums. It does so by utilizing datasets called DUTA and CoDA.

08

Mandiant Identifies a New OT Malware - Cosmicenergy

Tags: ICS, OT, Cosmicenergy, Russia

Cosmicenergy - an ICS/OT-oriented malware identified by researchers at Mandiant, is capable of sending remote commands to affect the actuation of powerline switches and circuit breakers, resulting in power disruption. The malware, believed to be of Russian state-sponsored origin, is currently targeting countries in Europe, the Middle East, and Asia. It is not capable of performing discovery activities and hence is also attributed to being used alongside exploited MSSQL servers and gaining access to target electric grids, specifically IEC-104 devices.

It works like **Industroyer**, a malware that targeted the Ukrainian power supply in 2016. However, it accomplishes the task through two components, namely **"Piehop"** and **"Lightwork"**. **Piehop**, which is written in Python, is a disruptive tool capable of uploading files and issuing remote commands to an RTU (Remote Terminal Unit). At the same time, it also utilizes **Lightwork** written in C++ to do the actual work and issue ON and OFF commands to IEC-104, by crafting Application Service Data Unit messages changing the state.

For IOCs, refer to **Appendix 1C.**

11

Appendix

Appendix 1A - Geacon payloads

SHA1
6831d9d76ca6d94c6f1d426c1f4de66230f46c4a
752ac32f305822b7e8e67b74563b3f3b09936f89
bef71ef5a454ce8b4f0cf9edab45293040fc3377
c5c1598882b661ab3c2c8dc5d254fa869dadfd2a
e7ff9e82e207a95d16916f99902008c7e13c049d
fa9b04bdc97ffe55ae84e5c47e525c295fca1241

Observed Geacon C2s
47[.]92[.]123[.]17
13[.]230[.]229[.]15

Bundle Identifiers
com[.]apple[.]ScriptEditor[.]id[.]1223
com[.]apple[.]automator[.]makabaka

Suspicious File Paths
~/runoob[.]log

Appendix 1B – Volt Typhoon

SHA-256
baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c
b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c-8b4a80af
9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aac-cb406401a
450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267
93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066
7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5
389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61
c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b-1552c283b
e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb-61c98a58b6e95
6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f-448461400baa984

17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2
d17317e1d5716b09cee904b8463a203dc6900d78ee2053276c-c948e4f41c8295
472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f-09352398c05be5d05d
3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642

Appendix 1C – Cosmicenergy

Filename	Description	Hash
r3_iec104_control.exe	PIEHOP PyInstaller executable	**MD5:** cd8f394652db3d-0376ba24a990403d20
		HA1: bc07686b422aa0dd01c87ccf557863ee62f6a435
		SHA256: 358f0f8c23a-cea82c5f75d6a2de37b-6bea7785ed0e32c-41109c217c48bf16010
r3_iec104_control	PIEHOP Python compiled bytecode entry point	**SHA1:** e91e4df49afa628f-ba1691b7c668af64ed-6b0e1d
		SHA1: e91e4df49afa628f-ba1691b7c668af64ed-6b0e1d
		SHA256: 7dc25602983f-7c5c3c4e81eeb1f-2426587b6c1dc6627f20d-51007beac840ea2b
r3_iec104_control.py	Decompiled PIEHOP entry point Python script	**MD5:** c018c54eff8fd0b-9be50b5d419d80f21
		SHA1: 4d7c4bc20e-8c392ede2cb0cef-787fe007265973b
		SHA256: 8933477e8220 2de 97fb41f4cbbe6af3 2596cec70b5b47da 022046981c01506a7

iec104_mssql_lib.pyc	PIEHOP Python compiled bytecode	**MD5:** adfa40d44a58e1b-c909abca444f7f616
		SHA1: a9b5b-16769f604947b-9d8262841aa3082f7d71a2
		SHA256: 182d6f5821a04 028fe4b603984b4 33574b782410514 2b722e3187 17a688969e
iec104_mssql_lib.py	Decompiled PIEHOP Python script	**MD5:** 2b86adb6afd-fa9216ef8ec2ff4fd2558
		SHA1: 20c9c04a6f8b95d-2f0ce596dac226d-56be519571
		SHA256: 90d96b-b2aa2414a0262d38c-c805122776a9405efece-70beeebf3f0bcfc364c2d
OT_T855_IEC104_GR.exe	LIGHTWORK executable	**MD5:** 7b6678a1c0000 344f4faf975c0cfc43d
		SHA1: 6eceb78acd106 6294d72fe86ed 57bf43b-c6de6eb
		SHA256: 740e0d2f-ba5503 08344b2fb0e 5ecfebdd09329bdcfaa-909d3357ad4fe5552532

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.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – Strategic, Operational and Tactical Intelligence, Risk Monitoring through social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platforming monitoring done for their brand.

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.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important

than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation Systems, etc., that can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.