RED PATRONUS

“One single vulnerability is all an attacker needs.” Window Snyder

About

Redpatronus is a security-oriented company focused on working on projects as a Red and Blue team. In the security field is more than 10 years experience in the public and private sector, even in the army.

We have strong experience with cloud providers as Google Cloud Platorm (GCP) and AmazonWebServices (AWS) and also with on-premise infrastructures.

Protocol offers

cert_commonName	SSLv2
vpn.hudiny.sk	not offered
petrzalka.sk	not offered
*.petrzalka.sk	vulnerable with 2 ciphers
ip.burso.eu	not offered
vpn.redpatronus.com	not offered

SSL vulnerability status

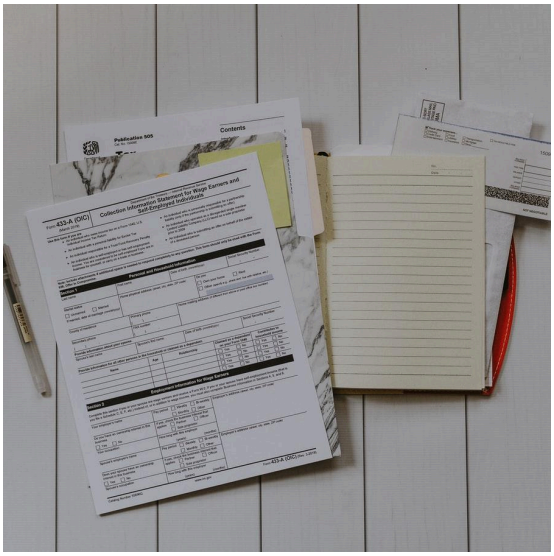
cert_commonName	heartbleed	CCS	ticketbleed	ROBOT
vpn.hudiny.sk	not vulnerable, no heartbeat extension	not vulnerable (timed out)	no session ticket extension	not vulnerable
petrzalka.sk	not vulnerable , timed out	not vulnerable	not vulnerable	not vulnerable

“

> If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.
>
> - Richard Clarke

GAP analysis

A cybersecurity gap analysis should encompass a comprehensive review of an organization's current security measures and practices compared to industry standards and best practices. It aims to identify vulnerabilities, weaknesses, and areas of improvement, providing a roadmap for enhancing the overall cybersecurity posture.



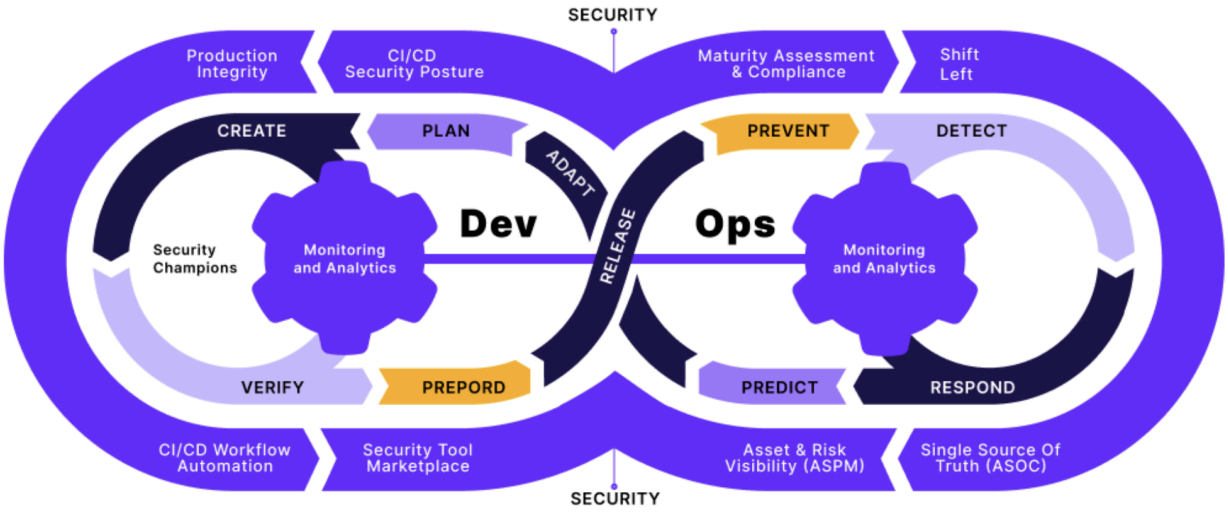
DevSecOps

- - - - X

Redpatronus is a security-oriented company focused on building the security infrastructure with a strong base in DevSecOps principle. As the company of security experts, we have numerous experiences with Terraform / Terragrunt. We can help you to build and manage your security infrastructure as a code.

CI/CD, Cloud Security Posture Management (CSPM)

- - - - X



Audit

- - - - X

Continuously audit your services in the cloud against CIS through our own solution (implemented via configuration management) or also we have experience with Security Hub (AWS) or Security Command Center (GCP).

Hardening environment (CIS benchmark) Cloud Security Posture Management (CSPM) (Sysdig)

- - - - X

Red team

- - - - X

The goal of a red team is to assess the security posture by identifying vulnerabilities, testing defenses, and providing insights into potential weaknesses from an external perspective, helping organizations improve their overall cybersecurity resilience.

Pentest, Continuous Pentest, Phishing Campaign, Table top exercises, Post Exploitation (only approved scenario).

- - - - X

Blue team

- - - - X

Responsible for defending and maintaining the security of a system or network, actively monitoring for threats, and responding to incidents to enhance overall cyber defense capabilities.

Dashboards, Anomalies, Alerts, Incident Investigation.

- - - - X

BCP

Evaluation of business continuity:

Assessing business continuity is critical because it can help minimise downtime in the face of unexpected disruptions. It is also an integral part of risk management, as it allows the organisation to prioritise the areas that need the most attention in terms of continuity planning.

Key components are typically:

- evaluation of storage & backup infrastructure to identify the potential impact on critical business functions, processes and resources after disruptive events (nature disaster, cyber attacks etc..)
- creating Business Impact Analysis document
    - this assesses the financial and operational consequences of a disruption
    - this helps to determine recovery time objectives (RTO), maximum allowable data loss (RPO) and prioritizations of recovery operations
- developing a Business Continuity Plan - creating detailed plans and procedures to ensure, that the organization can continue to function after a disruption (this includes a communications plan + data recovery plans)
- creating and testing DR procedures
    - planning and scheduling regular drills and exercises to test the plans designed above
    - regular review and update of plans

CyberSecurity Asset Management (CSAM)

Enterprise asset management (EAM) combines software, systems and services to help maintain, control and optimize the quality of operational assets throughout their life cycles. Including ASM (attack surface management).

(Sources: GCP AWS ISP), Shodan, Censys, URL scan.

Cyber Security Awareness

- - - - X

Redpatronus is educating individuals and organizations about the importance of protecting their digital assets from cyber threats such as hacking, phishing, and malware attacks. The service covers topics such as safe internet usage, password management, and recognizing and avoiding scams. Its goal is to raise awareness and provide knowledge and tools to prevent cyber incidents and protect against cyber attacks.

- - - - X

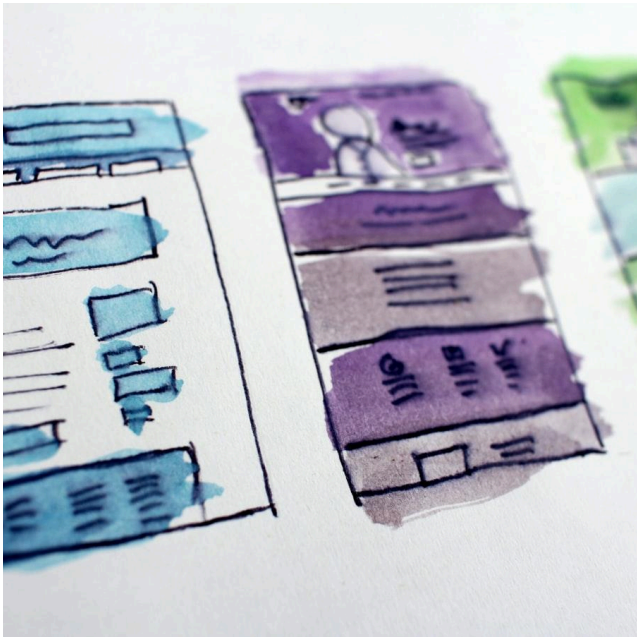
OSINT

Do you need to know what potential attackers can find out about your infrastructure, employees or you need to know more about common security threats?

We have experience with services as Shodan, Dehashed, haveibeenpwned, Censys, ProjectDiscovery, Maltego, sslscan, nmap, etc.

Next Generation RedPatronus Scanner - Service for scanning and getting information about domains, e-mail addresses, ssl configurations, etc.

> If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.
>
> - Richard Clarke



Web Application Firewall

- - - - ✗

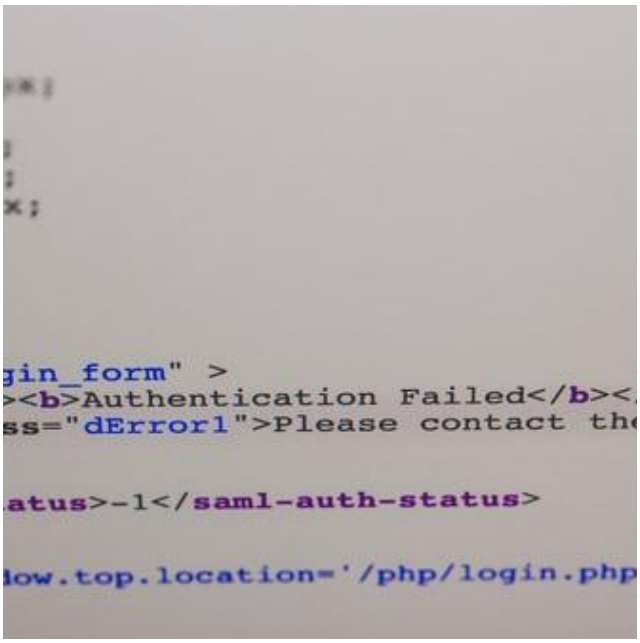
WAF will help you react to OWASP attacks immediately or before an attack occurs. We can set up positive and negative security models with almost 100% protection.

- - - - ✗

Our employees have daily experience and they are certified for these WAF technologies:

F5 Big-IP ASM
AWS WAF
Cloudflare
GCP CloudArmor

> Anything out there is vulnerable to attack given enough time and resources.
>
> – Kevin Mitnick



Vulnerability management

- - - - X

We are able to find vulnerabilities in your infrastructure.
Reviewing and
Scanning Computer, VM or K8s.

ECR/GCR or any other docker image repository? - we know how to do container scanning of your docker images

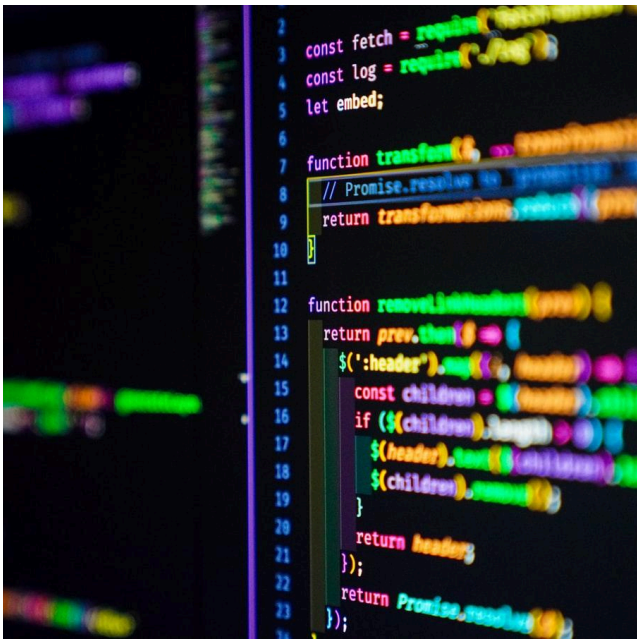
Also we are able to scan vulnerabilities in on-premise instances and provide regular reports for you.

- - - - X

“

Security is the chief enemy of mortals.

- William Shakespeare

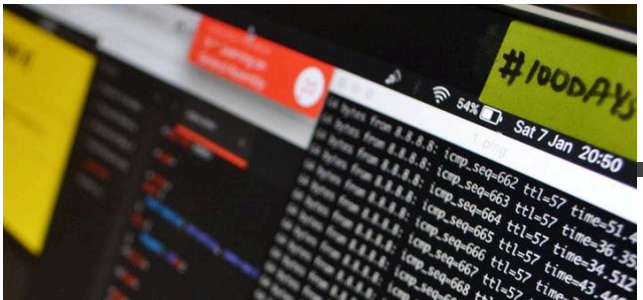


File Analysis

Scanning of malicious files or potentially unwanted files. It can be part of investigation of security incidents.

Our employees have experiences with analyzing malicious files in sandbox environment and digital forensics.

> Let your rapidity be that of the wind, your compactness that of the forest.
>
> – Sun Tzu



Network management

Palo Alto Networks Firewalls, VPNs, Identity firewall integration, Cisco Systems hardening network

Network Behaviour Analysis Detection - NBAD

Our employees have daily experience and they are certified for these technologies:

PCNSE Palo Alto Networks

Okta Professional

Cisco Systems

> Security is the chief enemy of mortals.
>
> – William Shakespeare

1. References

Areas of our services
Telco, Finance sector, Army, Customer Data & Experience Platform (CDXP)

Main area
Security operations
Pentesting web applications and infrastructure

Customers

External consultant 2015-2017 Security design and Security Devices	ALITER TECHNOLOGIES
External consultants 2011+	-B-
External Operation Engineers Audits & Implementation (All 2017-2022	ASENTI services
Security Operation Engineers 2018-2021	
Security Operation Engineers 2022+	bloomreach
Security Audits 2021+	BINARY CONFIDENCEd

2. Awards & Certifications

OSCP
CEH
SSCP
NATO clearance (SECRET)

#24 rank in CTF (capture the flag) on Cyber Apocalypse 2021


CYBER
APOCALYPSE
CTF 2021
HACK THE BOX
CERTIFIED CTF PLAYER
Matus Bursa
Participated in the Hack The Box
Cyber Apocalypse CTF in April 2021
24/4740
Team Ranking
assembly
Team Name
51/62
Solved Challenges
15650/19650
Total Points
CERTIFICATION OF PARTICIPATION
CYBER APOCALYPSE CTF 2021


CYBER
APOCALYPSE
CTF 2021
HACK THE BOX
CERTIFIED CTF PLAYER
Martin Zichacek
Participated in the Hack The Box
Cyber Apocalypse CTF in April 2021
CERTIFICATION OF PARTICIPATION
CYBER APOCALYPSE CTF 2021