Place your bets! How we run security for the whole Superbet group and still have time to play Stray ;)

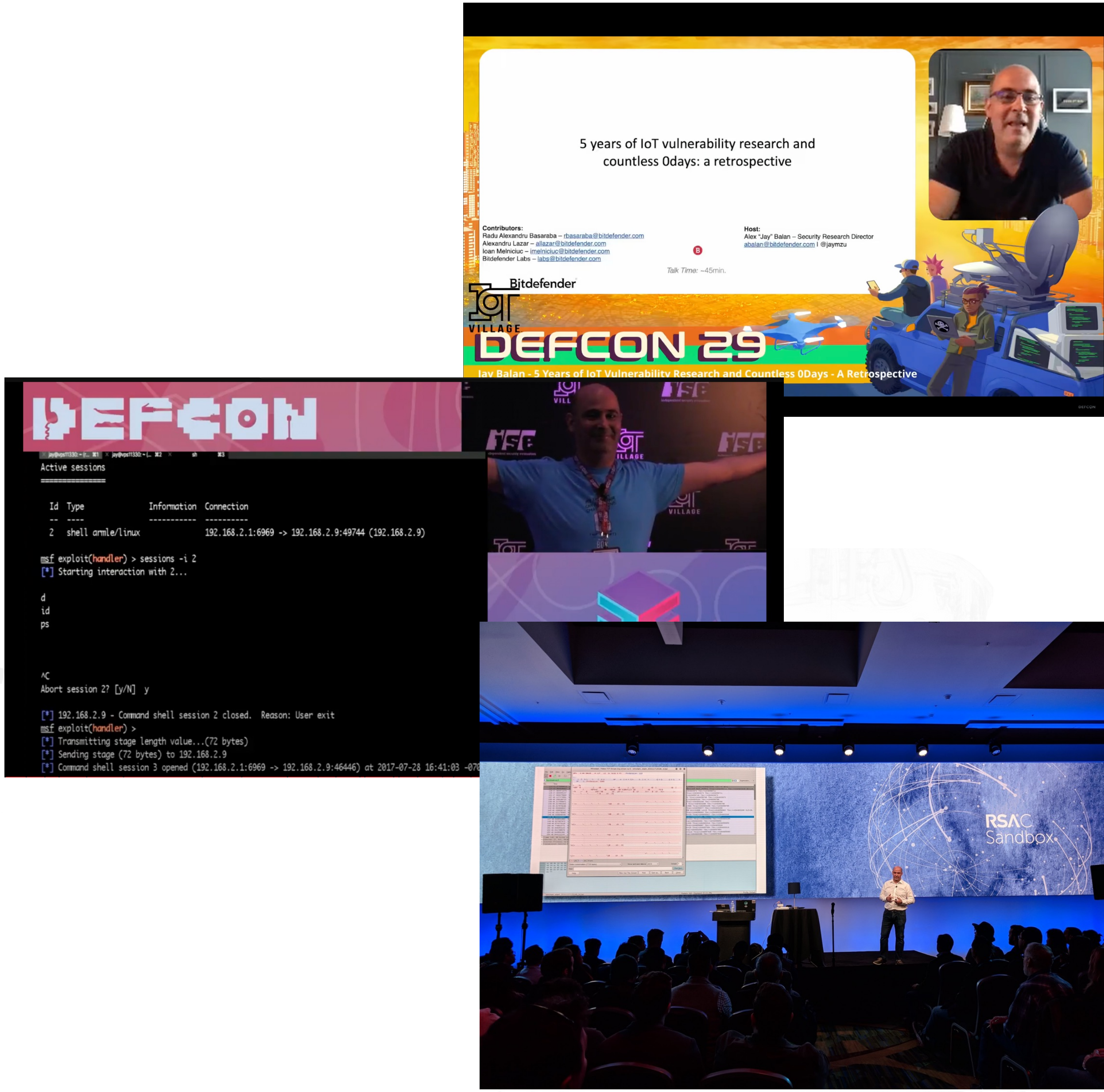
Alex “Jay” Balan | alex.balan@Superbet.com | @jaymzu

CISO, happening.xyz & Superbet Group

TLP:GREEN

about.me

- *NIX product line, Innovation, vulnerability research, internal red team, BugBounty program, spokesperson @Bitdefender
- Vulnerability research team published a lot of 0days, most in IoT
- Most of them presented at RSAC, DEFCON, DefCamp, DerbyCon and many others
- Glorified script kiddie
- Currently CISO @Superbet Group



5 years of IoT vulnerability research and countless 0days: a retrospective

Contributors:
Radu Alexandru Basaraba – rbasaraba@bitdefender.com
Alexandru Lazar – allazar@bitdefender.com
Ioan Melniciuc – imelniciuc@bitdefender.com
Bitdefender Labs – labs@bitdefender.com

Host:
Alex "Jay" Balan – Security Research Director
abalan@bitdefender.com I @jaymzu

Talk Time: ~45min.

Jay Balan - 5 Years of IoT Vulnerability Research and Countless 0Days - A Retrospective

```
Active sessions
===============

  Id  Type               Information  Connection
  --  ----               -----------  ----------
  2   shell armle/linux               192.168.2.1:6969 -> 192.168.2.9:49744 (192.168.2.9)

msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

d
id
ps




^C
Abort session 2? [y/N]  y

[*] 192.168.2.9 - Command shell session 2 closed.  Reason: User exit
msf exploit(handler) >
[*] Transmitting stage length value...(72 bytes)
[*] Sending stage (72 bytes) to 192.168.2.9
[*] Command shell session 3 opened (192.168.2.1:6969 -> 192.168.2.9:46446) at 2017-07-28 16:41:03 -070
```

About Superbet Group & happening.xyz

- Over 4500 employees across 10 countries
- A number of companies as part of the group. Some are recent acquisitions (own policies, infra, IT, etc)
- Not just online entertainment. Tech, robotics classes, chess tournaments, etc.
- happening.xyz is the technology engine that powers the Superbet group

SUPERBET

HAPPENING

NAPOLEON
SPORTS & CASINO

magic jackpot

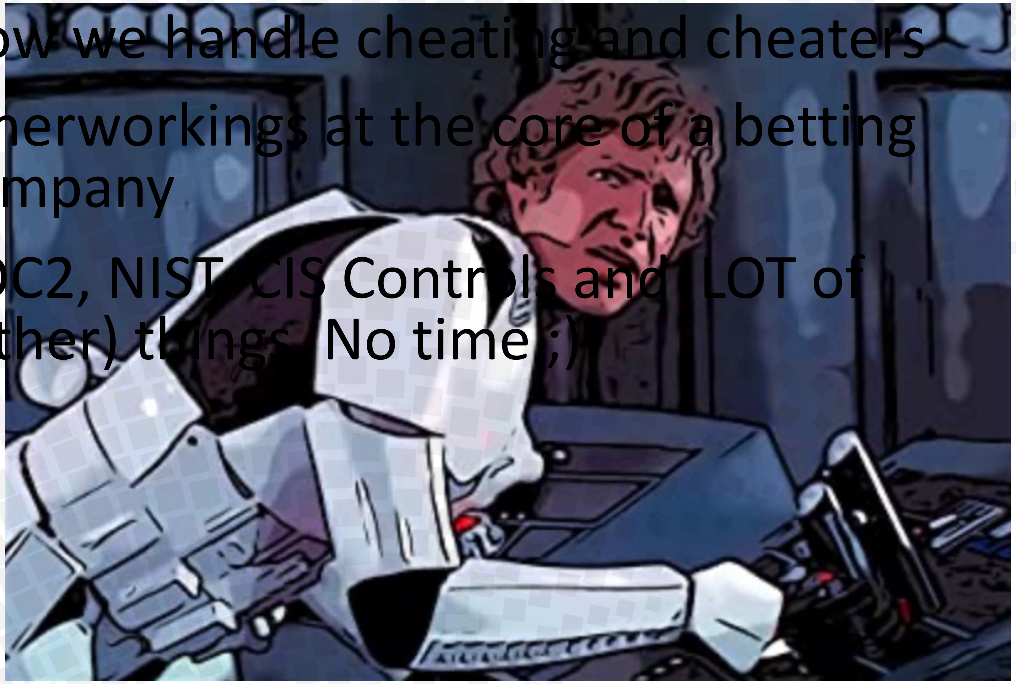
LUCKY DAYS™

TLP:GREEN

about.today

This talk will not feature

- How to cheat at sportsbets
- How to cheat the slot machines
- How we handle cheating and cheaters
- Innerworkings at the core of a betting company
- SOC2, NIST, CIS Controls and A LOT of (other) things. No time ;)



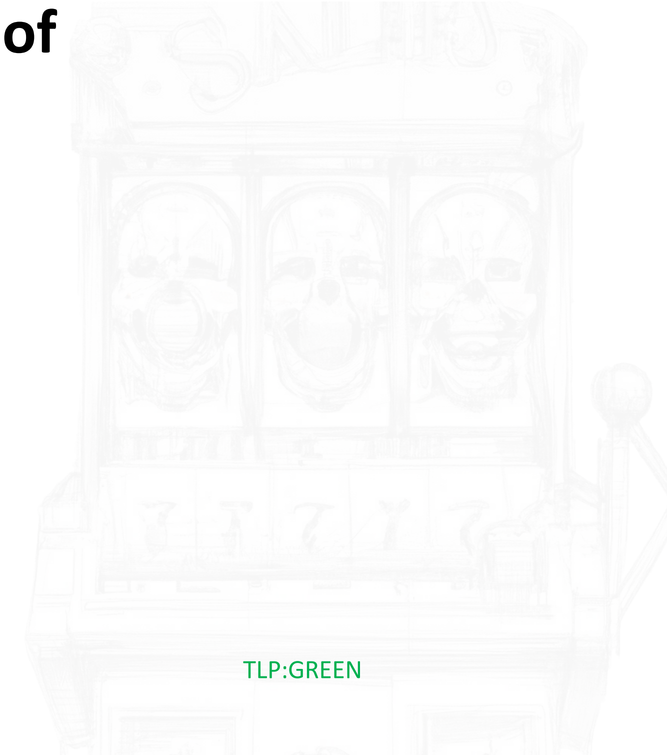
This talk will feature

- Challenges both technical and political
- Policies that some may consider controversial
- Concepts that will, hopefully, help your team, not matter where you are in the organisation

about.superbet.group

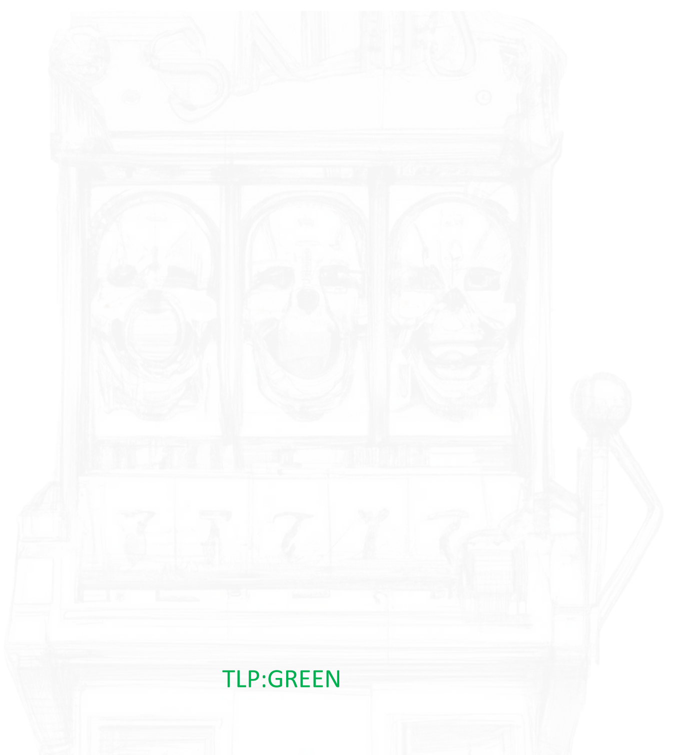
- Presence in 10 countries with operations and/or tech hubs
- Includes companies with their own policies and tech. Acquisition of another company must be factored in into the security strategy
- Engineering with an extreme level of diversity (languages, tools, etc) spread across multiple entities and geographical regions within the group
- 4500+ users/endpoints, also spread across multiple entities.
- Some entities are autonomous (their own tech stack) but still fall under our responsibility

Our main objective: manage the security of the whole ecosystem with as little disruption as possible and make it future-proof



about.future.proof

- Tech debt
  - Modern tools that increase productivity and employee loyalty. While a tough sell (they’re expensive), your users will love them. It can also be used to attract new talent
  - Eliminate internal hacks and subpar solutions
  - Eliminate and outsource as much as possible anything that’s not core IP
- Legacy & things that “can’t be fixed now”
  - They’re unavoidable
  - Pentest, isolation and full security stack (sensors, EDR, WAF, etc).
- Policies, playbooks and Single Source of Truth.



Team Structure

Everyone knows what to do and not to do. Writes more. Has a bigger text box.

Green

- Policies
- Trainings
- Compliance
- Internal comms

Defences & IR

Blue

- Threat Hunting
- Incident Response
- Forensics
- Defenses (WAF, EDR, etc)

Reduces the attack surface

Red

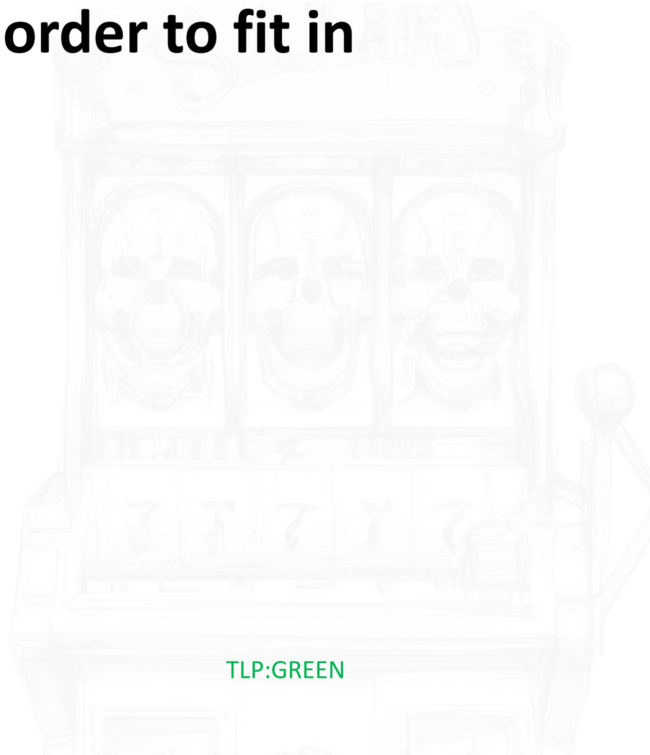
- Pentesting
- Automation
- Bug Bounty
- Rogue mentality

TLP:GREEN

More than CIS controls
The most underrated division: compliance

- Whatever documentation you have, make sure you always have a TLDR version of it
- Any policy you create should apply to the whole group
- Don’t worry about enforcing policies. Focus on communicating them!
- Any change you bring to the lifestyle of your users must be communicated at least 1 month before going in effect
  - Host webinars, AMAs, constant syncs with vertical leaders
- Budget a GRC platform
- Keep a public page with your plans

Always have updated policies and playbooks so every entity in the group (past, present and future) knows what’s expected from them in order to fit in



Cloud first

aws

splunk>

Azure Active Directory

- Eliminate dependencies on the local network (including AD). Move towards a **cloud-first** mindset
  - It's going to be a huge effort but totally worth it.
- Pick a strong identity provider. Enforce SSO everywhere and control access there
- Outsource as much as possible to trusted providers and reduce your management and maintenance to your core IP
- Eliminate any service on endpoints (SMB, RDP, VNC, etc). Be ready to be asked for (and challenge) exceptions.

slack

GitHub

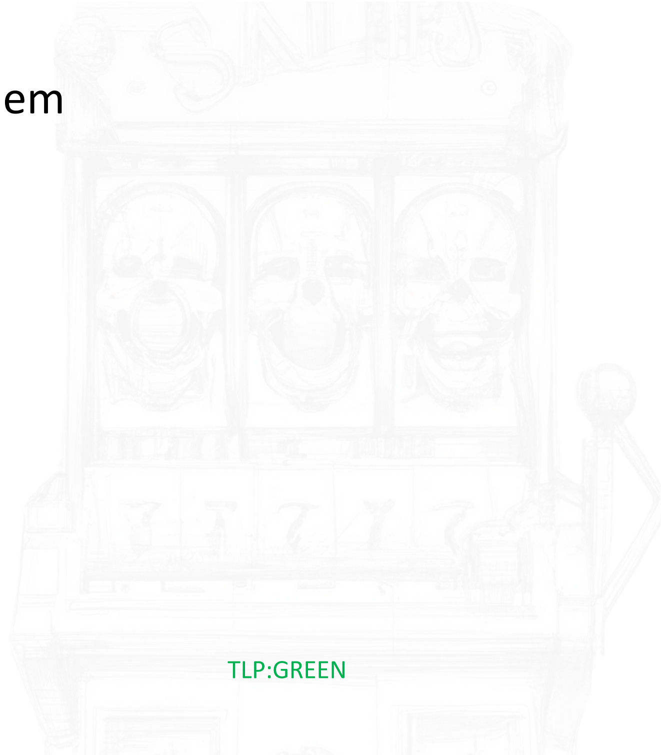
ATLASSIAN

Microsoft 365

ALWAYS AIM FOR HOW THINGS **SHOULD BE**

DON’T SETTLE FOR HOW THINGS **CAN BE**

You’ll be surprised of how things can change if you challenge them



TLP:GREEN

A few words on DIY on !core_ip

DIY is arrogance in believing that your v0.1 of a business app built inhouse with “just operational costs” is cheaper than an off the shelf mature solution that seems expensive.

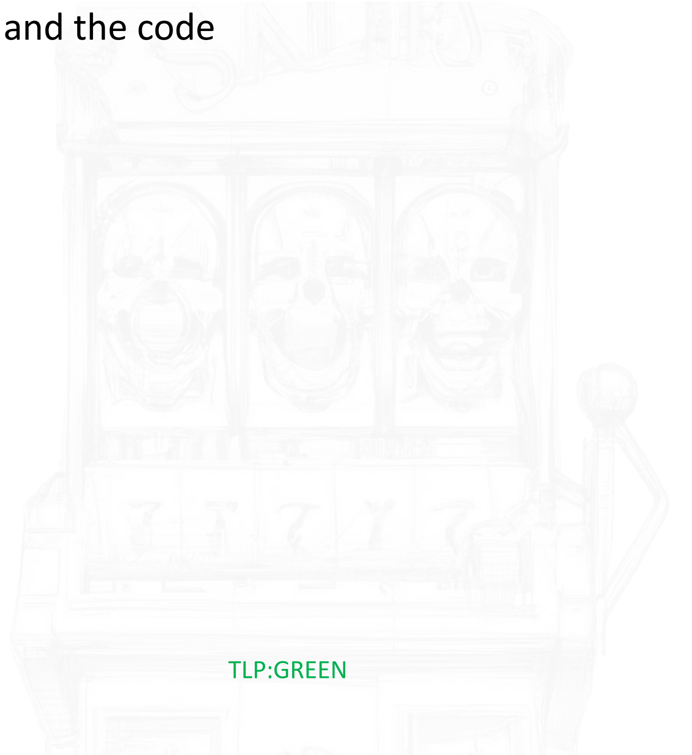
- Productivity costs
- Maintenance costs
- Security costs
- Employee retention

Priorities and first steps

- What are the low hanging fruits for attackers?
  - Focus on what’s really happening
- What are the most prevalent attacks?
- How much visibility do you have in the organisation?
- As your red team finds vulnerabilities, identify bad practices and use them to derive policies.
  - E.g. weak passwords on an internal app -> enforce SSO
  - E.g. ssh exposed -> enforce bastions

Make security part of everything

- Part of procurement – secure the supply chain
  - Avoid having to manage a risky vendor after the contract was signed
  - If data is compromised because of the weak security controls of your vendor – it’s your responsibility too
- Part of CI/CD
  - Security score for pull requests and reject anything below a predefined threshold. If things are on fire and the code must go through, it has to signed off by top mgmt.
- Part of CMDB / overall monitoring / automate everything
  - Identify Shadow IT and new (and unsanctioned) services
  - Constantly scan all the IP ranges and assets.
- Communicate. Communicate. Communicate.
  - Make sure people know where, how and why to reach you
  - Anything that’s not already automated should be ticket based



Tech and strategy to stay sane

- SSO everywhere – the silver bullet to managing access control & shitty passwords
  - Not everything supports SSO so additional development will be needed. Fight the good fight and outline how long term benefits outweigh the initial cost
    - Have the red team bruteforce their way into a few accounts to make a point
    - Outline the overhead on IT when decommissioning users
- CDN, WAF, Strict Origin – mitigate DDOS & Credential Stuffing
  - You won’t be able to add everything at once so make sure you prioritize
- Switch to TLP if you don’t use it already. It’s simpler and more elegant
  - TLP: RED – recipients only
  - TLP:AMBER – recipients and colleagues
  - TLP: GREEN – public domain

Vulnerability Management

- rEngine, Detectify, Nessus, Acunetix, Dependabot, Snyk
  - Also useful for spotting and mitigating shadow IT
- Research & manual Pentesting with Red Team
  - On demand (requests from other teams)
  - Proactive, Rogue mentality, Physical security, Social engineering, etc…
- Bugbounty
- Inventory and management of all vulnerabilities in JIRA & VM platform.
- Agree on SLAs with engineering
  - 24h for ACK & validation no matter the severity
  - (same) 24h for fix for P1
  - 5days for P2
  - Negotiable for P3 and lower (but still needs a roadmap)

BYOD & Conditional access

- Intune / JAMF
- AV/EDR/System updates/other checks. Pass = Identity manager lets you in
- Gradual rollout
- Communication is, again, key
- Easiest BYOD policy. Here’s the playbook – install the security tech stack and you can access resources.

A bit more blues

- Sensors! Sensors! Sensors!
  - Splunk agents in absolutely every system that supports it
    - Solve poor logging in the process and enhance your forensics capabilities
  - Netflows
  - EDR
  - WAF
  - NO MITM. It's overkill.
- Be forensics and IR ready

LEGACY. Some things you can't fix

- "It's being phased out"
  - Ask for a clear roadmap
- Isolate the service. Have the red team assess how an attacker can pivot or what can be achieved by compromising it
- Extra tooling. You're not going to put EDR everywhere. Put it here. Prioritise it for WAF & Splunk deployment.
- Have a list with things you need to keep a closer eye on

TLP:GREEN

Secure by design? No! Compromised by design

- Treat each asset (including people) as if it was already compromised
- …and with this mindset, tailor least privilege access
- Run tabletops and simulations
- Run purple team exercises
- Run phishing exercises
- BE BRUTAL! Rogue philosophy
- Max out the benefits from your red team and have them identify the main pain points to focus on
  - Most damage
  - Insufficient monitoring
  - Poor access control

TLP:GREEN

Remember: There will ALWAYS be a way to bypass any and all security measures.
Be prepared for when it happens.

To sum up…

- Compliance/Green team to align all entities (past, present and future) to the same principles
  - Make everything as easy to understand and adopt as possible
  - Internal comms
- Cloud first and phase out any “local” dependancies
- Enforce IAM and SSO
- Endpoint AV/EDR/MDM & Conditional access
- Automated vulnerability assessment for code and services
- Manual Pentesting with red team and bug bounty
- CDN, WAF, Strict Origin
- Visibility on everything
- Extra measures for legacy stuff

aws

splunk>

Azure Active Directory

slack

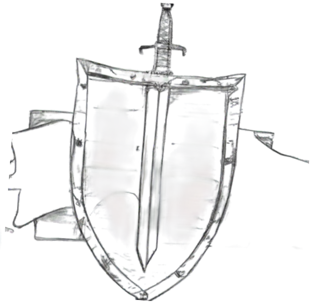
GitHub

ATLASSIAN

Microsoft 365

TLP:GREEN

Images generated with DALL-E



Q/A

alex.balan@superbet.com | security@superbet.com | superbet.ro/security.txt

Careers (red, blue, SRE, go, pretty much everything): https://happening.xyz

TLP:GREEN