clarified security

we break security to bring clarity

Red on Blue – Infinity war

@ The Future of Cyber Risk

Sille Laks
Cyber Security Expert
@v50slak

clarified security

we break security to bring clarity

- **Founded: 2011**
- **CEO: Mehis Hakkaja**
- **Employees: 17**

- **Penetration testing (WebApps & Networks & special) - ~100 applications per year**

"We break security to bring clarity" | “What can we break for you today?”| “You buy it, we break it!”

- **Hands-on Hacking Series | Web Application Security | Secure Logging | Hunt the Hacker**

- **Red Teaming for NATO CCDCoE live fire Cyber Defence Exercises (CDX) Locked Shields and Cyber Range eXercises (CRX):**
  - **2010 May, CDX10 "Baltic Cyber Shield" - 20 RT members & 6 Blue Teams**
  - **2019 April, LS19 – 77 RT members & 23 Blue Teams**
  - **2015 - … - CRXs for 1-2 Blue Teams**

- **Red Teaming on production**

  “Play for real” - adversary simulation

@Locked Shields you see the RT impact but not RT itself

- **Red Team (RT)** – Attackers
- **Blue Team (BT)** – Defenders
- **Green Team (GT)** – Infrastructure, BT systems development
- **White Team (WT)** – Communications, User Simulation, Media, Legal, Strategical, Operational
- **Yellow Team (YT)** – Situation awareness
- **Purple Team (PT)** – integrating the defensive tactics and controls from BT with the threats and vu by the RT into a single narrative

clarified security
we break security to bring clarity

Red Team

An independent group

that challenges an organization to improve its effectiveness

by taking an adversarial role.

Threat Hunting

Pro-actively searching for attack indicators & attackers that could be lurking in your network.

Always assume that you either already are or will get compromised!

Voluntarily getting attacked? But WHY?!

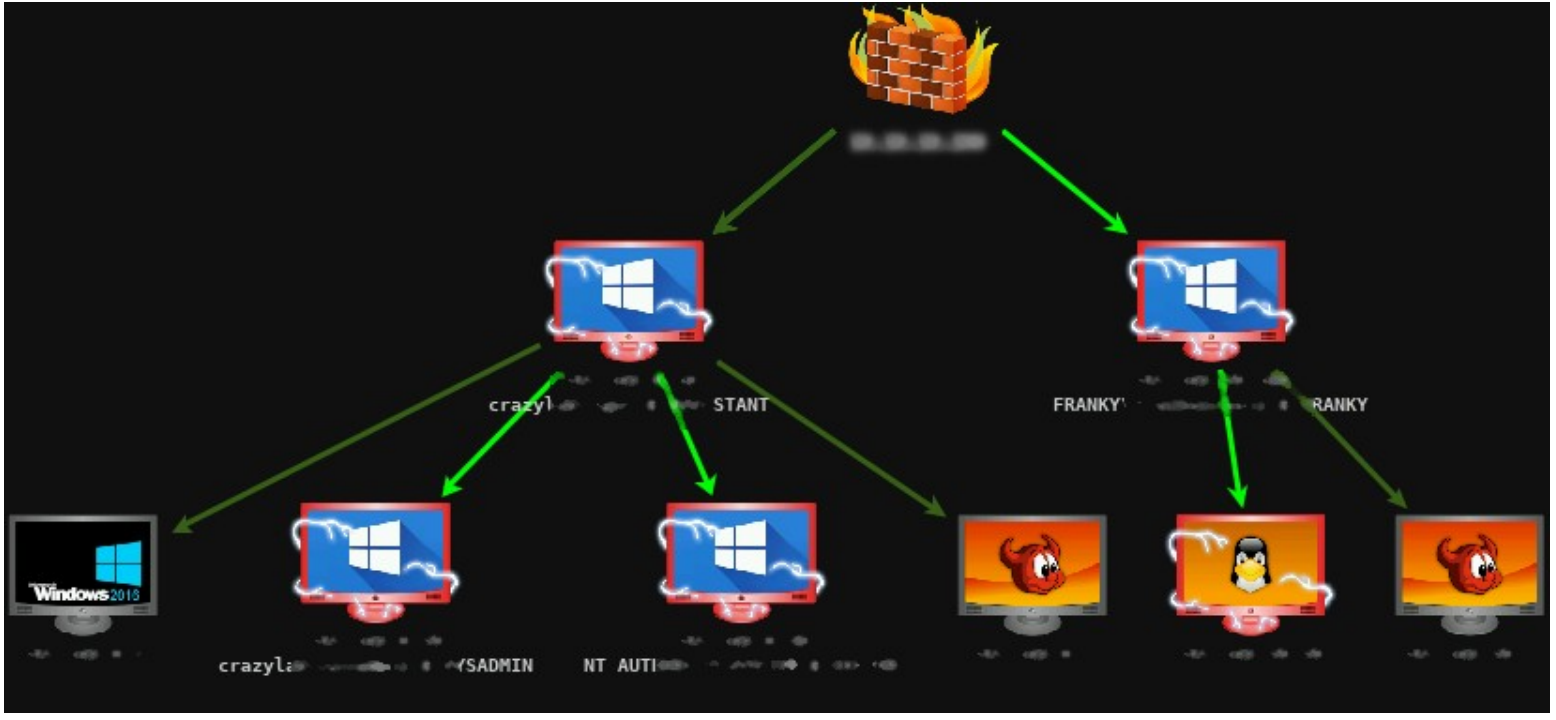
- Highlight "viable attack vectors as paths of least resistance" **against YOUR own and very real company** and its current security situation

- Your employees get the experience to detect, respond and defend as they would in case of a real incident BUT with the benefit of **comparing notes with your adversary!** Various iterations: mitigate your weak spots together with the RT:
  - replay successful attack phases (in plain sight)
  - fine-tune your detection and response
  - verify fixes and improvements
  - verify internal procedures
  - not limited to cyber only

- Iterative simulated intrusions will be cheap and effective training compared to “learning the hard way with possibility of actually losing your business gems” '

clarified security
we break security to bring clarity

Blue Teams
through
Red Team's
RDP



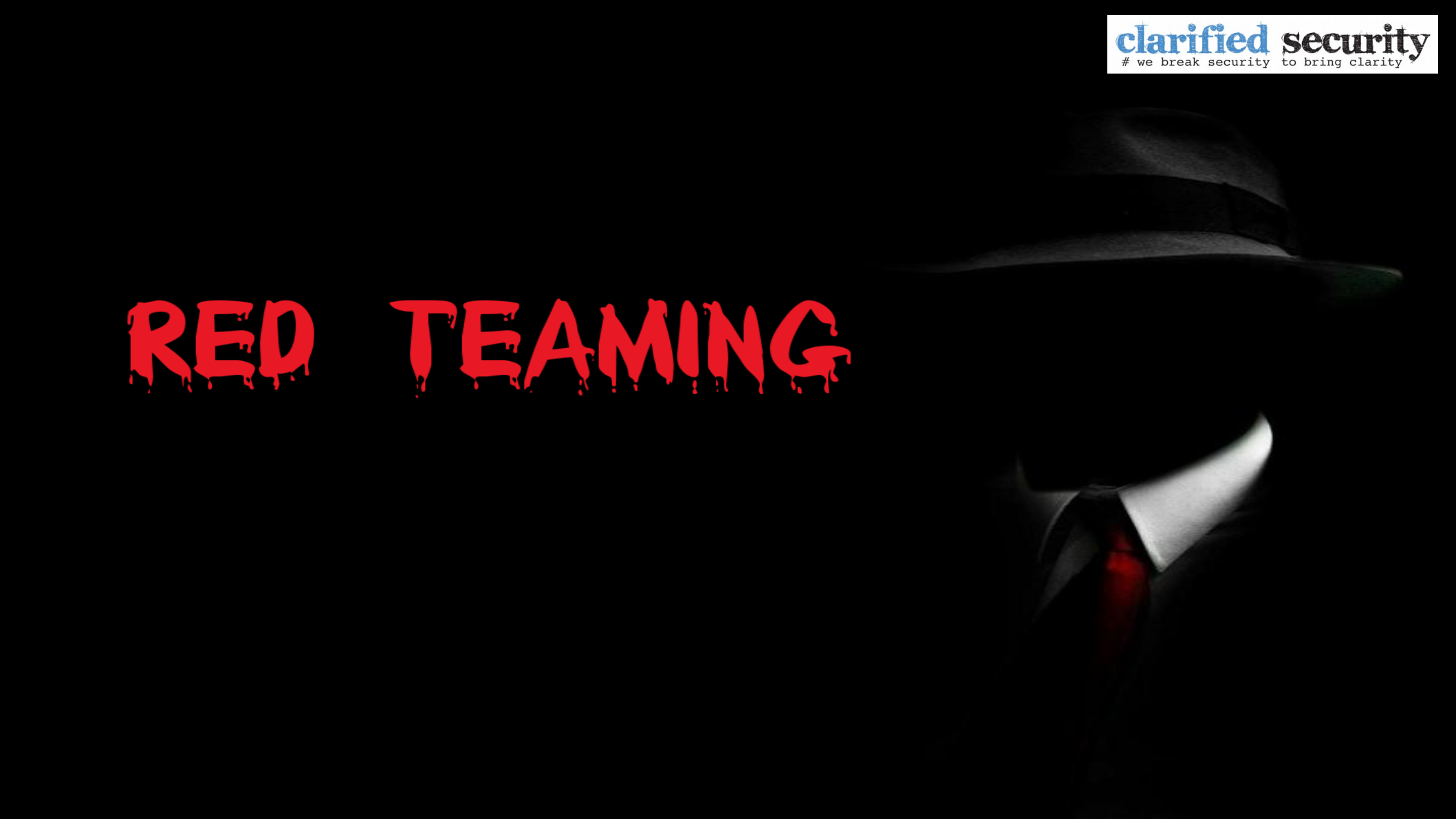
- OS?
- AV?
- Browser?
- Office?
- MFA?
- VPN?
- E-mail?
- Communication channels?
- Monitoring?

Red Teaming

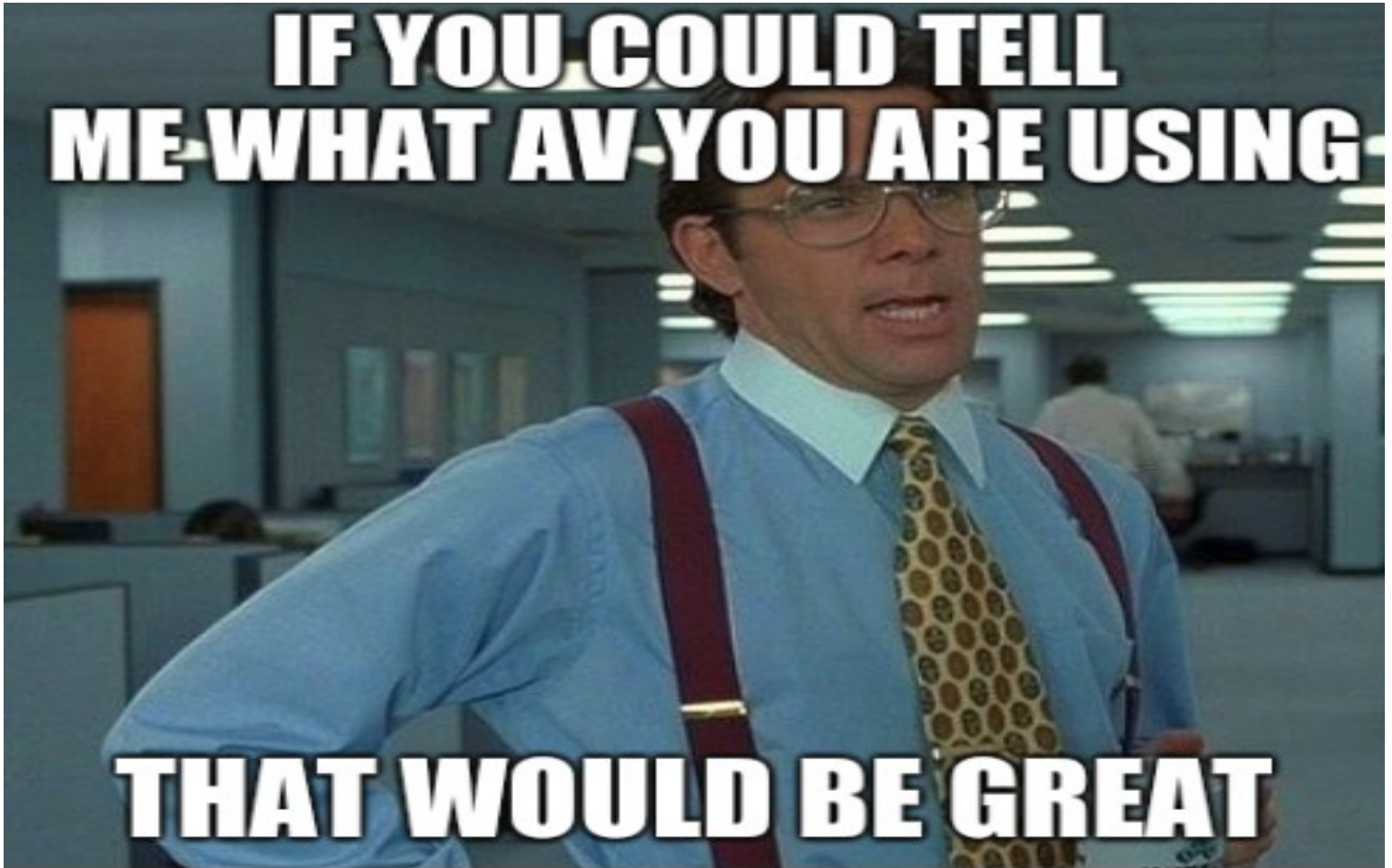
- 3-4 weeks of work, 3-4 months period
- A lot of red teams start from "*assumed compromise*"
- We prefer to execute the entire attack life-cycle:
  - *OSINT, phishing x many, (spear)phishing, watering hole & supply chain attacks*
  - *living off the land, escalation, lateral movement … **repeat** → "crown jewels"*
  - *Not limited to cyber only (depending on ROE)*
- = more realistic, more lessons learn for the whole organization

clarified security
we break security to bring clarity

RED TEAMING



If you don't know the answer - ASK



< This slideset has been modified from its original version to ensure the
continuity of successful RT on production >


ACCESS GRANTED

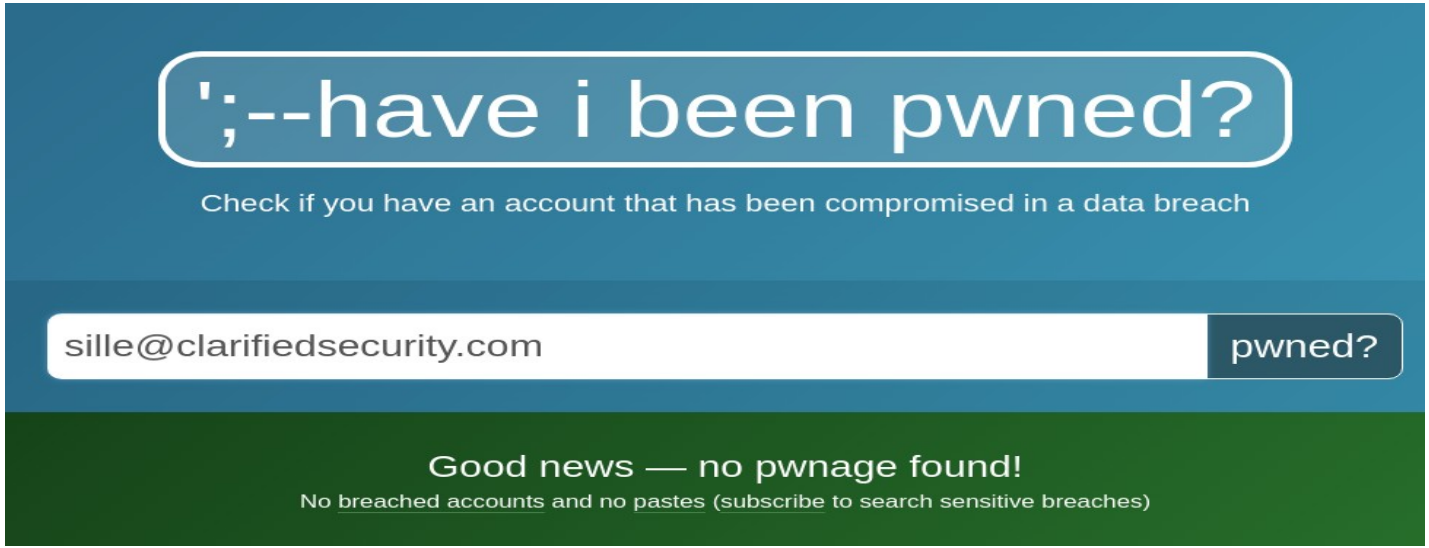
clarified security
we break security to bring clarity

The future - S in IoT stands for security

Q & A

clarified security

we break security to bring clarity



Clarified Security OÜ

https://www.clarifiedsecurity.com/

Thank you!