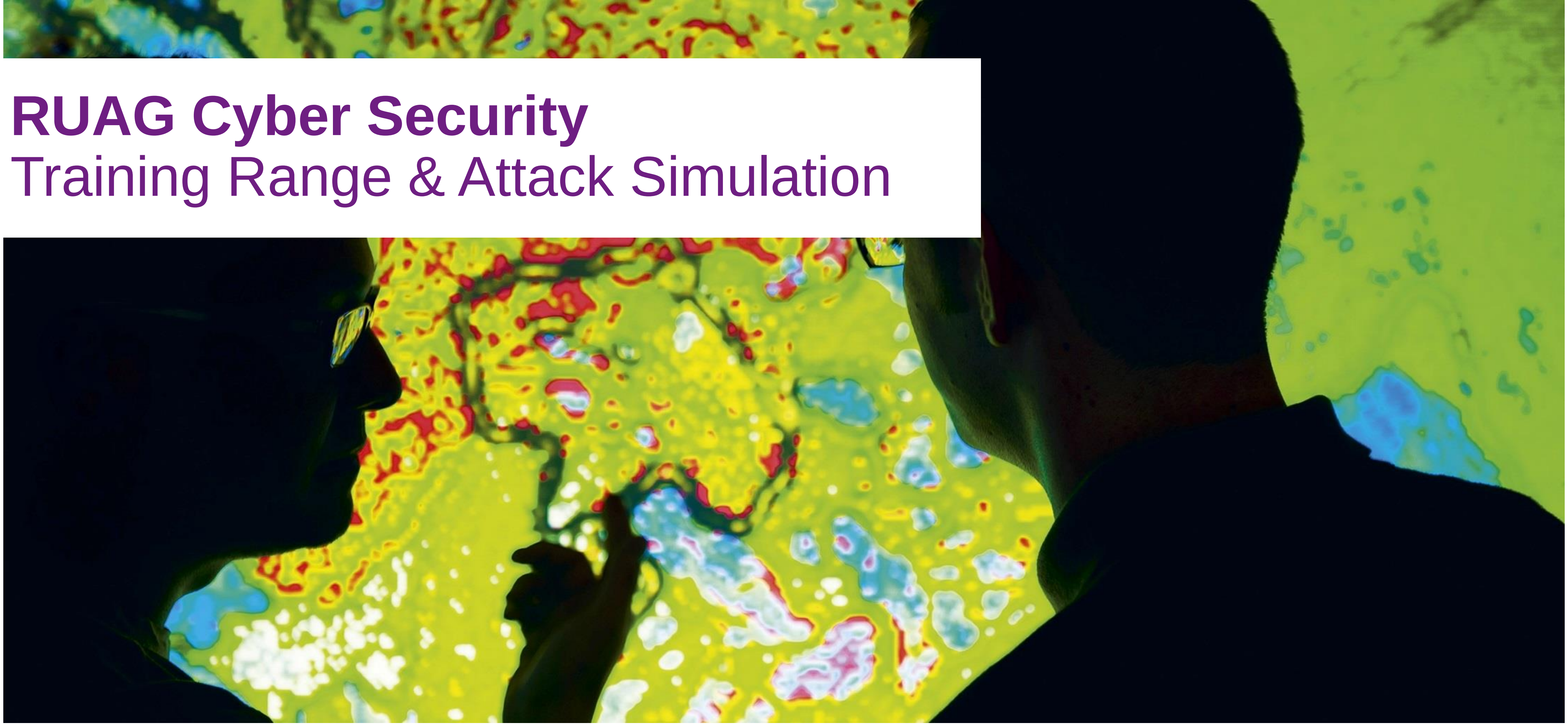


RUAG Cyber Security
Training Range & Attack Simulation

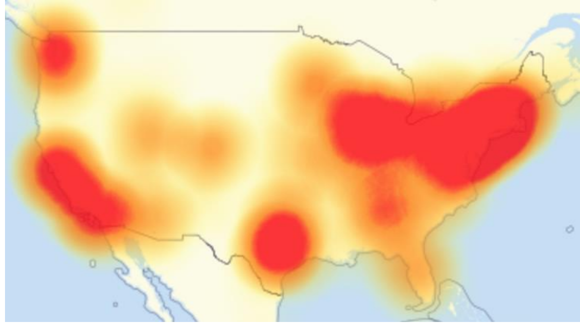
Peter Hladký
Senior Cyber Security Specialist
RUAG Defence

Together ahead. RUAG

What is the current state of affairs?

(In Cyber Security)

Recent (D)DoS Attacks and Mirai Malware



*

19 Sep 2016	**French Web Host OVH**	~1	Tbps
20 Sep 2016	**KrebsOnSecurity**	~660	Gbps
21 Oct 2016	**DNS service provider DYN**	~1.2	Tbps
03 Nov 2016	**Liberia’s Internet Infrastructure**	~600	Gbps
28 Nov 2016	**Deutsche Telekom**	~900’000 customer routers	

Attributed to Mirai malware and botnet consisting primarily of online consumer devices (IoT). [1]

* Map of areas most affected by attack. [6]

NATO / European Union / Swiss Confederation

- **9 July 2016: Warsaw Summit Communiqué, Article 70**
  “Now, in Warsaw, **we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations** in which NATO must defend itself as effectively as it does in the air, on land, and at sea.” [2]

- **6 July 2016: NIS Directive**
  The NIS Directive provides legal measures to **boost the overall level of cybersecurity** in the EU by ensuring **preparedness, cooperation**, **culture of security across sectors.** [3]

- **May 2016: Max Klaus, MELANI**
  “The nature of the attacks is **continuously evolving**. One overarching trend is that the **level of professionalism** on the attacker’s side is **increasing**.” [4]

Time to Compromise / Time to Exfiltration

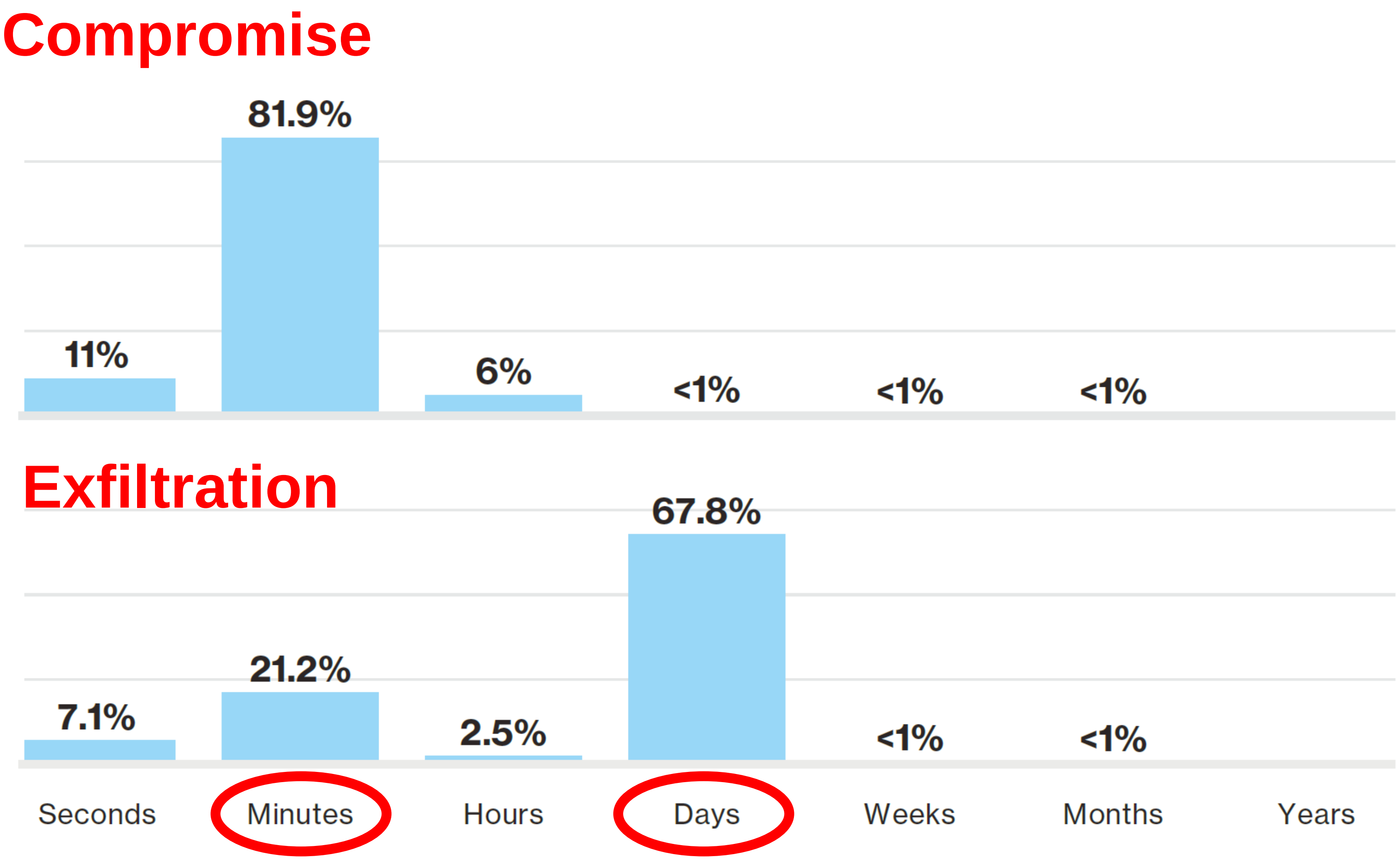
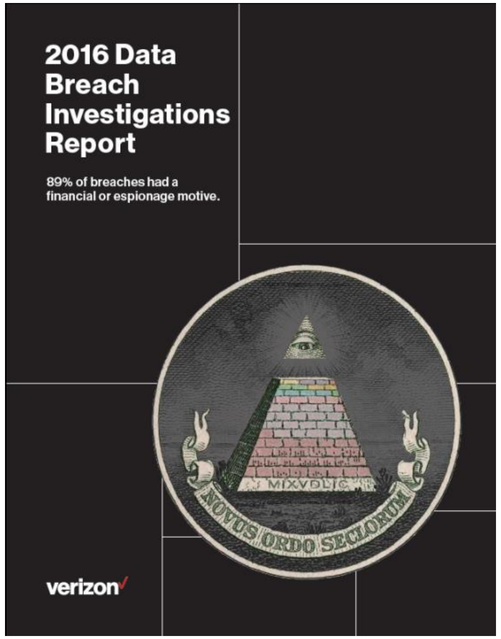


Figure 7, 2016 Data Breach Investigations Report – Verizon [5]



2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

verizon

Time to Compromise / Time to Discover

% where “days or less”

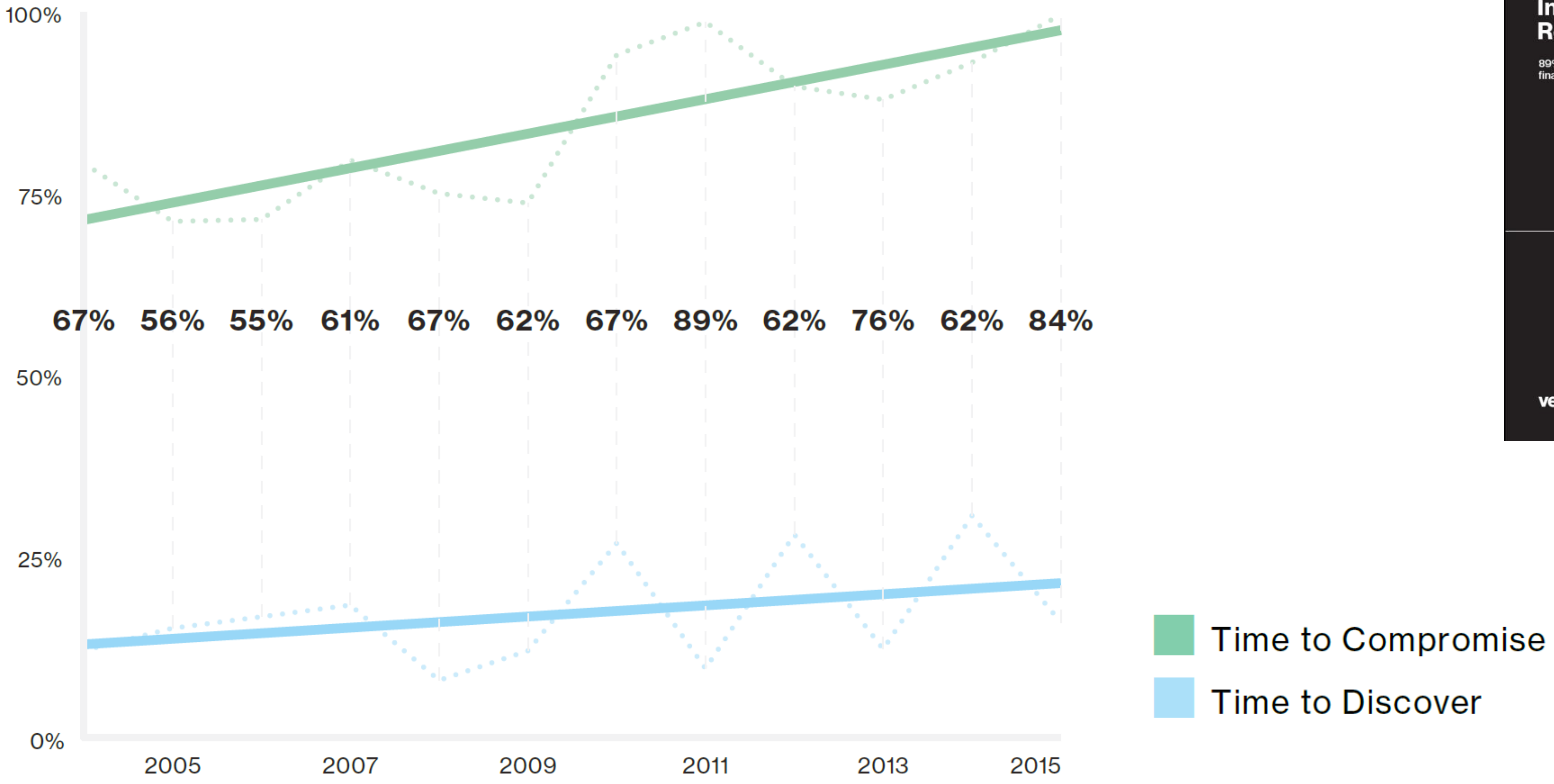
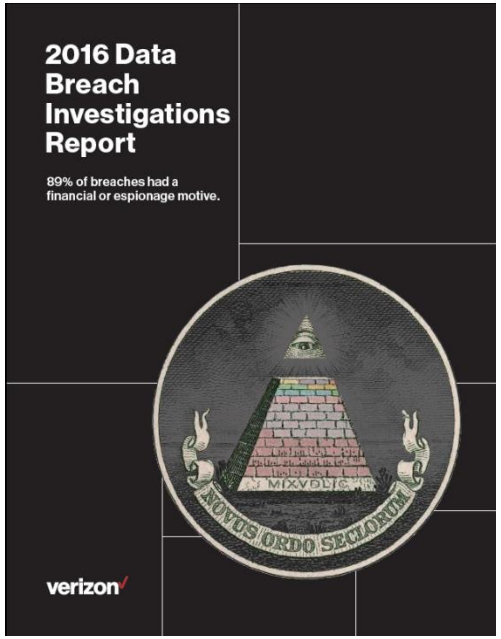


Figure 8, 2016 Data Breach Investigations Report – Verizon [5]


2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

verizon

Are we ready?

Can we do anything about it?

RUAG Cyber Training Range

Improving the Security Posture

- Education and Training for **IT/OT specialists, administrators and executives.**

- The training includes **automated**, **repeatable cyber attack simulations** in a realistic environment.

- It enables the improvement of **emergency processes** and **operational behavior.**

- Simulation of attacks on **IT & SCADA Systems.**

References:

- NATO Cyber Defence Exercise “**Locked Shields 2012**”.
- **Bootcamp for Traffic Analysis** (Banks / Telecommunications).
- Large Swiss Financial, Logistical and Transport Organizations.

Together ahead. RUAG

Training Principles

- The goal of the training is to **improve operational behavior**.
- The focus of the training is **on the organization**, not on individuals.
- We train **methods, techniques and processes**, not tools.
- Trainings are **repeatable and comparable** to measure the changes in the maturity.
- Training and scenarios are **tailored** to your business and operations.
- Training is an **ongoing process** not one occasion.
- «**Lessons Learned**» is the most important outcome of the training.
- Each training ends with the most important **recommendations**.

Together ahead. RUAG

Training Offering

Training of Executives

Improving **incident and crisis management** as well as communication during a crisis.

Tactical / Operational Training

Early **detection and reduction of impact**, technical analysis and early investigation steps.

Special Operations Training

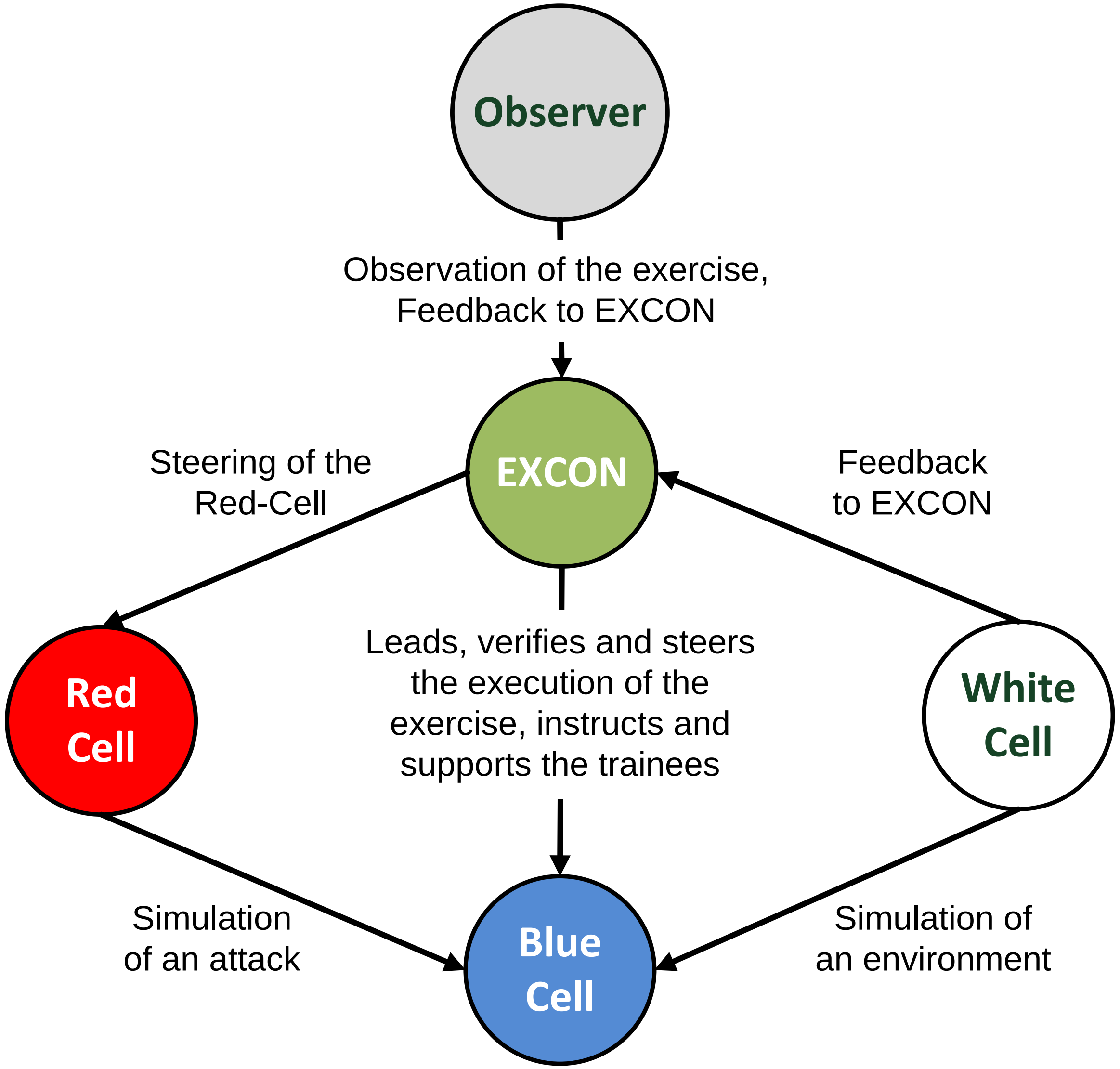
Simulation of **advanced threat actors**. Increased sophistication of simulated attacks in the areas of Information Technology (IT) and Operational Technology (OT).

Joint Training

A joint training of **executives, technical employees and specialists**.

The focus of this training is to ensure that the **cooperation between different units** functions flawlessly.

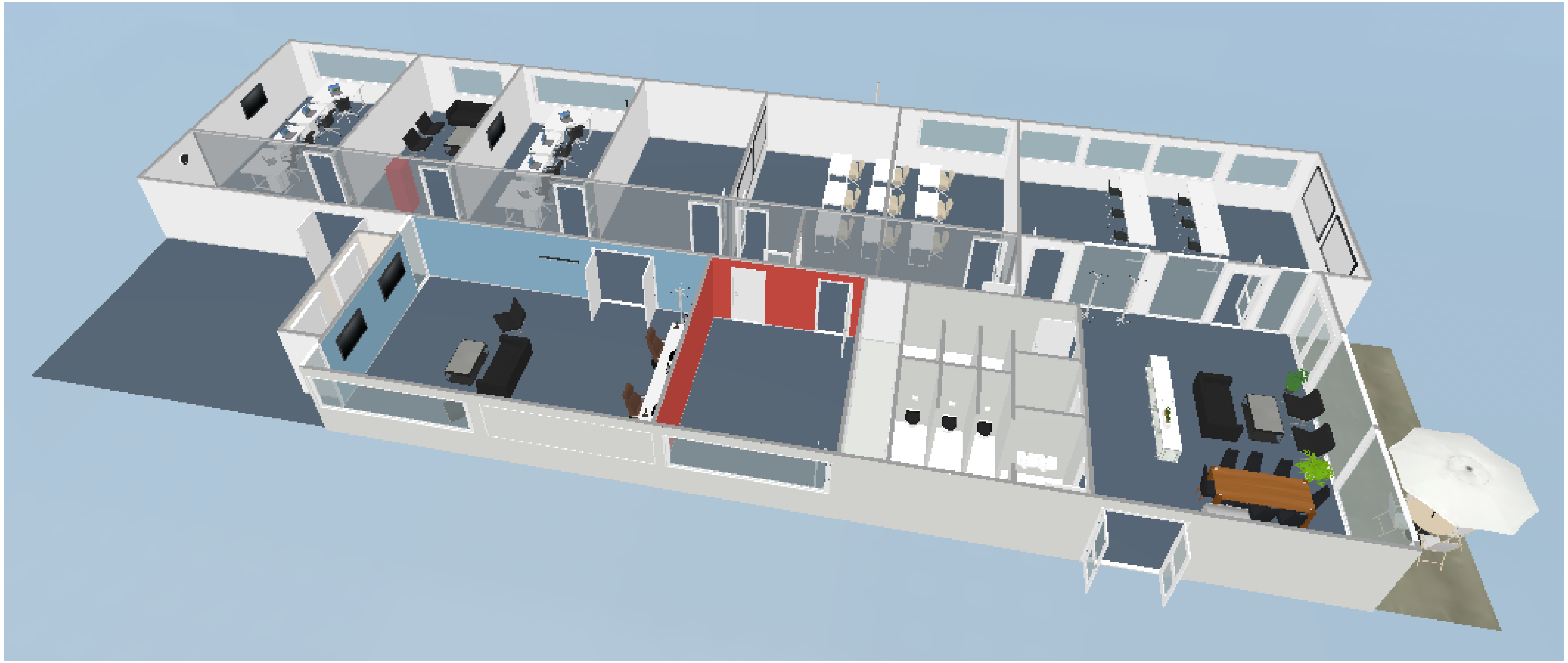
Organization, Roles and Responsibilities



Together ahead. RUAG

RUAG Cyber Security Training Range Bern

3d walk @ http://applet.roomsketcher.com/3dwalk/view/?ctxt=rs_app&pid=2171379



Main Areas of Improvements

Our Perspective

- Incident management processes are **defined, but not exercised**.
- **Communication** within **technical teams**, individual vs. team work.
- **Communication** between **technical and crisis management** teams.
- **Clarity on direction** and **delegation of tasks** by the crisis management team.
- **Documentation** of technical analysis as well as crisis management team’s decisions.

Your Contacts

Peter Hladký
Senior Cyber Security Specialist

RUAG Defence
Stauffacherstrasse 65
3000 Bern I Schweiz

Mobile +41 79 192 63 75
peter.hladky@ruag.com

Bruno Affolter
Senior Sales Manager
Cyber Security

RUAG Defence
Stauffacherstrasse 65
3000 Bern I Schweiz

Mobile +41 79 678 10 31
bruno.affolter@ruag.com

https://cyber.ruag.com

Together ahead. RUAG

References

[1] Mirai (malware)
https://en.wikipedia.org/wiki/Mirai_(malware)

[2] Warsaw Summit Communiqué, 09.07.2016
http://www.nato.int/cps/en/natohq/official_texts_133169.htm

[3] The Directive on security of network and information systems (NIS Directive), 28.07.2016
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[4] Clarity on Cyber Security, KPMG, May 2016
https://home.kpmg.com/ch/de/home/themen/2015/05/clarity-on-cyber-security.html

[5] 2016 Data Breach Investigations Report
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[6] 2016 Dyn cyberattack
https://en.wikipedia.org/wiki/2016_Dyn_cyberattack