Future is Cyber..

Where is the global cybersecurity industry going and why is it failing to protect against cyberattacks?

The Country that is not Ready for Cyber, is a Country without a Future!

Palo Alto- 2010
Future is Cyber..

The Country that is not Ready for Cyber is a Country without a Future!

Aug 2010 – Palo Alto

Stefan Uygur
### Security Standards & Frameworks

3000 Global Vendors but still...

<table>
<thead>
<tr>
<th>Framework/Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technologies</td>
</tr>
<tr>
<td>HITRUST</td>
<td>HITRUST Information Trustworthiness Framework</td>
</tr>
<tr>
<td>The CIS Critical Security Controls</td>
<td>Center for Internet Security Critical Security Controls</td>
</tr>
<tr>
<td>System and Organization Controls</td>
<td>Center for Internet Security System and Organization Controls</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Federal Information Security</td>
<td>National Institute of Standards and Technology Federal Information Security</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>Center for Internet Security</td>
<td>National Institute of Standards and Technology Center for Internet Security</td>
</tr>
<tr>
<td>Cyber Essentials</td>
<td>National Institute of Standards and Technology Cyber Essentials</td>
</tr>
<tr>
<td>Committee of SponsorIn</td>
<td>National Institute of Standards and Technology Committee of SponsorIn</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>NIST SP 800-171</td>
<td>NIST Special Publication 800-171 Information Security Controls for Federal Information Systems and Organizations</td>
</tr>
<tr>
<td>Sarbanes–Oxley Act</td>
<td>National Institute of Standards and Technology Sarbanes–Oxley Act</td>
</tr>
</tbody>
</table>
Cyber Attacks are the new Pandemic

<table>
<thead>
<tr>
<th>Amount</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$8 Trillion</td>
<td>Cost of Cybercrime by 2023</td>
</tr>
<tr>
<td>$10.5 Trillion</td>
<td>Global Crime Damage by 2025</td>
</tr>
<tr>
<td>$1.7 Trillion</td>
<td>Cyber Expenditure by 2025</td>
</tr>
<tr>
<td>$265 Billion</td>
<td>Ransomware Cost by 2031</td>
</tr>
<tr>
<td>$14.8 Billion</td>
<td>Cyberinsurance Market by 2028</td>
</tr>
<tr>
<td>$30 Billion</td>
<td>Cryptocrime by 2025</td>
</tr>
</tbody>
</table>

2023 Cyber Expenditure

$162-$188 Billion

Source: Cybersecurity ventures - Gartner - Statista
Stefan Umit Uygur - 4Securitas
Current Industry Response?

**243 Days**
Average time to identify and contain a breach

**327 Days**
Lifetime of a malicious attack from breach to containment

**€4M**
Average cost of a data breach

*Source: IBM - Ponemon Institute*
Cyber Attack Trends - Historical

Figure 2: Percentage of organizations compromised by at least one successful attack.

Source: Comparitech
New Threats - The War - A Use Case - 
Things are getting worse...

- Started with one youngster
- Main group counting members now ~91k
- Total members (includes affiliates)~450k
- Sudan joined with members ~27k
Countries with a Bright Future

Source: CyberDB

Stefan Umit Uygur - 4Securitas
Sovereignty in Cyber is a Must

Cybersecurity is the future
Industry Hype and Buzzwords

ARTIFICIAL INTELLIGENCE
A program that can sense, reason, act, and adapt.

MACHINE LEARNING
Algorithms whose performance improve as they are exposed to more data over time.

DEEP LEARNING
Subset of machine learning in which multilayered neural networks learn from vast amounts of data.

SASE Architecture
Integrated Security Framework
Modern User Provisioning
Advanced Threat Protection
Zero Trust Models

Stefan Umit Uygur - 4Securitas
ConfGARR23
So what is wrong with the industry?
The Reality - The Current Model

No matter how good the product is...
Confusion - What is proactive?

OFFENSIVE SECURITY OVERVIEW
Be Proactive against Cyber Security Threats

Predict
Prevent
Respond
Detect

NETWORK
WEB APPLICATION
MOBILE APPLICATION
INTERNET OF THINGS
SCADA

SECURITY ASSESSMENT

Stefan Umit Uygur - 4Securitas
Cyber defense in 3 simple steps

- PROTECT
- DETECT
- REACT

Unpopular
Focus/Hype
Getting there
The Ideal Cybersecurity Defense Model

**Predictive**

| Threat Hunting Intelligence | Up to 90% |

Source of attacks can be predicted. 90% of attacks are originating from:
- Anonymous networks
- Bad reputation IP addresses
- Known C&C bad URLs
- Known malware signatures
- more known sources

**Proactive**

| While Planning the attack | Up to 98% |

The only way to break in:
- Information gathering
- Reconnaissance

**Reactive**

| While attack is in progress | 2% |

Where the industry focus is!!
Thank You!

Stefan Uygur

stefan@4securitas.com