AI. READY? GO!

Sergej EPP
Chief Security Officer, Central Europe
NETWORK ENGINEERS VS HACKERS

ROUND 1
<table>
<thead>
<tr>
<th>Acute</th>
<th>Severe</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected vehicle</td>
<td>AI voice fraud</td>
<td>AI Exploit Fuzzing</td>
<td>Supervisory Oversight</td>
<td>Advanced regulations</td>
</tr>
<tr>
<td>(air/rail/car) threats</td>
<td>AI phishing</td>
<td>AI Malware Gen.</td>
<td>BYOD threats</td>
<td></td>
</tr>
<tr>
<td>Quantum computing</td>
<td>AI chatbots</td>
<td></td>
<td>Cryptojacking</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data exfiltration in</td>
<td>Firmware implants</td>
<td>Biometrics loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the cloud</td>
<td>Destructive threats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID mass blackmailing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OT/IoT Threats</td>
<td>CEO Fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insider Threat</td>
<td>Compromised patch control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Crimeware-as-a-service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Third Party Threat</td>
<td>Spyware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identity theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ransomware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virus</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Impacts:**

- Acute
- Severe
- High
- Medium
- Low

**Impacts:**

- Emerging
- Unlikely
- Possible
- Likely
- Very Likely

**Risks:**

- Connected vehicle (air/rail/car) threats
- Quantum computing
- Data exfiltration in the cloud
- Cyber Hygiene
- AI voice fraud
- AI phishing
- AI chatbots
- Firmware implants
- Destructive threats
- ID mass blackmailing
- OT/IoT Threats
- Insider Threat
- Third Party Threat
- Spyware
- Identity theft
- Ransomware
- Virus
- AI Exploit Fuzzing
- AI Malware Gen.
- Biometrics loss
- CEO Fraud
- Compromised patch control
- Crimeware-as-a-service
- Phishing
- Supervisory Oversight
- BYOD threats
- Attack obfuscation
- Denial of Service
- Banking Malware
- Advanced regulations
- Cryptojacking
- Emerging
- Unlikely
- Possible
- Likely
- Very Likely

**Matrix:**

- Acute
- Severe
- High
- Medium
- Low

**Legend:**

- Emerging
- Unlikely
- Possible
- Likely
- Very Likely

**Impact Levels:**

- Acute
- Severe
- High
- Medium
- Low
ROUND 3

ROBOTS
SECURITY LIFECYCLE

- Detection
  - Burden to triage
  - Costs of false negative

- Prevention
  - Interability of alerts
  - Often EDR limited
  - Highly time-intensive

- Response
  - Enforcement
  - Feedback Loop

Constantly changing environment
„I will fix your detection problems“
- AI
INTRODUCTION INTO MACHINE LEARNING

Traditional Programming

INPUT DATA
PROGRAM
OUTPUT DATA

Machine Learning

INPUT DATA
OUTPUT DATA
PROGRAM

Reference: Prof. Domingos
HOW TO GET EFFECTIVE TRAINING DATA?

1. Use public dataset
2. Review incidents
3. Use Honeypots
4. Run Red Team Exercises
5. Cross-organizational telemetry
BEISPIEL: SPAM
IT’S A TEAMSPORT!
1. CREATE TRUST FOR CLOUD SECURITY PRODUCTS
INTERABILITY OF ALERTS
COMPREHENSIVE ANALYSIS

THREAT INTELLIGENCE
- MalwareTags
- Indicators
- File Activity

UEBA
- HTTPS
- office365.com

CLOUD SECURITY

EDR
- malware.exe

ACTIVE DIRECTORY
- Bob

NTA
- Unknown domain
- Hosted in Canada
2. ESTABLISH RICH DATA VISIBILITY
EXAMPLE: THREAT INTELLIGENCE

Indicators

ExploitKits, Scanning IPs

C2 IPs

APT IPs

Signatures

Block list

Quarantine list

Alert list

Firewall

Notify user

Move to quarantine network

Analyze device

Rebuild device

Sandbox

AI: beaconing

User

Violation

SHARING
3. AUTOMATE YOUR SECURITY PLAYBOOKS
IT’S SURVEY TIME

“How many security tools do you use in your organization?”

100

50

30
4. REVIEW YOUR POINT PRODUCTS
MY PLAN FOR CYBERHYGIENE AND FOCUS ON WHAT MATTERS

30 Days
Create inventory for security products and rate them on
- Penetration level across network, endpoint, cloud
- Prevention maturity
- API maturity
- Crowd intelligence

90 Days
- Introduce SecDevOps for key products and validate recommendation from your inventory
- Create a plan and share with vendors

270 days
Rationalize security products