Collaboration in the Cyber Security Defence

Oscar Koeroo – Security advisor
KPN CISO :: Strategy & Policy
“To keep KPN reliable and secure and trusted by customers, partners and society”
Why We Need To Transform
From a Telecom Operator into an “Integrated Connectivity Provider”

Content Drives Customer Value…
…unfortunately not Telco Value

Voice Dominates

Data Dominates

Customer Revenues
& Operator Traffic Decoupled

Traffic Volume

Customer Revenues

Time

Value

TCO

NPS

…unfortunately not Telco Value
Transformation Through Technology
Organization, way of working, services and cost structure

Transforms into

Using Software Defined Networking and Network function Virtualization architecture

Agile / OTT like player
Telco unlike Customer Service
TCO < 50% / Quality > 2x
Attacks can’t always be prevented. Focus on detection and proper resolution.
## Different type of attackers

<table>
<thead>
<tr>
<th>Actors</th>
<th>Motivation</th>
<th>Threat vector</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Individual Hacker | − Opportunistic  
| (KPN 2012) | − Disenfranchised | − Opportunistic vulnerabilities  
| | | − Insider | − Integrity of systems and data  
| | | | − Reputational and Brand loss  
| | | | − Regulatory |
| Hacktivists | − Targeted  
| (ZIGGO ATTACK, Panama Papers) | − Ideological  
| | − Political cause | − Compromise of 3rd Party & Service Provider  
| | − Malicious havoc | − Volume, Targeted attack  
| | | − Opportunistic vulnerabilities | − Disruption of operations  
| | | | − Defacement of public sites  
| | | | − Reputational and Brand loss |
| Cyber Criminal | − Illicit gain  
| (Talk, Talk, $1bn Carbanak) | − Fraud  
| | − Identity Theft | − Insider  
| | − Competitive Intelligence | − Data Breach  
| | | − Intellectual Property theft | − Customer Privacy  
| | | | − Financial impact  
| | | | − Intellectual Property loss |
| State Actor | − Geopolitical target  
| (Belgacom, SONY) | − National Security gain  
| | − Disrupt others Critical Infra | − Advance Persistent Threat (time/assets)  
| | − Economic Espionage | − SCADA/ ICS  
| | | − 3rd Party & Service Provider | − Critical Infra damage  
| | | | − Intellectual Property theft  
<p>| | | | − Economic &amp; Political destabilization |</p>
<table>
<thead>
<tr>
<th>MONTHLY BRONZE</th>
<th>MONTHLY SILVER</th>
<th>MONTHLY DIAMOND</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>19.99$</strong></td>
<td><strong>24.99$</strong></td>
<td><strong>29.99$</strong></td>
</tr>
<tr>
<td>☎️ XyZ Public Network</td>
<td>☎️ XyZ Public Network</td>
<td>☎️ XyZ Public Network</td>
</tr>
<tr>
<td>☐ 250Gbps Network Capacity</td>
<td>☐ 250Gbps Network Capacity</td>
<td>☐ 250Gbps Network Capacity</td>
</tr>
<tr>
<td>☐ 27 Attack Methods</td>
<td>☐ 27 Attack Methods</td>
<td>☐ 27 Attack Methods</td>
</tr>
<tr>
<td>☐ 1800(s) Stress Time Per Attack</td>
<td>☐ 2400(s) Stress Time Per Attack</td>
<td>☐ 3600(s) Stress Time Per Attack</td>
</tr>
<tr>
<td>☐ 1 Months Membership</td>
<td>☐ 1 Months Membership</td>
<td>☐ 1 Months Membership</td>
</tr>
<tr>
<td>☐ 1 Concurrent attacks</td>
<td>☐ 1 Concurrent attacks</td>
<td>☐ 1 Concurrent attacks</td>
</tr>
</tbody>
</table>

[REGISTER](#) [REGISTER](#) [REGISTER](#)
100k IP-cameras infected with MIRAI
IoT
Attack surface expansion

- Increased deployments
- Highly diverse build quality
- Low/no physical security
- Hyper connectivity
How we look at ourselves: security monitoring at a SOC
The world can observe your weaknesses in detail

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Use Shodan to monitor your network and ensure that it is secure from potential threats.

Get a Competitive Advantage

Stay ahead of your competitors by knowing what your opponents are doing on the Internet.
Why you need Threat Intelligence
Incident Response process

Response Capability

Triage → Analyse → Respond → Eradicate → Recover

Knowledge → Analysis → Insight → Processing → Information → Collection

Threat Intelligence
Threat Intelligence architecture

- CERT incidents
- Extract Intel
- CERT analyst
- Analyse Intel
- Third party intel

- Big Data
- Feed DB
- MISP

- Input Intel
- Enrich Intel
- Export Intel
- Enrich

- Trusted Sharing

- VirusTotal
- Shodan
- ThreatCrowd
- ThreatMiner
- Malwr
- ShadowServer
- MISP
- Honeypots
- …
The attackers are not rapidly changing their techniques. They do return more often and improve existing skills.

- Proper forensic analysis can take weeks
- Attackers can hide their tracks
- Attackers can disrupt with easy attacks
- Attackers are agile
What we wish to have in our future network

• (Plan) Sharing information with peers in a standardized and structured way
  • STIXX, TAXII, CyBox to share (contextual) information and IoCs
• (Do) Take a decision on what to do.
  • Templated or semi-automated
  • Keep human control in the automated loop
• (Do) Fitting countermeasure deployment in our network
  • FlowSpec/filter, scrub, null-routing, or other
  • Reconfiguration of the network
  • Dynamically add different monitoring for analyses
  • Adaptive segmentation
• (Check) Verify effectiveness
MONEYBALL
BASED ON A TRUE STORY
ORIGINAL MOTION PICTURE SOUNDTRACK
MUSIC BY MYCHEL DANN
FIGHT FOR THE USER