PLATZHALTER:
Intro Film SOC

Neu von mBox
Prevention is no longer enough...
Who can detect whether an attacker has already infiltrated your infrastructure in 24/7?

Managed cyber defense with innovative SOC operation

Comprehensive use case library out of all industries
We run Europe’s largest integrated Cyber Defense and Security Operation center in Bonn

1. Master CDC + SOC
2. Magenta heartbeat for cyber security “Made in Germany”
3. Central incident coordination, Threat-Intelligence, Forensic
4. Collaboration of all SOCs (Darmstadt, Kiel, Bad Kreuznach, Leipzig, Prague, Košice, Budapest, Vienna, Madrid, Johannesburg/Cape Town, Singapore (coming soon))
5. 240 Cyber Security Professionals
6. Use cases out of each industries
PLATZHALTER:
40 Sekunden Film SOC

Neu von Nordisch
integrated CDC + SOC: One Platform for all Customers

In total > 70

Threat intelligence / Threat Hunting / Forensic

SOC + SIEM Tools

Corporation 1
Corporation 2

DAX

Corporation 1
Corporation 2

Linde Group

Corporation 1
Corporation 2

SME

Corporation n

Telekom

DAX

Corporation 1

Linde Group

SME

Corporation 1

LIFE IS FOR SHARING.
BENEFIT from our Self-Learning / SELF-IMPROVING platform

Strict data separation
Data exchange between clients is impossible!

Knowledge-Transfer: All clients benefit automatically and immediately from new insights into types of attacks!
demand for complete Outsourcing Security Operation

- Security Operation Center
- 24 / 7 / 365
- 16 / 5 / 365
- Optional: De-only Resources
- Otherwise: Mix De / Nearshore

Prevent
- Policy Auditing
- Vulnerability Scanning
- Mobile/Endpoint Protection
- Anti-SPAM
- Firewall
- Security Gateway

Detect
- Consulting
- Reporting
- Service Management
- Threat Intelligence
- SIEM
- IDS / IPS
- Advanced Threat Protection
- Endpoint Detection & Response
- Threat Hunting

Respond
- CERT
- Incident Response
- IT Forensics
- Malware Analysis
- Incident Coordination

Security Outsourcing

LIFE IS FOR SHARING.
DDOS Protection
APT Protection
PLATZHALTER: VIDEO

Mobile Protection
Fraudulent Domain Monitoring

No suspicious domain found yet.
Last Line Of Defense / Database Activity Monitoring

**DAM Alert Severity per Day**
- Graph showing the amount of alerts per day for Low, High, and Medium severity.

**DAM Agent - Amount of Connection of all Agents**
- Graph showing the amount of connections over time.

**DAM Agent - Amount of Throughput of all Agents**
- Graph showing the throughput over time.

**DAM Alerts - Severity Split**
- High Severity: 156
- Medium Severity: 82
- Low Severity: 23

**DAM Alert - Open Alerts List**

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Severity</th>
<th>Alert Name</th>
<th>Alert Time: Descending</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>205,045</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 23:00:10.000</td>
<td>1</td>
</tr>
<tr>
<td>205,044</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 23:00:28.000</td>
<td>1</td>
</tr>
<tr>
<td>205,043</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 22:59:02.000</td>
<td>1</td>
</tr>
<tr>
<td>205,042</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 22:00:02.000</td>
<td>1</td>
</tr>
<tr>
<td>205,041</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 22:00:02.000</td>
<td>1</td>
</tr>
<tr>
<td>205,039</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 22:00:29.000</td>
<td>1</td>
</tr>
<tr>
<td>205,038</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 20:00:25.000</td>
<td>1</td>
</tr>
<tr>
<td>205,037</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 20:00:21.000</td>
<td>1</td>
</tr>
<tr>
<td>205,036</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 20:00:01.000</td>
<td>1</td>
</tr>
<tr>
<td>205,033</td>
<td>Medium</td>
<td>DTAG - Suspicious user behavior</td>
<td>October 8th, 2018, 18:19:12.000</td>
<td>1</td>
</tr>
</tbody>
</table>
MONITORING OF Leaked Credentials
Company Usernames and Passwords

Leaked Credentials are a RISK for the Company

peter.schmidt@company-group.com
dfernando.torres@group.com.mx
verena.heise@group.com
veronica.dubio@group.com
vincent.sprint@group.com
vincent.eye@group.de
vladmir_jir@group.ru
vlasta.walesa@group.com
flex.dominus@group.com.hk
voskov@group.ua
francesco.pecunia@group.com
frederic.pferd@group.de
brit.obst@group.com
peter.pan@group.com
winnie.puh@group.com.hk
patric.leclercgh@group.com
steve.wurst@group8.com
jay.kim@group.com

peter_200
lmm98f
lon2013mdx
dubio416
marseille1
puiseaux
bestgroup
rudhila1958
kugivri
wangping
voskovf234
m4rc3114
600000
joebbooth
hakansson80
oop71/ooop
leqlerc2002
misawa72
co0larch

Deutsche Telekom
Credential Leakage Monitoring

1. Daily Monitoring of typical internet sources for Leaked Credentials
   (Pastebin, ...)
2. Trigger: Customer related domains incl. Subsidiaries
   (e.g. ttelekom.de)
3. Data Sanitization, REMOVAL of DUPLICATES
4. 24/7 Monitoring on 57 different Sources, Own Crawler technology,
   ADHOC Alarming (TICKET) or Daily Report
5. STATISTICAL Analysis comparing to other companies (anonymous)

Search on March 2019 revealed
512 leaked accounts
New dimension of targets

Comprehensive protection established:

- Corporate Networks
- Industrial Networks
- Connected Car
- Autonomous Driving Infrastructure

Photocredit: PublicDomainPictures, 127071, geralt, wasimkhanssrk, pexels, Pixabay
In the future, Every car needs to be protected like a corporate network

1. Advanced Security Hub necessary for every car
2. Secure in-vehicle network
3. Secure E2E connection to datacentre/cloud
4. Secure identity for each car
5. Security analytics on automotive data
6. Central Car-SOC for Europe
7. Honey-Cars to collect attack data & new threats
Autonomous Driving: “Everycar connectivity“ needs “everything security“
European Car-SOC is Necessary

<table>
<thead>
<tr>
<th>CAR-SOC Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
</tbody>
</table>
How you Could benefit from more than 20 years of expertise in cyber security

- 1,500 cyber security professionals
- Europe’s largest integrated CDC and SOC
- Zero Impact approach
- Security by Design based
- Different attack vectors out of all industry sectors
- Same high professional tools like in internal use
- One of the largest threat intelligence databanks
- Security and data privacy made in Germany
T-Systems
Let’s Power higher performance!

Connectivity
Digital
Cloud & Infrastructure
Security

Ready for 5G, Designed for Security, Digital and Scalable

LIFE IS FOR SHARING.
Key Take-Aways

1. Cyber Security - Knowledge & Experience is the Biggest USP
2. Self-learning system as the key to success
3. Security is for sharing
4. Vision: AI Of the defender levers out the AI of the attacker
5. We Create ...
WE CREATE THE ARMY OF THE GOOD GUYS!
PLATZHALTER:
Outro Film SOC

Neu von mBox