User Threat Detection
The next level of IT Security

Ransomware reverse Engineering durch Endpoint Monitoring
Company overview

Company Background:

- Enterprise People Analytics (solving Security, HR & IT problems)
- Global company with 15 years solving Insider Threat

Some of our Customers:
Andreas Kunz
Channel Manager DACH & EE

Dtex Systems (EMEA)
19 Eastbourne Terrace
Paddington, London
W2 6LG
United Kingdom

T: +49 (0) 7243 35426970
M: +49 (0) 1522 1949601
F: +49 (0) 7243 35426979

andreas.kunz@dtexsystems.com
http://dtexsystems.com
USERS ARE THE KEY

People account for **90% of all security incidents** with confirmed data breaches.

2015 Verizon Data Breach Investigation Report

60 percent of all attacks were carried out by insiders.

2016 X-Force Research Cyber Security Intelligence Index
IN THE NEWS

ComputerWeekly.com Sage data breach underlines insider threat

theguardian Ofcom tackles mass data breach of TV company information

InformationWeek DARK Reading Ex-Cardinal Exec Jailed For Hacking Astros

THE WALL STREET JOURNAL. FBI Suspects Insider Involvement in $81 Million Bangladesh Bank Heist
THE NEW ENTERPRISE

Cloud Applications

Cloud Hosting

Millennials Intolerant of Lock & Block

Work from Home

Work from Coffee Shop

Mobile

BYO Devices

Colocations
THE NEW ENTERPRISE

Cloud Applications

Cloud Hosting

Work from Home

Colocations

Work from Coffee Shop

Millennials Intolerant of Lock & Block

BYO Devices

Mobile

THE ENDPOINT: THE ONLY WAY TO SEE USER BEHAVIOR

Thousands of patterns of known bad behavior

Advanced analytics to find new and unknown attacks

Scalable endpoint collector focusing on metadata

Integrate into your existing systems and process
THE DTEX USER THREAT PLATFORM

USER FLIGHT RECORDER
Scalable Online & Offline

PRIVACY COMPLIANCE
Anonymization Regulatory Exp.

EXPERT LIBRARY
5,000+ patterns Known-bad Behavior

USER BEHAVIOR
Anomalies Auto-learn behavior

ALERTS & HUNT
Dashboard SIEM Integration

EXPERT ANALYSTS | Training | Threat Assessments
DTEX FINDS WHAT OTHERS MISS

**MALICIOUS USERS**
- Creative Data Theft
- Obfuscation & Covering Tracks
- Bypassing Controls
- On and Off Network
- Flight Risk

**NEGLIGENT USERS**
- Online File Sharing
- Webmail
- Pirated Media and Applications
- Gambling

**CREDENTIAL THIEVES**
- Unusual Data Aggregation
- Privilege Escalation
- Lateral Movement Tools
- Ransomware
USER THREAT ALERTS
RANSOMWARE
Ransomware reverse engineering

1. Bekannte Dateienendungen / Filenames von Ransomware

<table>
<thead>
<tr>
<th>Time</th>
<th>Device_Name</th>
<th>User_Name</th>
<th>Activity_Type</th>
<th>Source_File_Name</th>
<th>Source_File_Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 16th 2016, 11:55:03.105</td>
<td>WORKGROUP\WIN-NQUVG50U4H7</td>
<td>WIN-NQUVG50U4H7\JOHN</td>
<td>FileCreated</td>
<td>21E41BF2ADFA198B453C6A1480CA81AC</td>
<td>.locky</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Device_Name</th>
<th>User_Name</th>
<th>Activity_Type</th>
<th>Source_File_Name</th>
<th>Source_File_Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 16th 2016, 14:07:02.927</td>
<td>WORKGROUP\WIN-NQUVG50U4H7</td>
<td>WIN-NQUVG50U4H7\JOHN</td>
<td>FileCreated</td>
<td>_locky_recover_instructions</td>
<td>.txt</td>
</tr>
</tbody>
</table>

2. Wo kam die Ransomware her?

<table>
<thead>
<tr>
<th>Time</th>
<th>User_Name</th>
<th>Device_Name</th>
<th>Network_Destination_IP</th>
<th>Network_Host_Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 16th 2016, 09:05:01.221</td>
<td>WIN-NQUVG50U4H7\JOHN</td>
<td>WORKGROUP\WIN-NQUVG50U4H7</td>
<td>112.78.2.153</td>
<td>443</td>
</tr>
</tbody>
</table>

Bei bereits bekannten Ransomware-Samples erkennt Dtex auch den jeweiligen Hash von bekannten Ransomware-Dateien und ausführbaren Dateien.
Merkmale
# USER THREAT ASSESSMENT

---

**DTEX INTERNAL RISK ASSESSMENT: CUSTOMER**

This Internal Risk (IR) Assessment report is based on metadata collected from Tuesday, December 1, 2015 until Thursday, December 31, 2015. The metadata covered 209 users over 237 endpoints.

In this assessment, Dtex generated almost 7x the number of high risk alerts vs. those we’ve observed in other, tightly controlled environments. Customer would benefit from a program of activity monitoring, user education, and better control improvements.

## KEY FINDINGS

<table>
<thead>
<tr>
<th>Area</th>
<th>Risk Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Theft Risk via Cloud or USB</td>
<td>SEVERE</td>
<td>63 User(s)</td>
</tr>
<tr>
<td>Security/Hacking Tool Usage</td>
<td>HIGH</td>
<td>5 User(s)</td>
</tr>
<tr>
<td>High Risk Account Usage</td>
<td>MODERATE</td>
<td>2 User(s)</td>
</tr>
<tr>
<td>Inappropriate Internet Usage</td>
<td>MODERATE</td>
<td>6 User(s)</td>
</tr>
<tr>
<td>Software or Media Piracy</td>
<td>MODERATE</td>
<td>15 User(s)</td>
</tr>
</tbody>
</table>

## RISK LEVELS

- **SEVERE**
  - 35% of Users
- **HIGH**
  - 5% of Users
- **MODERATE**
  - 1% of Users

---

**RISK PROFILE:**

- Customer - Risk Profile Score: 2.3
- Dtex Baseline Daily Rate of High Risk Alerts per 1,000 Users: 16.8

**46% OF USERS**

Users with Moderate or above Alerts
Vielen Dank für Ihre Aufmerksamkeit