



User Threat Detection
The next level of IT Security

Ransomware reverse Engineering durch Endpoint Monitoring
Cologne – 3.November 2016

Company overview



Company Background:

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

Some of our Customers:



DACH & EE

Andreas Kunz

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



2015 DATA BREACH
INVESTIGATIONS REPORT

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
DARKReading

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



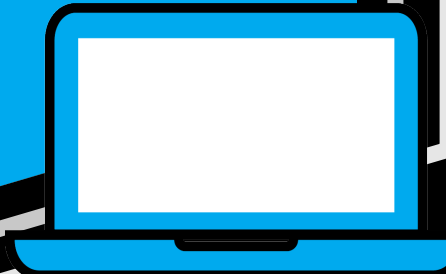
Work from Home



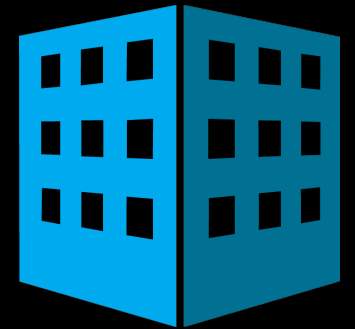
Work from Coffee Shop



Mobile



BYO Devices



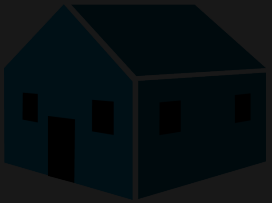
Colocations

Cloud Applications

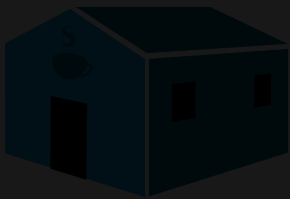
Cloud Hosting



Thousands of patterns of known bad behavior



Advanced analytics to find new and unknown attacks



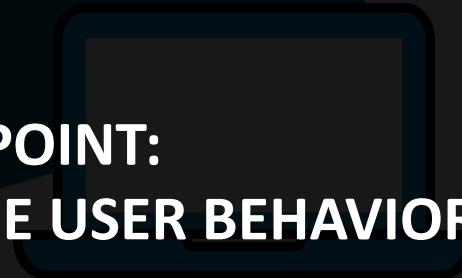
Scalable endpoint collector focusing on metadata



Integrate into your existing systems and process



**THE ENDPOINT:
THE ONLY WAY TO SEE USER BEHAVIOR**



THE DTEX USER THREAT PLATFORM



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



dtex ≡

GLOBAL THREATS

- Threat Overview
- Alerts**
- Explore
- Dashboards >

HEALTH MONITORING

- Endpoints

DASHBOARD SETTINGS

Alerts

user_risk_score:>500 70 hits

User	Occurred	User Score	Severity	Category	Score	Detected
<input type="checkbox"/> Josh Smith	350 Yesterday	High Urgent High	Known Ransomware Extension Known Ransomware Command & Control Unusual File Delete Activity	70 100 60		

Process_Name:(dropbox): 7520

Source_File_Directory:(dropbox): 7268

Destination_File_Directory:(dropbox): 688

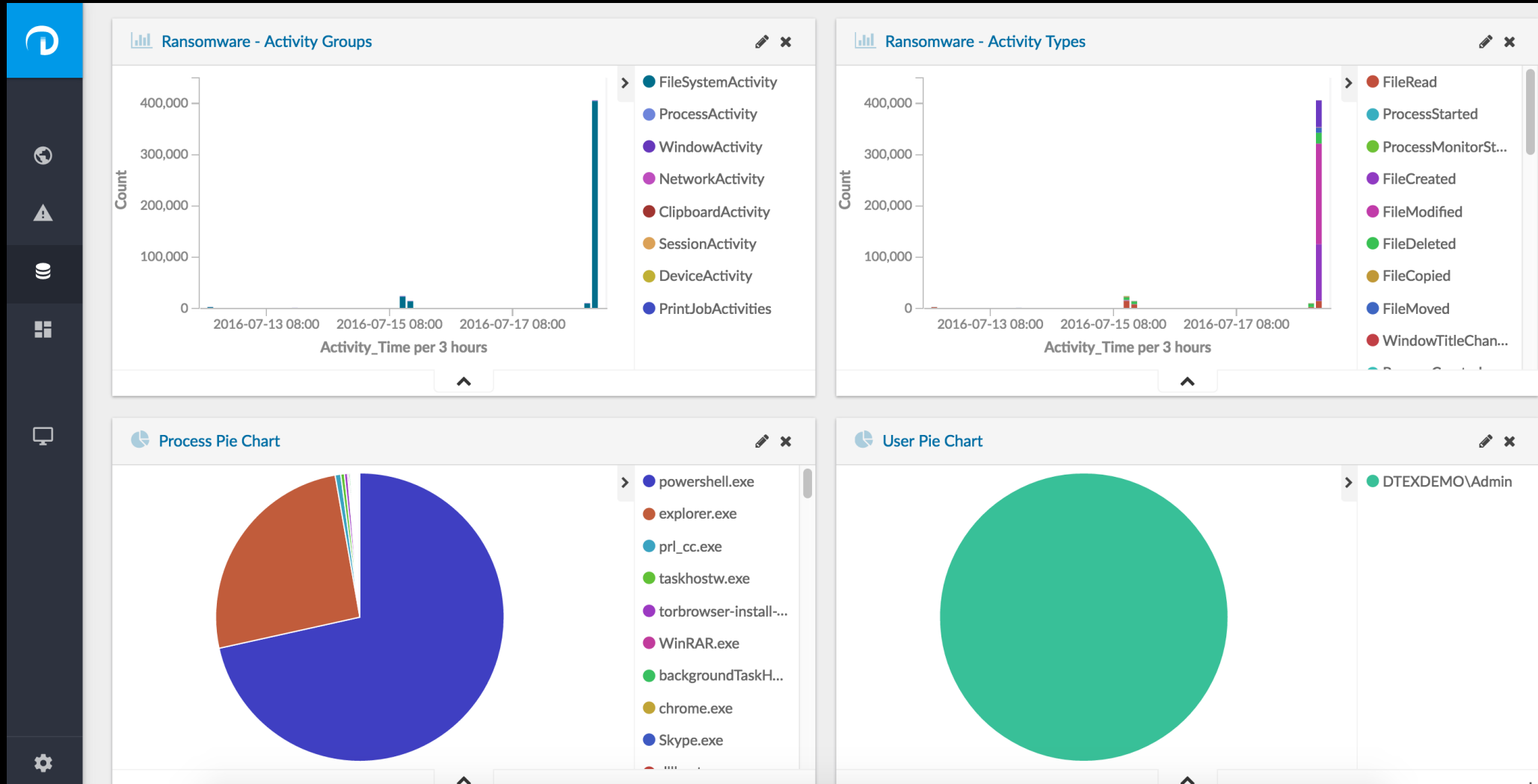
Alert created at Friday, September 16th 2016, 11:17:13 am and updated at Friday, September 16th 2016, 11:17:13 am based on 10700 activities.

Activities occurred between Tuesday, September 13th 2016, 8:08:00 pm and Wednesday, September 14th 2016, 7:08:15 pm

Activities received by server between Wednesday, September 14th 2016, 10:00:08 pm and Wednesday, September 14th 2016, 7:08:15 pm

High Cyber Security Tools 2820.80 2016-09-15

RANSOMWARE



Ransomware reverse engineering

1. Bekannte Dateiendungen / Filenames von Ransomware

Time	Device_Name	User_Name	Activity_Type	Source_File_Name	Source_File_Extension
▶ June 16th 2016, 11:56:05.105	WORKGROUP\WIN-NQUVG50U4H7	WIN-NQUVG50U4H7\JOHN	FileCreated	21E41BF2ADFA19BB453C6A1480CA81AC	locky

Time	Device_Name	User_Name	Activity_Type	Source_File_Name	Source_File_Extension
▶ June 16th 2016, 14:07:02.927	WORKGROUP\WIN-NQUVG50U4H7	WIN-NQUVG50U4H7\JOHN	FileCreated	_Locky_recover_instructions	txt

2. Wo kam die Ransomware her

Time	User_Name	Device_Name	Network_Destination_IP	Network_Host_Port	Net
▶ June 16th 2016, 09:05:01.221	WORKGROUP\WIN-NQUVG50U4H7	WIN-NQUVG50U4H7\JOHN	112.78.2.153	443	vin

Ransomware reverse engineering

Meist ändert Ransomware auch den Desktop-Hintergrund des Benutzers. Dtex sucht nach neuen Bilddateien, die Ausdrücke wie „verschlüsseln“ und „entschlüsseln“ enthalten.

Time ▾	Device_Name	User_Name	Activity_Type	Source_File_Name	Source_File_Extension
▶ June 16th 2016, 14:06:01.722	WORKGROUP\WIN-NQUVG50U4H7	WIN-NQUVG50U4H7\JOHN	FileCreated	paycrypt	bmp



Bei bereits bekannten Ransomware-Samples erkennt Dtex auch den jeweiligen Hash von bekannten Ransomware-Dateien und ausführbaren Dateien.



Time ▾	Device_Name	User_Name	Activity_Type	Source_File_Checksum_SHA256
▶ June 16th 2016, 12:18:22.184	WORKGROUP\WIN-NQUVG50U4H7	WIN-NQUVG50U4H7\JOHN	FileCreate	508F5770F18098CBE8C14EBB696998AE

Merkmale

Description:

Type:

Created: Date: Today | 
Time: Now | 
Note: You are 1 hour ahead of server time.

Updated: Date: Today | 
Time: Now | 
Note: You are 1 hour ahead of server time.

LIST LEXONS

LEXON

ListLexon object

ListLexon object

ListLexon object

ListLexon object

Add lexon

Keyword:

Fieldname:

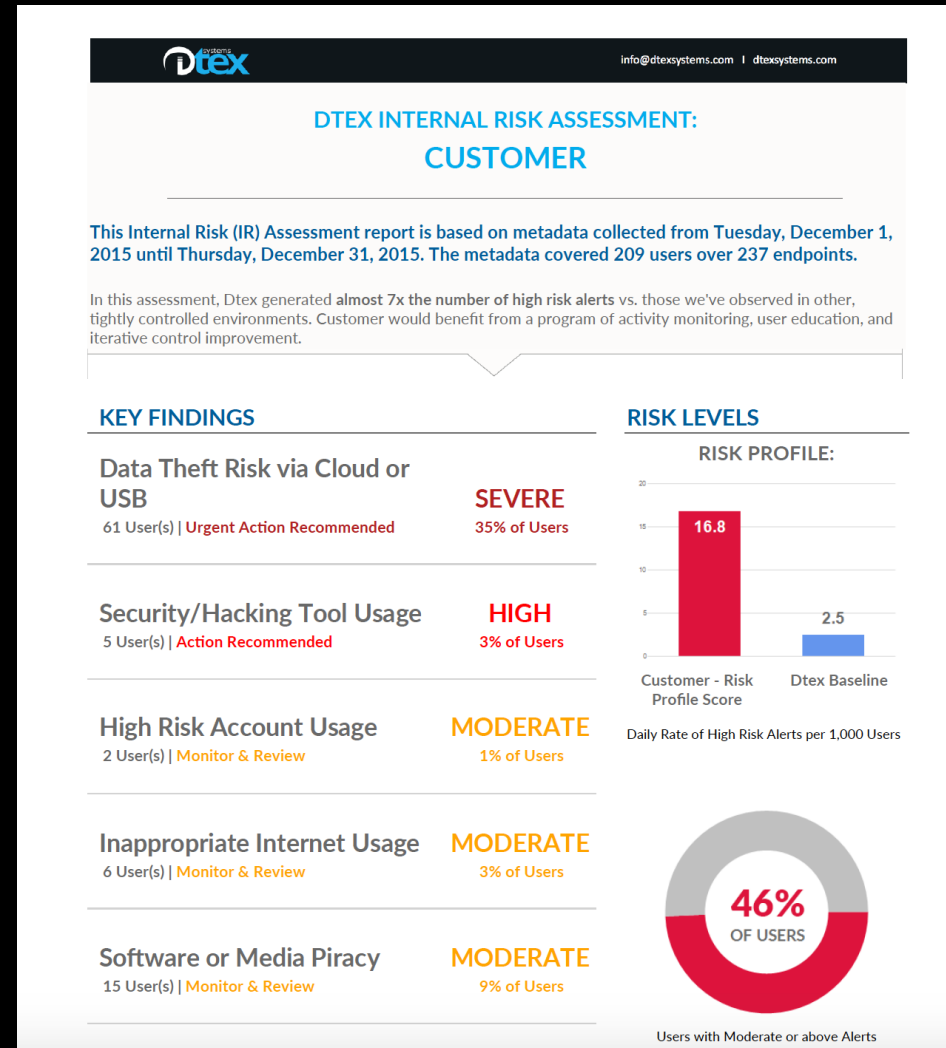
Description:

Created:

✓ -----

- destination_file_extension
- source_file_extension
- source_file_drive_details.type
- website_primary_url
- process_drive_details.type
- Process_name**
- process_name
- source_file_directory
- destination_file_name
- source_file_name
- process_is_elevated
- destination_file_directory
- website_domain
- window_title
- destination_file_drive_details.type
- activity_type

USER THREAT ASSESSMENT





Vielen Dank für Ihre Aufmerksamkeit