

A dark, atmospheric landscape featuring a winding road that leads the eye into the distance. The terrain is rugged and rocky, with sparse vegetation. The sky is filled with soft, textured clouds. The overall mood is mysterious and contemplative. The text 'DSIRF' is prominently displayed in the center of the image.

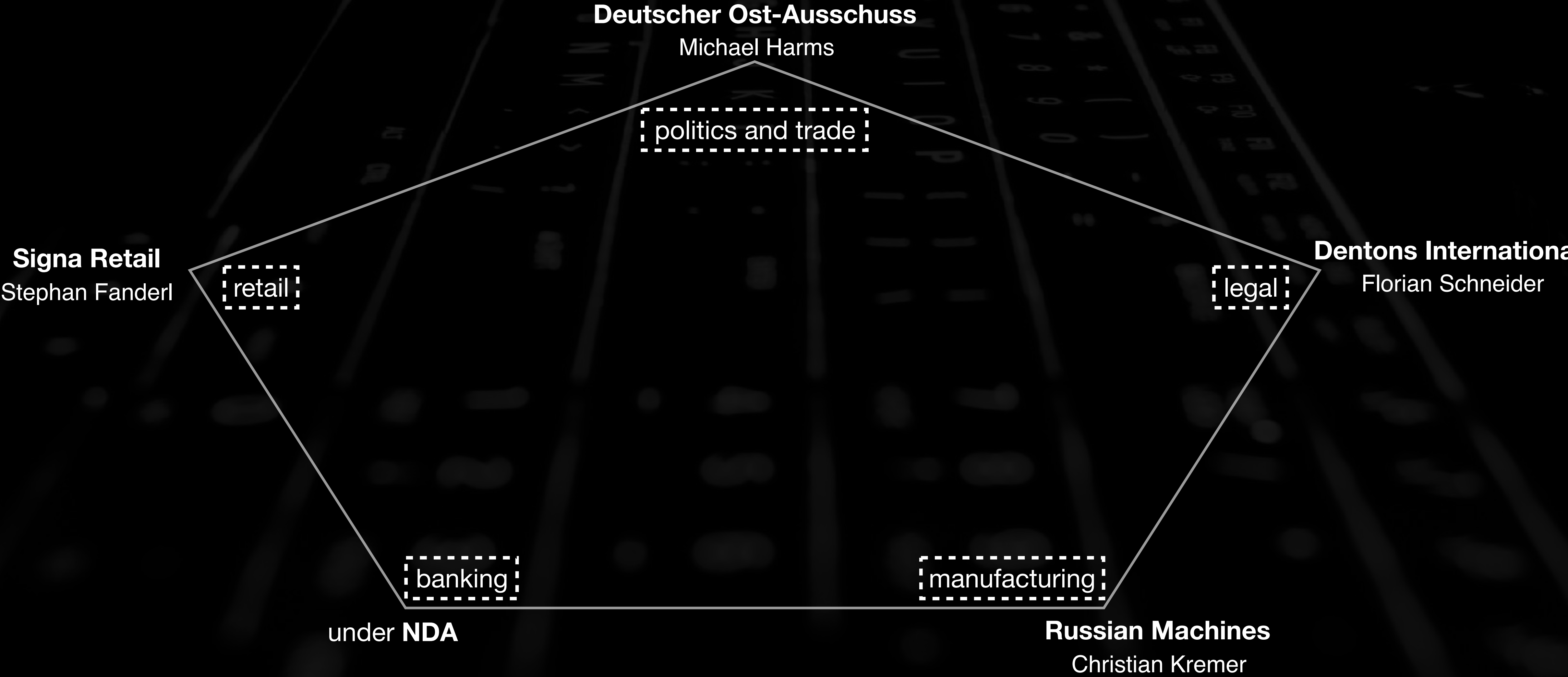
DSIRF

About Us

- ▶ established in June, 2016
- ▶ spanning a network of over 30 employees and contractors
- ▶ operating in 5 countries in and around Europe
- ▶ dedicated to deeptech and security



References



Our Storyline

1

Deep Dive Research and Analytics

- analysis of elections and campaigning methods
- analysis of rogue hacking operations
- unmasking foreign information warfare tactics

2

Advanced Biometrics

Cyber Warfare

- face, object, pattern recognition*
- commercial and public security
 - smart cities
 - intelligence offices
 - law enforcement
 - border control (immigration)

- subzero, red team*
- tools development for automated exfiltration of sensitive/private data
 - tailored access operations: identification, tracking and infiltration of threats

3

- machine-learning powered categorisation of many data sources (including documents, image and video files)

Evidence Lab

- consolidate, archive & access evidence
- fast forensics and crime detection

The Rationale

Evidence is becoming primarily digital.

Technical obstacles make it increasingly difficult for governments and law enforcement agencies to de-anonymise and access data from suspects.

Encrypted channels allow criminals to exchange information and hide from law enforcement surveillance.



Advanced Biometrics

Perfected Investigations



Rapid Forensic Analysis

100 hours of accessible CCTV footage can be analysed for faces of criminals in just 10 hours by our algorithms



Offline to Online

images of terrorists or of any person of interest can be checked against social networks, blogs and other digital sources and databases



Predictive Policing

learning from criminal activities in the past, our algorithms derive risky areas and predict strategies of outlaws to make police work more effective

real-world demonstration video: <https://bit.ly/2MzpV2T>

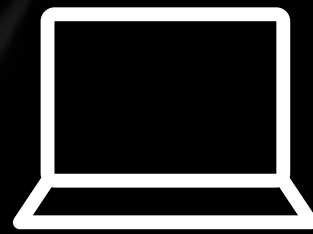
SUBZERO

NEXT GENERATION CYBER WARFARE

DSIRF

At A Glance

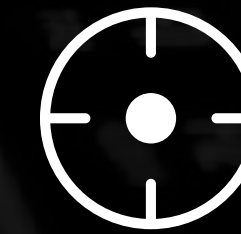
A state-of-the-art computer surveillance tool designed for the cyber era which enables



FULL CONTROL
of the target PC



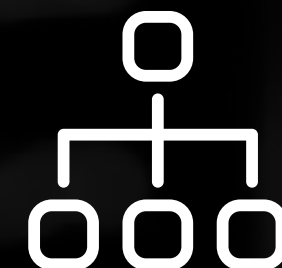
COMPLETE ACCESS
to all data and passwords



LOCATION TRACKING
no matter where in the world



STEALTH MONITORING
by utilising unique anti-virus
evasion techniques



MULTIPLE ATTACK VECTORS
allowing remote and local infiltration
methods



TEAM OF EXPERTS
ready to provide assistance and
trainings on advanced attack
techniques

THE PRODUCT

Control Center

The easy to use, web based control center allows easy data exfiltration and full control of the target computer.

The screenshot shows the Control Center interface for an agent named 'laura.doe'. The top navigation bar includes the 'S' logo, 'Operations', a '+ Terminal' button, and the user 'Admin' with the email 'admin@company.com'. The main content area is titled 'Sandstorm > Agents' and 'laura.doe'. A blue 'Launch Shell' button is prominent. On the left, a sidebar menu contains 'Info', 'Passwords', 'Screenshots', 'Files', 'Shell Logs', 'Jobs', and 'Settings'. The 'Activity' section features a heatmap for the 'Last Week' with columns for each hour from 0a to 23p and rows for each day of the week (M, T, W, T, F, S, S). The heatmap uses green and yellow blocks to indicate activity. Below the heatmap is an 'Info' section with a 'System' tab and a table for system details.

System	Computer Name	User Name	Language

Passwords

Extract credentials from the target PC
with a single click.

The screenshot shows a web interface for managing agents. The top navigation bar includes a logo 'S', the word 'Operations', a '+ Terminal' button, and a user profile 'Admin admin@company.com'. The main content area is titled 'Sandstorm > Agents' and 'laura.doe'. A sidebar on the left contains a 'Launch Shell' button and a menu with 'Info', 'Passwords', 'Screenshots', 'Files', 'Shell Logs', 'Jobs', and 'Settings'. The 'Passwords' section is active, displaying three tables of extracted credentials.

Google Chrome

LOGIN	PASSWORD	URL
user00321	p4ssword!	https://paypal.com
diego_summers@gmail.com	if33lsafe#	https://gmail.com/login
008827362	88736251	https://meine.deutsche-bank.de/trxm/db/
user00321	p4ssword!	https://paypal.com

Outlook 2013

LOGIN	PASSWORD	URL
summers13@yahoo.com	safe13\$	https://login.yahoo.com
diego_summers@gmail.com	if33lsafe#	https://gmail.com/login

Internet Explorer

LOGIN	PASSWORD	URL
-------	----------	-----

Screenshots

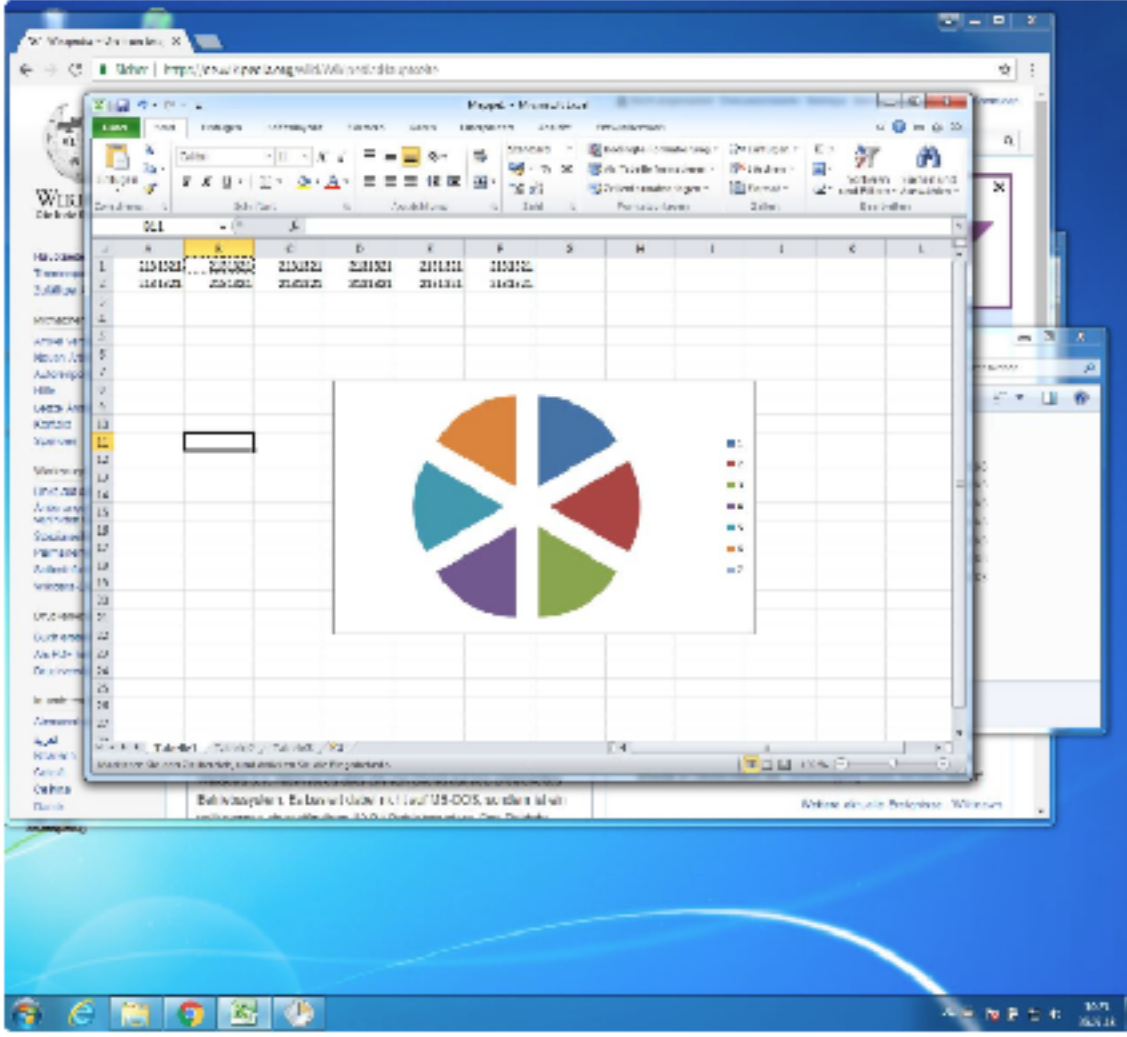
Easily take screenshots from the target PC for intelligence and evidence collection.

S Operations + Terminal Admin admin@company.com

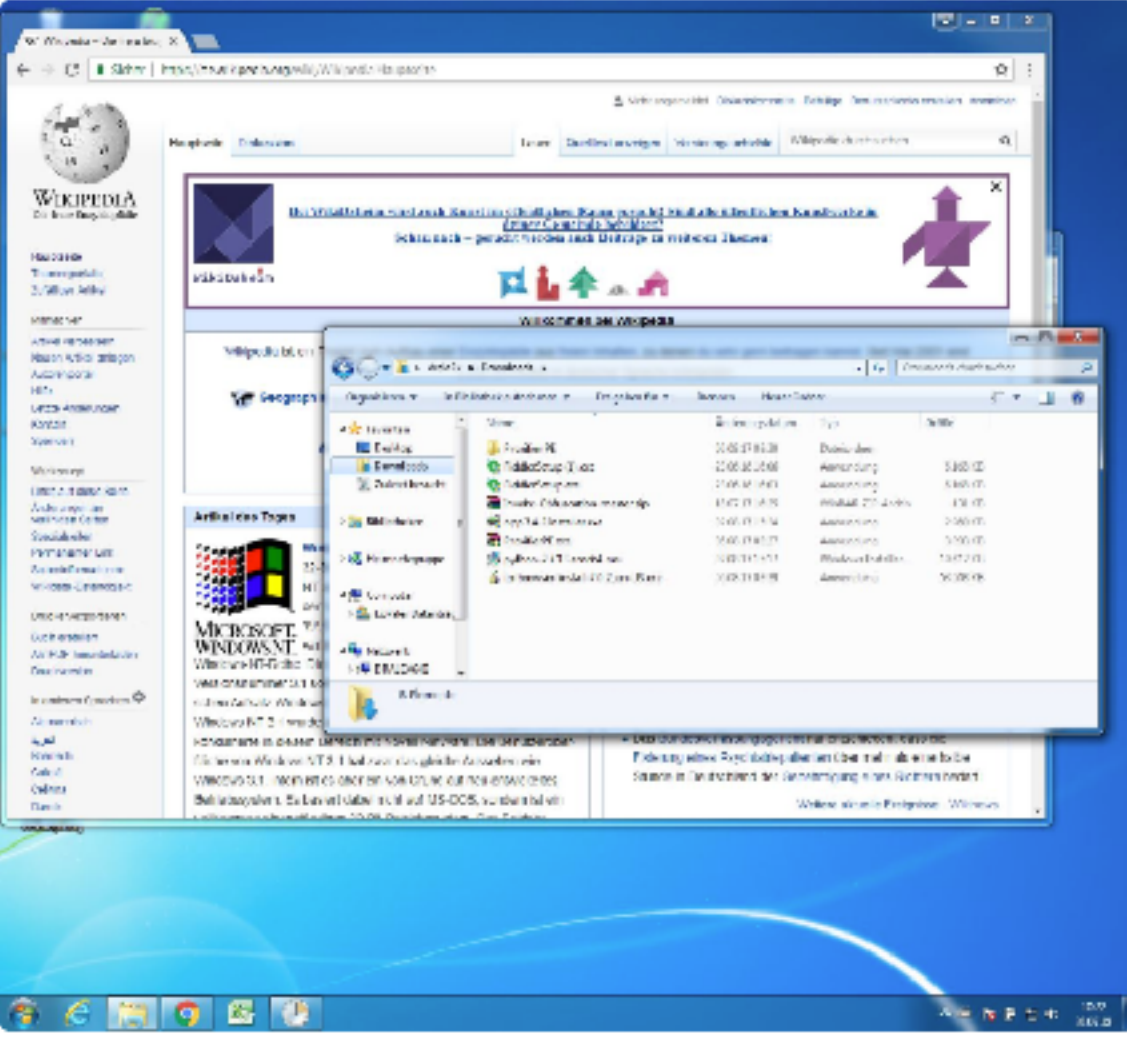
Sandstorm > Agents
laura.doe

Launch Shell

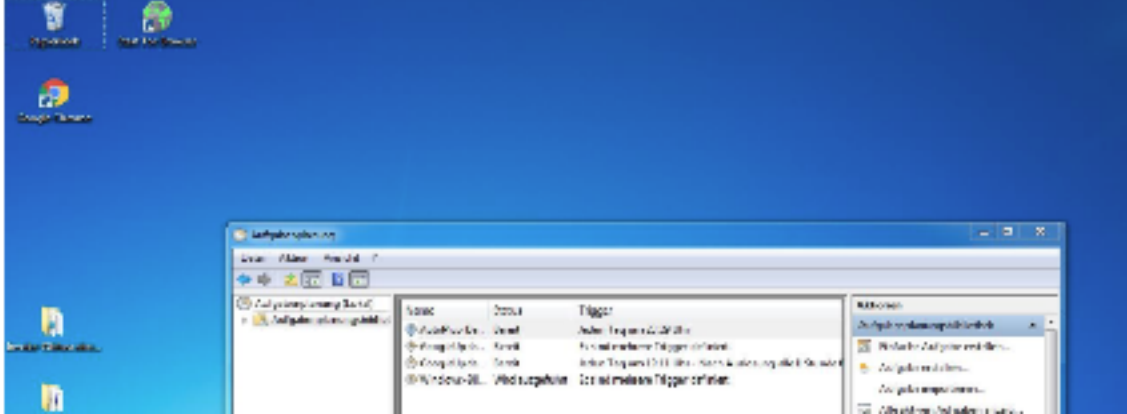
- Info
- Passwords
- Screenshots**
- Files
- Shell Logs
- Jobs
- Settings

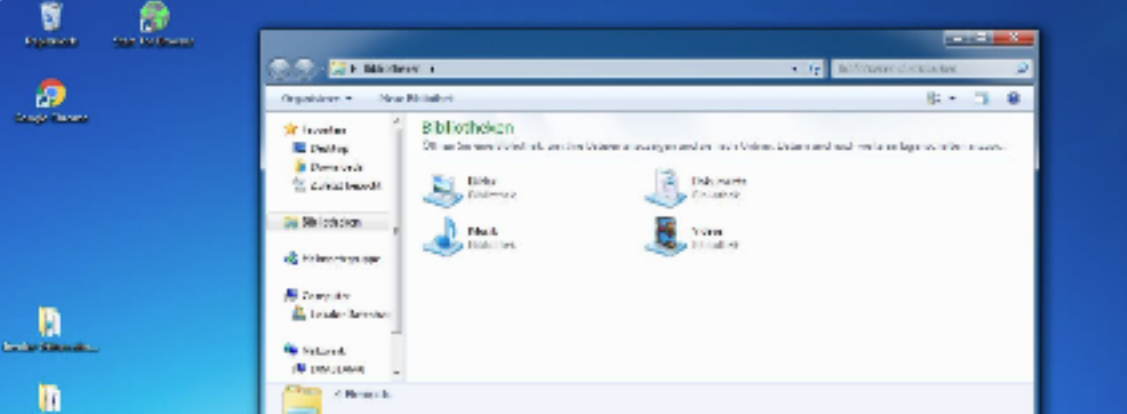


a minute ago



2 minutes ago





Files

Allows you to access, download, modify and upload files from the target computer.

The screenshot shows a web interface for file management. At the top left, there is a logo 'S' and the text 'Operations'. At the top right, there is a '+ Terminal' button and a user profile 'Admin' with the email 'admin@company.com'. Below the header, the breadcrumb 'Sandstorm > Agents' is visible, followed by the agent name 'laura.doe'. On the left side, there is a sidebar with a 'Launch Shell' button and a list of navigation items: Info, Passwords, Screenshot, Files (highlighted), Shell Logs, Jobs, and Settings. The main content area is titled 'Files' and contains a table of files.

Files	
secret_plan.docx	340 KB
project_titan.pdf	1.2 MB
bank_transactions.xlsx	800 KB
passport.jpg	3.2 MB
passwords.txt	450 KB
call_with_diego.mp3	12 MB
forecast_2019.xlsx	2.3 MB
drug_customer_list_2018.xlsx	4.5 MB

Location Tracking

View the current and past geo-location of your target. Worldwide.

S Operations + Terminal Admin admin@company.com

Sandstorm > Agents
laura.doe

The map displays a street grid in Vienna, Austria. A blue dot marks the current location of the target 'laura.doe' at the intersection of Weimarer Straße and Hasenauerstraße. A green trail shows the path of movement, starting from the bottom right and moving north-west towards the current location. Labeled landmarks include: Botschaft der Sozialistischen..., Tierklinik Hutter, Hotel Park-Villa, Felix Salten Wohnung (1911-1939), Embassy of the Republic of Indonesia, Botschaft des Königreiches Thailand, Währinger Park, Fischer Bräu - Erste Wiener Gasthausbrauerei, Teka Sushi, and Betriebshof Gürtel. Street names visible include Felix-Mottl-Straße, Hasenauerstraße, Weimarer Straße, Colloredogasse, and Gymnasiumstraße.

Evidence Lab

NEXT BIG FEATURE

A dedicated place to securely store, organise and search collected evidence using state-of-the-art AI technology.



Secure

Evidence is stored encrypted. Permissions can be easily applied to restrict who can see what.



Smart

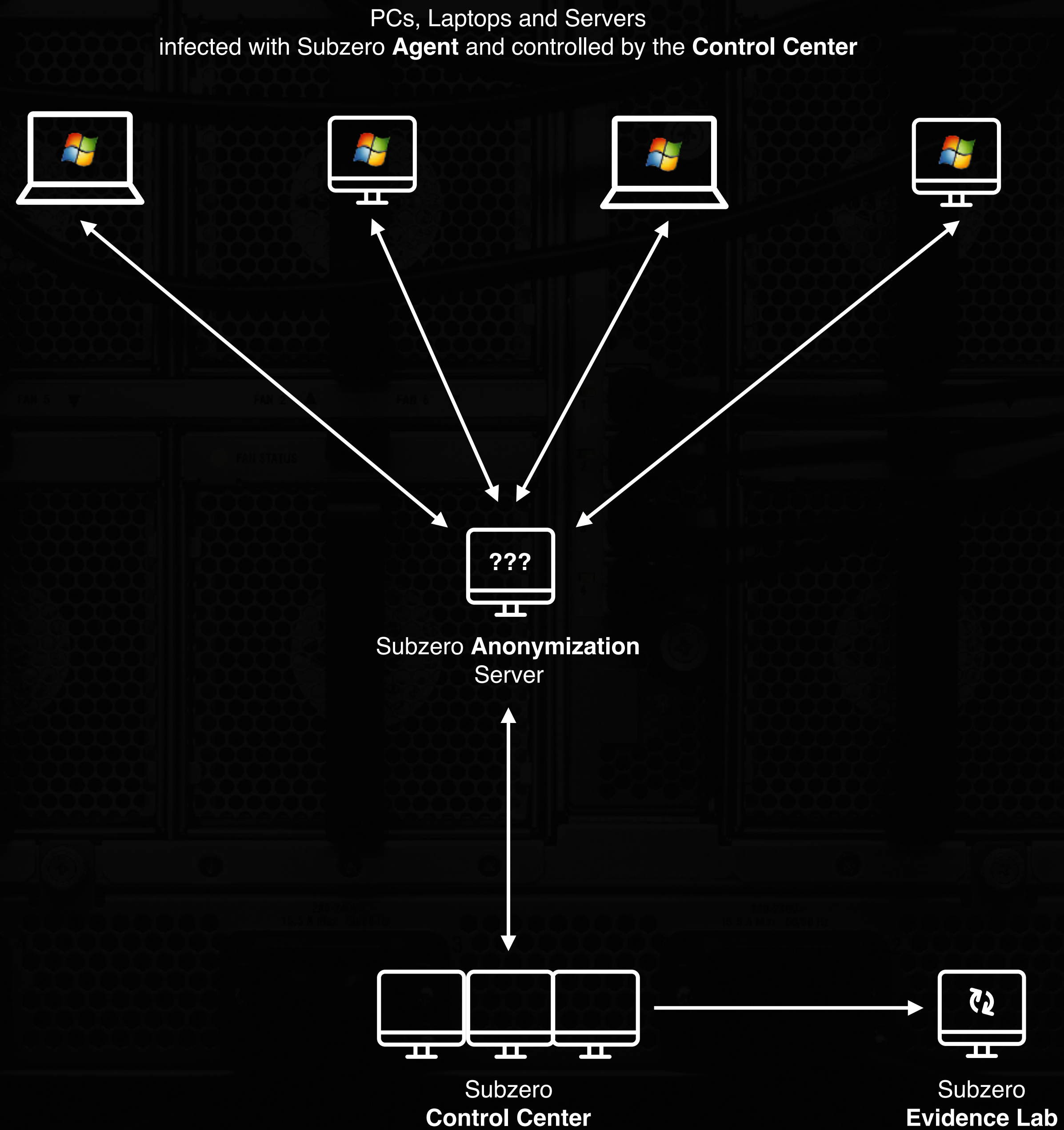
Using cutting edge technologies like machine learning, large amounts of data can be quickly searched and automatically categorised.



Advanced

An advanced biometric recognition feature which allows to quickly search and categorise image and video files looking for objects, faces or patterns.

Architecture



* Simplified Architecture

Use Cases

**ANTI
TERRORISM**

**HUMAN
TRAFFICKING
&
CHILD
PORNOGRAPHY
RINGS**

**FINANCIAL
FRAUD**

**CYBER
CRIME**

**DARKNET
CRIMES**

THE TEAM

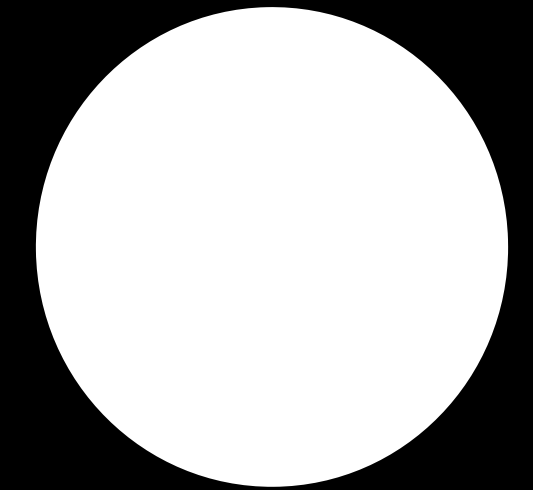
Leadership

Our leadership works with contracted specialists around the globe. Our intellectual property remains exclusively in our hands.



DRAZEN MOKIC

Product Manager &
Team Lead



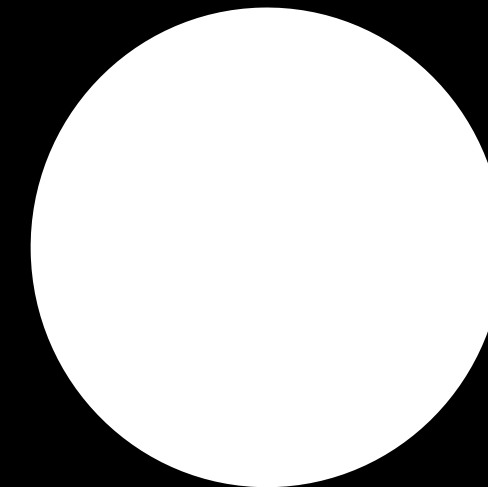
SASA B

Cyber Security Expert &
Security Researcher



JULIAN ERDOEDY

Managing Director



KUBA G

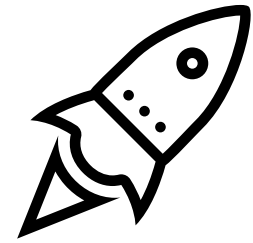
Lead Engineer &
Security Researcher

CEM BAYKAM

Machine Learning & AI
Lead Engineer

NEXT STEPS

Next Steps



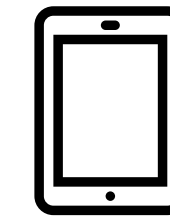
Ready-to-Ship

Market introduction supporting Windows OS & Windows Server.



macOS

Add support for the macOS operating system.



Mobile Devices

Add support for Android and iOS mobile devices.

CONTACT

www.dsirf.eu

Julian Erdoedy

Tel. +43 676 73384 ■■

Email. ■■@dsirf.eu

Drazen Mokic

Tel. +43 676 73384 ■■

Email. ■■@dsirf.eu