

Cybercrime & Cyberwar

Halle 7
Stand 7-339

RÜDIGER TROST

ruediger.trost@withsecure.com | [@ruedigertrost](https://twitter.com/ruedigertrost)
| [@ruediger@chaos.social](https://twitter.com/ruediger@chaos.social)

W / T H
secure



15

W / T HTM
secure

Halle 7
Stand 7-339

W / T H[®]
secure

15

Cybercrime & Cyberwar

Halle 7
Stand 7-339

RÜDIGER TROST

ruediger.trost@withsecure.com | [@ruedigertrost](https://twitter.com/ruedigertrost)
| [@ruediger@chaos.social](https://twitter.com/ruediger@chaos.social)

W / T H
secure

Game #13769228142

Previous #13769223849

LEAVE TABLE

VIEW LOBBY

ff75
\$23,954

POT \$11,420

ickseycat
\$2,808

adam
\$6,265

mwp
\$2,900

seycat
\$9,620

renzo1
All In

vick7
\$6,363

ddiedem
\$4,170



Chat

Notes

Stats

Info

Dealer: ff75, it's your turn. You have 12 seconds to act
 Dealer: ff75 has two pair, Aces and Sixes
 Dealer: snookmachine has two pair, Kings and Queens
 Dealer: Game #13769207627: ff75 wins pot (21353) with two pair, Aces and Sixes
 Dealer: snookmachine finished the tournament in 9th place
 Dealer: ff75, it's your turn. You have 12 seconds to act
 snookmachine [observer]
 Dealer: gagz420, it's your turn. You have 12 seconds to act
 Dealer: Game #13769216489: adam01 wins pot (3600)
 Dealer: Game #13769223849: ff75 wins pot (1800)









GOOD
NEWS
ONLY!



MOSTLY
GOOD
NEWS!

SOME
GOOD
NEWS!

LockBit BLOG

lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.pet

Not secure

lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.pet

LOCKBIT 3.0

LEAKED DATA

TWITTER

PRESS ABOUT US

HOW TO BUY BITCOIN

AFFILIATE RULES

CONTACT US

MIRRORS

richard-wolf.com

2D 18h 02m 30s

Richard Wolf GmbH is a company that operates in the Medical Devices industry. It employs 1,001-2,000 people and has \$250M-\$500M of revenue.

Updated: 07 Nov, 2022, 14:21 UTC181

coopavegra.fi.cr

1D 03h 10m 57s

En 1957 un grupo de vecinos del cantón de Palmares tuvo la idea de organizarse cooperativamente para buscar la manera de colaborar con el incipiente desarrollo de este

Updated: 06 Nov, 2022, 22:28 UTC3310

multicareinc.com

PUBLISHED

MultiCare Hospitals & Physicians Clinics · Idaho, United States · 322 Employees MultiCare is a local business, operated by a local family, caring for the people of this local community.

Updated: 06 Nov, 2022, 22:25 UTC12572

mtrx.com

PUBLISHED

rpca.com.au

Updated: 06 Nov, 2022, 22:18 UTC9555

osde.com.ar

PUBLISHED

OSDE is a network of medical care services in Argentina created in 1972. 2 In 1991 it became the first network of medical-care services in Argentina , with a system of open health plans. 3 It currently

Updated: 06 Nov, 2022, 22:11 UTC15357

parrottsims.com

PUBLISHED

We are a full-service law firm providing our clients with superior legal services by leveraging our resources and personnel to deliver timely legal advice... Phone: +1 832-485-6000

Updated: 06 Nov, 2022, 22:08 UTC14407

seaviewresortkhaolak.com

PUBLISHED

Seaview Resort Khao Lak is set on Nang Thong Beach, an extensive stretch of fine sands framed by the emerald blue waters of the Andaman Sea and against a verdant mountainous background. The

Updated: 06 Nov, 2022, 22:03 UTC10810

KEARNEYCO.COM

18D 14h 52m 30s\$ 2000000

Founded in 1985, Kearney is the premier CPA firm focused on the Government, providing services across the financial management spectrum. Kearnev has helped the Federal Government

Updated: 06 Nov, 2022, 21:09 UTC1246

rockworthindia.com

7D 22h 38m 32s

Rockworth Systems Furniture (india) Private Limited

thenet.group

9D 05h 23m 22s

he Net Group is specialized in express courier

optiprint.ca

8D 05h 21m 10s

Optiprint Inc. provides comprehensive services

bliss-d.com

PUBLISHED

BLISS Co., Ltd. Business content Architecture,



LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE
UK, THE US AND THE CRONOS TASK FORCE



Press Releases

1D 18H 49M 11S



Updated: 02 May, 2024, 13:37 BST



Who is LockbitSupp?

1D 18H 49M 11S

The \$10m question



Updated: 02 May, 2024, 13:37 BST



But there's more...

1D 18H 49M 11S



Updated: 02 May, 2024, 13:37 BST



What have we learnt?

1D 18H 49M 11S

Some facts and figures from the backend!



Updated: 02 May, 2024, 13:37 BST



More LB hackers exposed

1D 18H 49M 11S



After compromising Lockbit's platform, Law Enforcement will be coordinating activity to deal with Lockbit's affiliates.

Updated: 02 May, 2024, 13:37 BST



What have we been doing?

1D 18H 49M 11S



Supporting victims worldwide!

Updated: 02 May, 2024, 13:37 BST



Preventing and protecting

1D 18H 49M 11S



National Cyber
Security Centre
a part of GCHQ

Updated: 02 May, 2024, 13:37 BST



Report Cyber Attacks!

1D 18H 49M 11S

Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement.

Updated: 02 May, 2024, 13:37 BST





LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE
LAW ENFORCEMENT AGENCIES

NCA
National Cyber Agency



Who is LockbitSupp?

1D 18H 49M 11S

The \$10m question



Updated: 02 May, 2024, 13:37 BST

7

What have we learnt?

1D 18H 49M 11S

Some facts and figures from the backend!

NCA
National Cyber Agency

LOCKBIT

Updated: 02 May, 2024, 13:37 BST

1

Report Cyber Attacks!

1D 18H 49M 11S

Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement.

Updated: 02 May, 2024, 13:37 BST

1

IDENTITY REVEAL



LockBitSupp is:

Dmitry Yuryevich Khoroshev





IDENTITY REVEAL



LockBitSupp is:

Dmitry Yuryevich Khoroshev



\$10.000.000



2. Mai

Übernahme

Übernahme der
LockBit Darknet-
Seite

9. Mai

“Neue” Opfer

77 Opfer auf der
Name & Shame
Seite von LockBit /
72% aus März oder
früher

Bekanntgabe

Bekanntgabe der
Identität von
LockBitSupp

7. Mai



2. Mai

Übernahme

Übernahme der
LockBit Darknet-
Seite

9. Mai

"Neue" Opfer

77 Opfer auf der
Name & Shame
Seite von LockBit /
72% aus März oder
früher

7. Mai

Bekanntgabe

Bekanntgabe der
Identität von
LockBitSupp

IT-SA

LockBit noch da

Aber kleiner!



kumhotire.com

1D 14h 26m 34s

Kumho Tire (formerly known as Samyang Tire) is a South Korean tire manufacturer. Kumho Tire was previously operated as a business unit of the Kumho Asiana Group. Since 2018, it is a

Updated: 15 Oct, 2024, 20:18 UTC 7235

tpgagedcare.com.au

6D 09h 57m 14s

Greetings! Today we are posting here the new company, "TPG Aged Care". Company Description: At TPG Aged Care, we believe that everyone has the right to be treated with dignity.

Updated: 03 Oct, 2024, 15:50 UTC 3862

oleopalma.com.mx

PUBLISHED

Greetings! Today we are posting here the new company, "Oleopalma Compania Agroindustrial Cia Ltda LLC". Company Description: Oleopalma is a company specialized in the cultivation,

Updated: 30 Sep, 2024, 13:48 UTC 7474

chcm.us

PUBLISHED

Greetings! Today we are posting here the new company, "College Hospital Costa Mesa". Company Description: College Hospital Costa Mesa is a facility specializing in psychiatric and

Updated: 30 Sep, 2024, 13:47 UTC 7446

nhbg.com.co

PUBLISHED

Greetings! Today we are posting here the new company, "Nuevo Hospital de Bocagrande". Company Description: The New Bocagrande Hospital is a high-level comprehensive health

Updated: 26 Sep, 2024, 17:09 UTC 12972

bnsgroup.co.uk

PUBLISHED

Greetings! Today we are posting here the new company, "BNS GROUP Ltd". Company Description: Founded over twenty years ago B&S GROUP has grown into a organisation focused on

Updated: 26 Sep, 2024, 17:05 UTC 27069

oyaksgs.com.tr

PUBLISHED

Greetings! Today we are posting here the new company, "OYAK Defense and Security Systems Inc.". Company Description: Oyak Savunma Ve Guvenlik Sistemleri A.S. is an enterprise located

Updated: 26 Sep, 2024, 17:05 UTC 54001

paybito.com

PUBLISHED

Quick Launch Self Branded Crypto Exchange. Create an exchange theme from scratch or go headless PayBitoPro APIs. Who We Serve Our experienced teams provide comprehensive

Updated: 18 Sep, 2024, 15:17 UTC 7687

efile.com

PUBLISHED

eFile.com offers free or low-cost tax preparation and e-filing for federal and state returns. Compare eFile.com with other services, get free tax support from Taxperts, and use tax

Updated: 18 Sep, 2024, 15:16 UTC 7627

yesmoke.eu

PUBLISHED

Sede legale | C.so Europa, 7 20122 Milano, Italia;
Sede Operativa | Via San Giusto, 5 10036 Settimo Torinese (To), Italia;
contact@yesmoke.eu +39 011 821 1653

Updated: 18 Sep, 2024, 15:15 UTC 7385

lakelandchamber.com

PUBLISHED

The Lakeland Chamber of Commerce serves as the Catalyst for business success, Convener of leaders and influencers, and Champion for our thriving community.

Updated: 18 Sep, 2024, 15:14 UTC 7174

crbrandsinc.com

PUBLISHED

CR Brands, Inc. was an American private-label consumer goods company, owned by the Beachwood, Ohio-based Resilience Capital Partners. It was formed in 2006 by Allied Capital

Updated: 18 Sep, 2024, 15:14 UTC 7193

bspcr.com

PUBLISHED

Dogecoin And Bitcoin Become Latest Additions To Robinhood Wallet After a long stretch of only offering Polygon (MATIC) in its Web3 wallet

rhp.com.br

PUBLISHED

We've got information about more than 70000 patients staff contractors investors internal information

policiaauxiliarcusaem.com.mx

PUBLISHED

Greetings! Today we are posting here the new company, "POLICIAAUXILIARCUSAEM.MX". Company Description: Government-funded private police auxiliary. Headquarters: 26-A

nfcaa.org

PUBLISHED

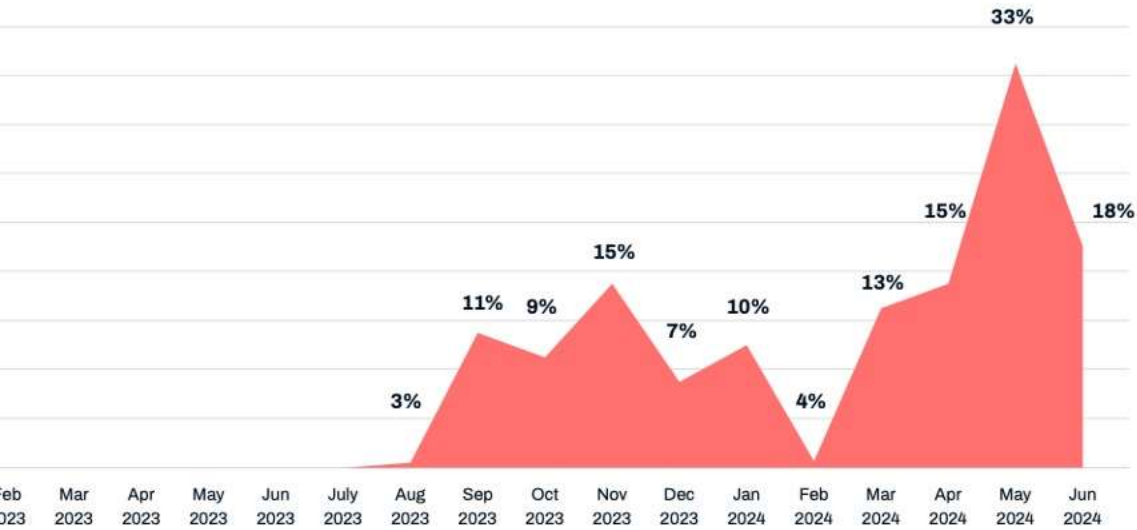
UTILITY ASSISTANCE. The Northeast Florida Community Action Agency, Inc. (NFCAA) is taking steps to maintain the health and safety of our customers, our employees, and our communities.

SOME
GOOD
NEWS!

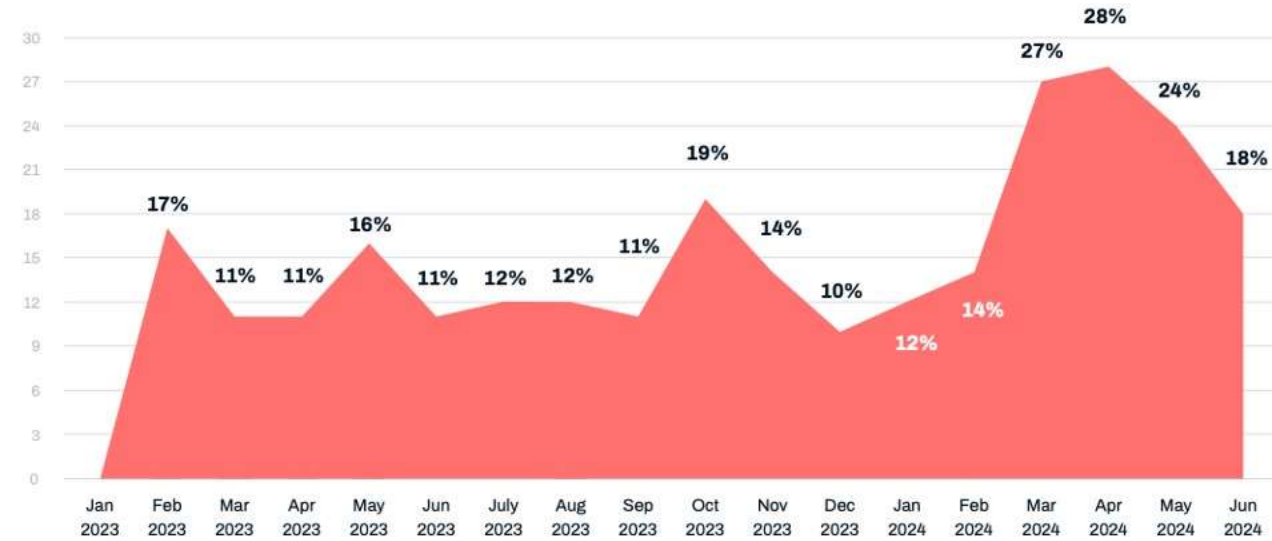


AFFILIATES VERLIEREN
VERTRAUEN IN LOCKBIT...

INC Ransom

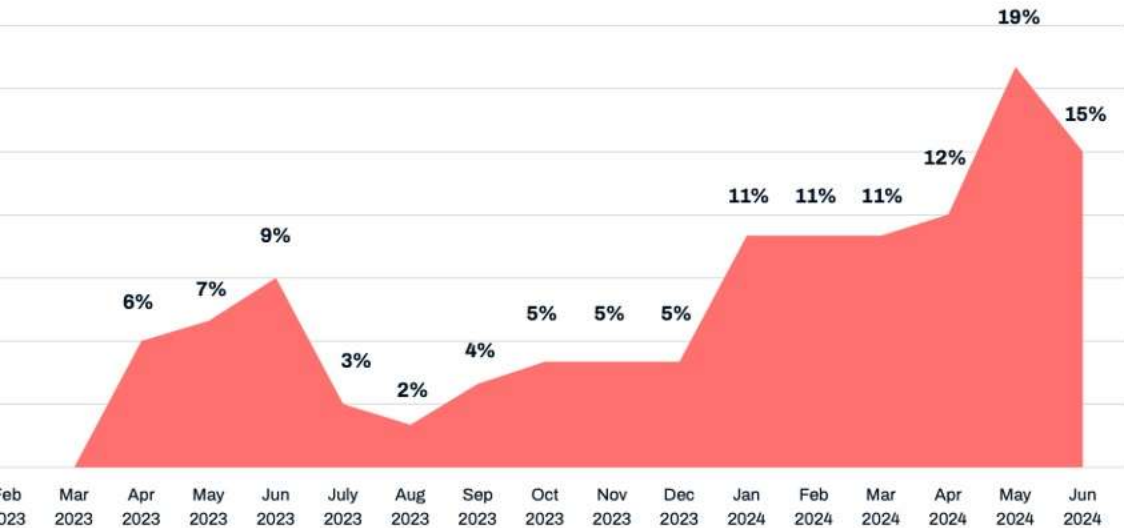


Medusa

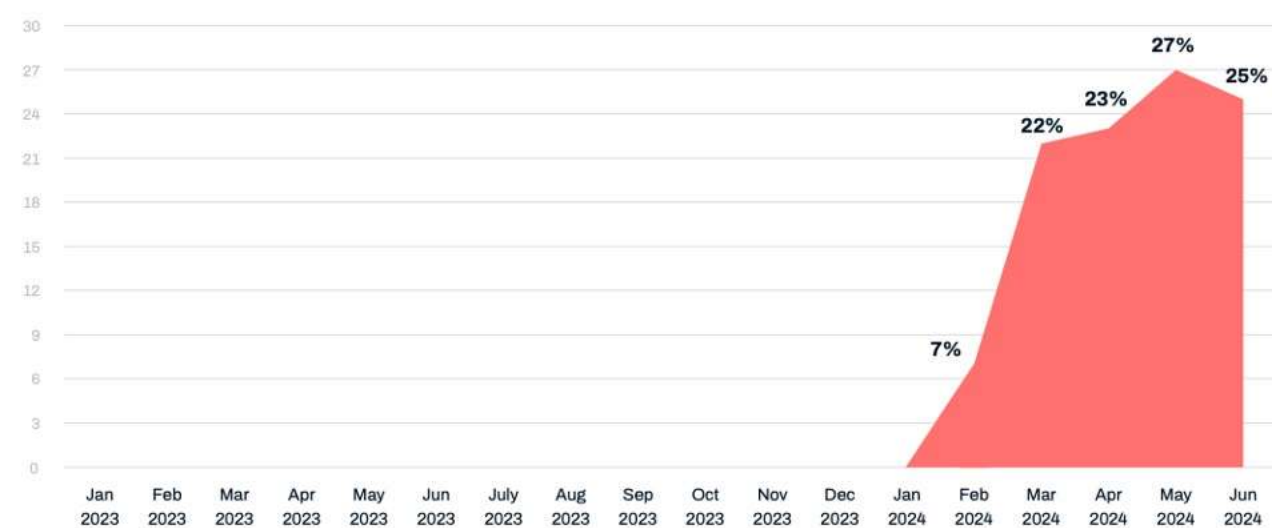


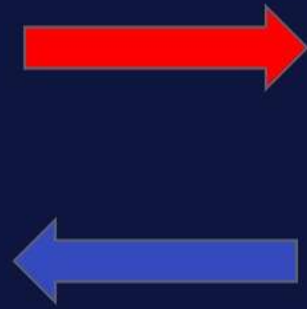
... STÄRKEN ABER ANDERE RANSOMWARE-GRUPPEN

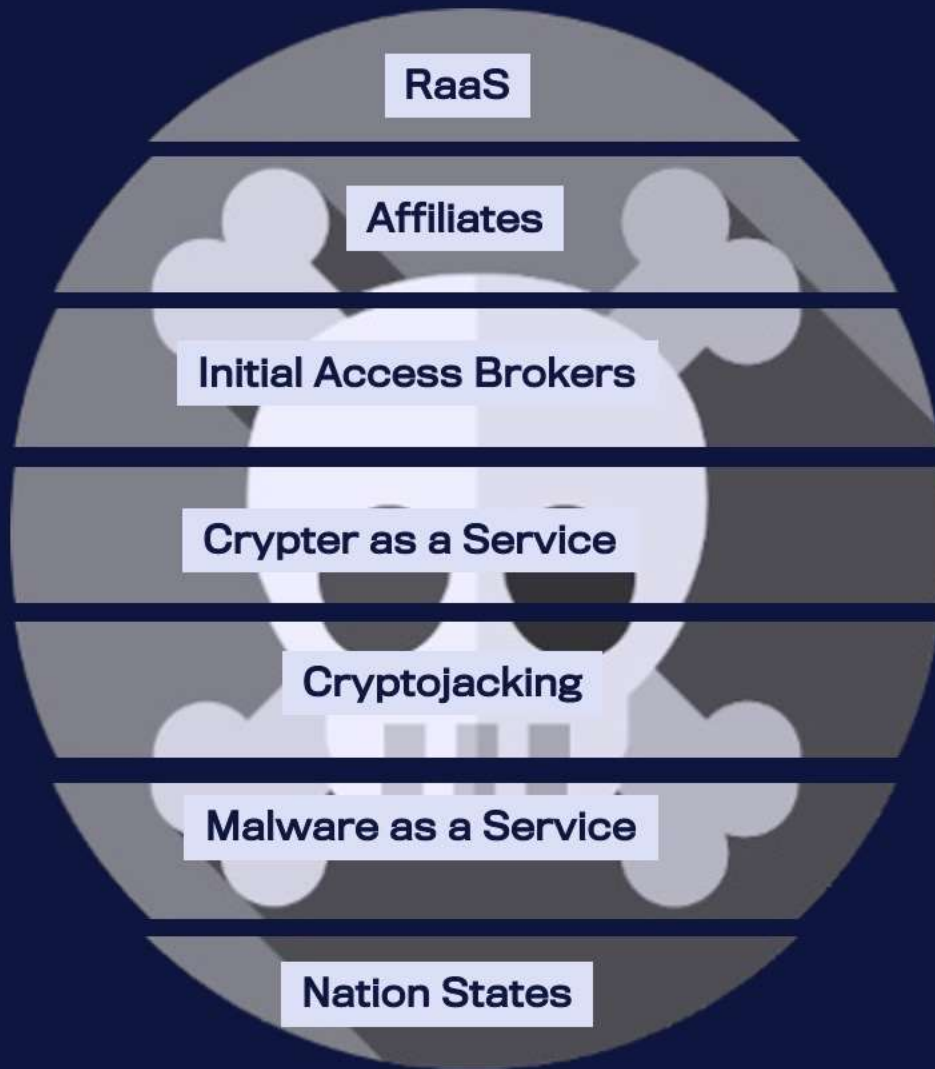
Qilin



RansomHub









***-as-a-Service
macht es leichter für
Einsteiger...**

...aber diese
Zusammenarbeit
bietet Chancen für
Ermittler!





„Die deutschen Geheimdienste warnen vor vermehrten russischen Destabilisierungsversuchen.

Man beobachte ein "aggressives Agieren der russischen Nachrichtendienste".

Der Kreml sehe Deutschland als Gegner.“

14.10.2024





Nützliche Tarnung für staatlich geförderte Angriffe

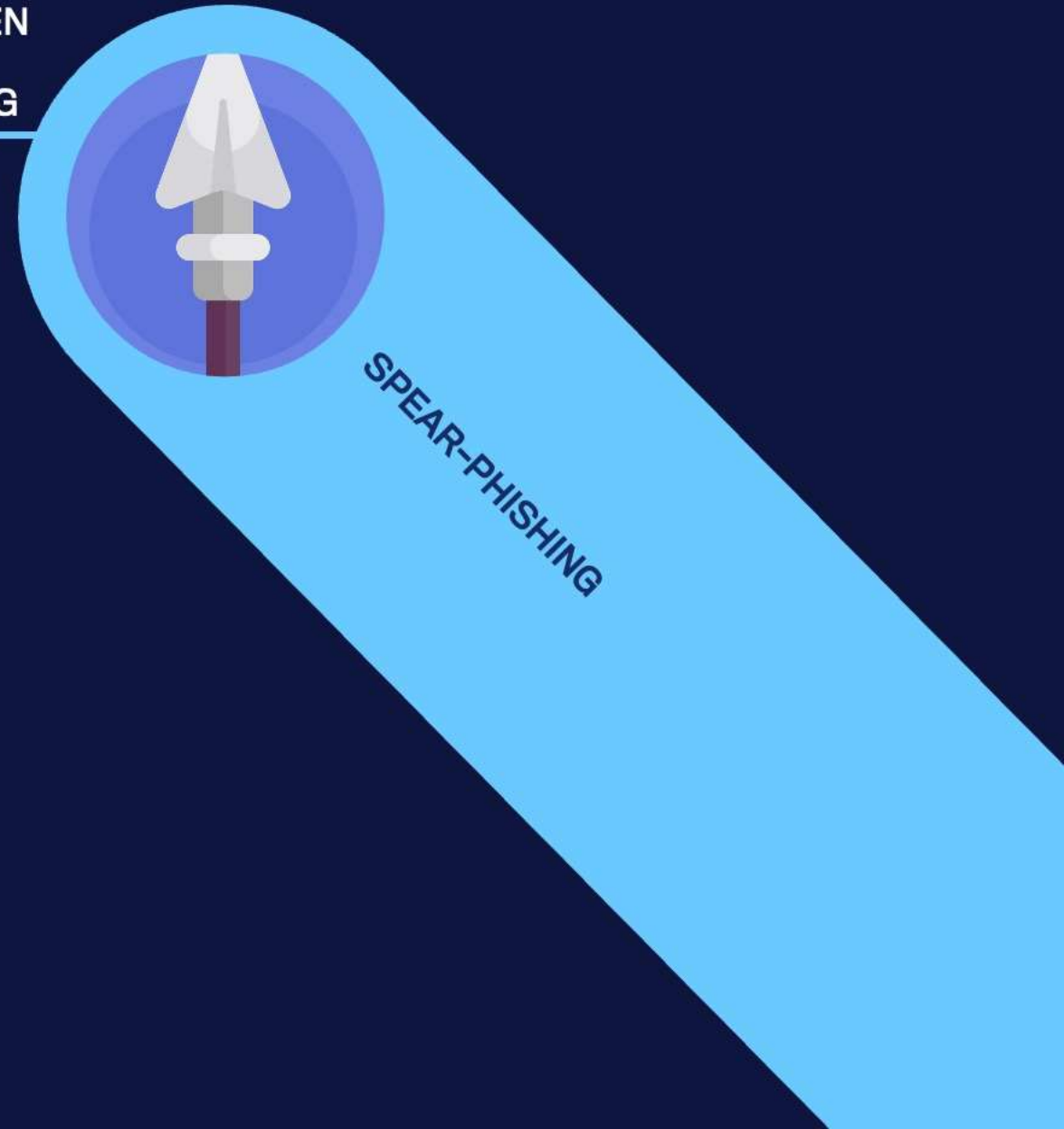


Nordkorea finanziert Teile des Haushalts mit Ransomware



TACTICS?

- AWARENESS-SCHULUNGEN
- (SPAM-)FILTER
- ANOMALIE ÜBERWACHUNG



- AWARENESS-SCHULUNGEN
- (SPAM-)FILTER
- ANOMALIE ÜBERWACHUNG



SPEAR-PHISHING

- PATCHING
- ANOMALIE ÜBERWACHUNG
- ÜBERSICHT ÜBER ASSETS



EXPLOIT
PUBLIC-FACING
APPS

- AWARENESS-SCHULUNGEN
- (SPAM-)FILTER
- ANOMALIE ÜBERWACHUNG



SPEAR-PHISHING

- PATCHING
- ANOMALIE ÜBERWACHUNG
- ÜBERSICHT ÜBER ASSETS



EXPLOIT
PUBLIC-FACING
APPS

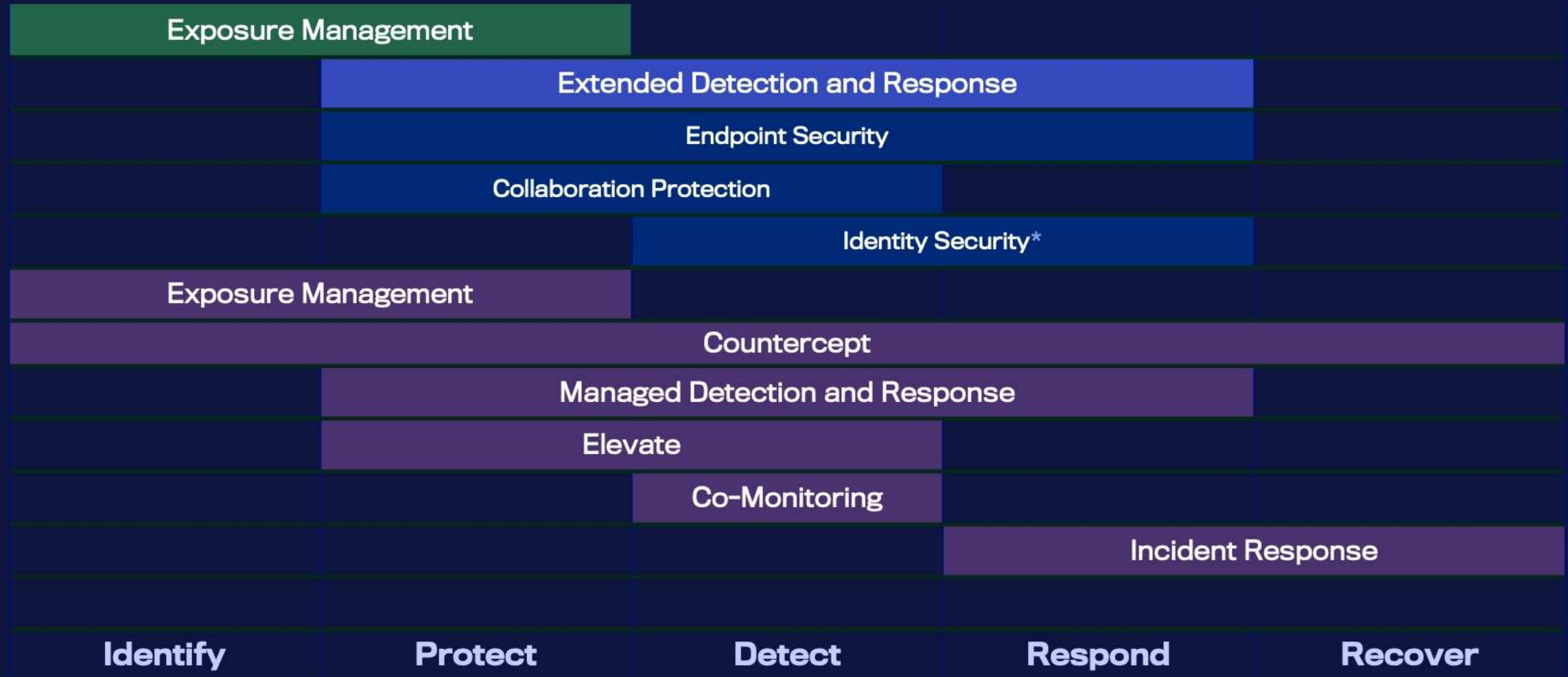
- ANOMALIE ÜBERWACHUNG
- DARKNET MONITORING
- PASSWORT POLICY



VALID
ACCOUNTS

GOOD
NEWS
ONLY!

WithSecure™ Elements Cloud – NIST

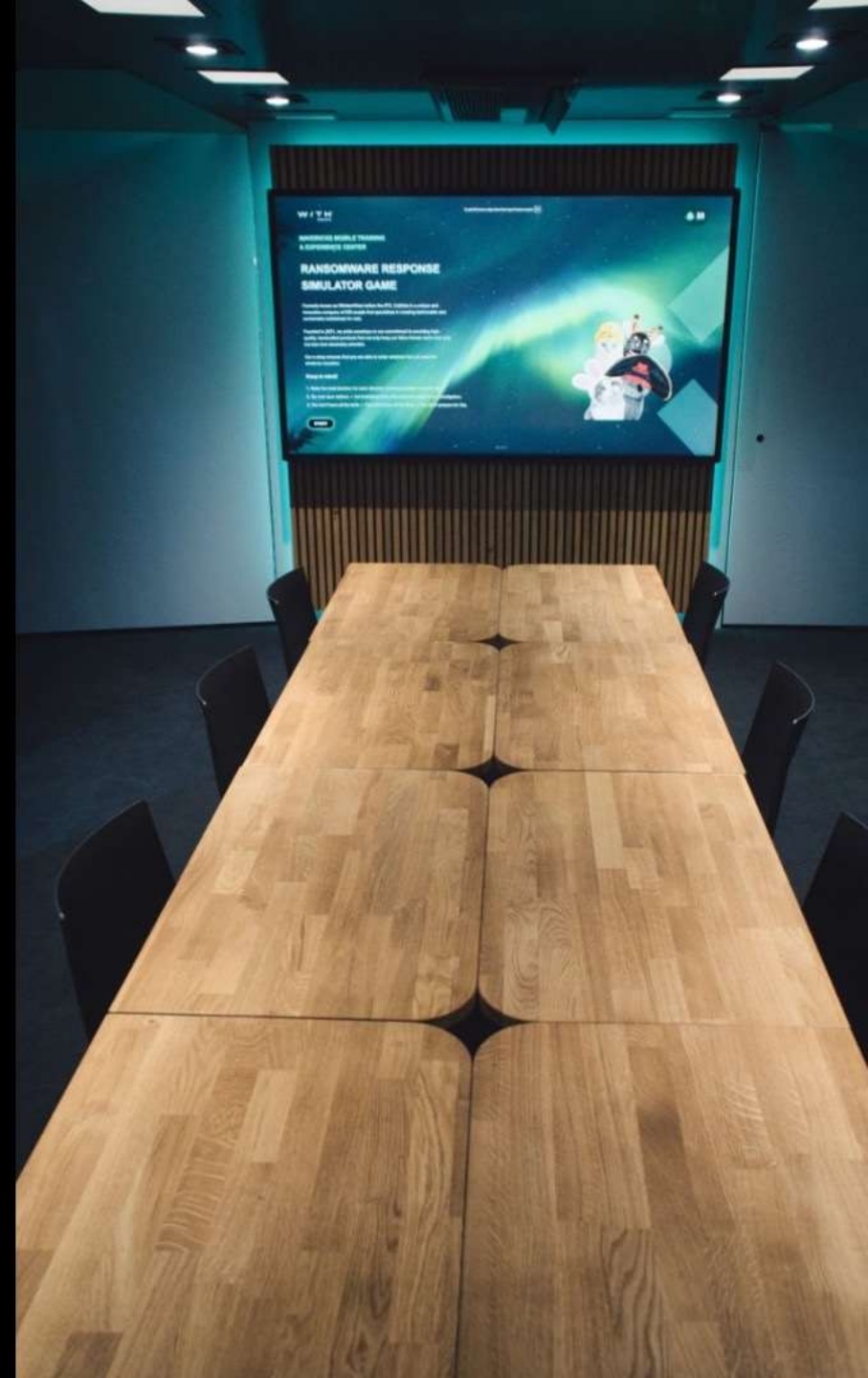


*Identity Security will be extended to respond capability later in 2024





Halle 7
Stand 7-339



Cybercrime & Cyberwar

Halle 7
Stand 7-339

RÜDIGER TROST

ruediger.trost@withsecure.com | [@ruedigertrost](https://twitter.com/ruedigertrost)
| [@ruediger@chaos.social](https://twitter.com/ruediger@chaos.social)

W / T H
secure