ARCTIC WOLF & michael wessel THINK DIGITAL

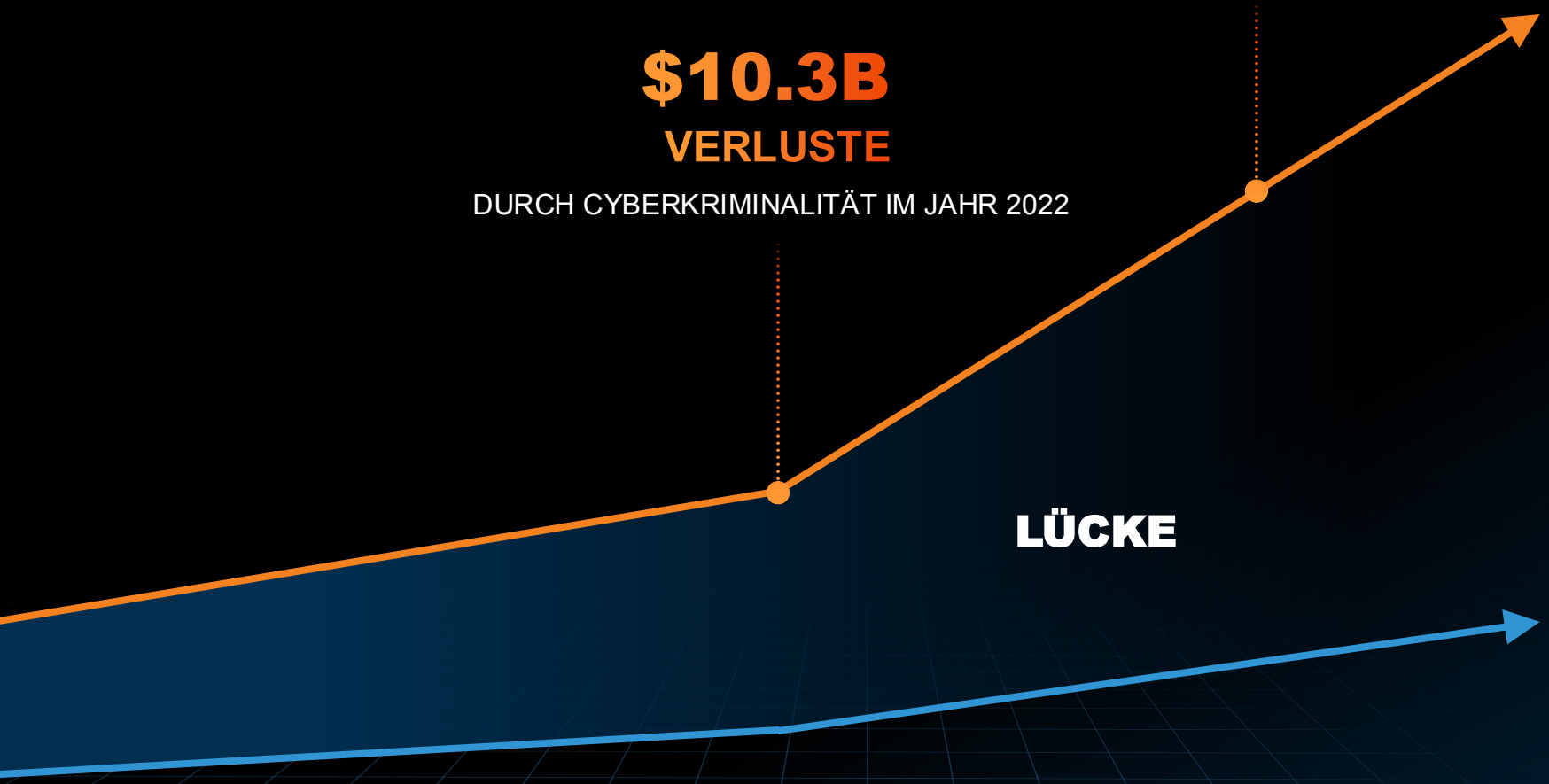
Cybersecurity komplett gedacht:
Arctic Wolf, Ihr Security Operations Partner

END CYBER RISK

CYBER RISIKO steigt weiter an

12,5 Mrd. USD
VERLUSTE
DURCH CYBERKRIMINALITÄT IM JAHR 2023

$10.3B
VERLUSTE
DURCH CYBERKRIMINALITÄT IM JAHR 2022



SECURITY HERSTELLER INSGESAMT IM JAHR 2023:
3.318+

GESAMTAUSGABEN FÜR SECURITY:
188 Mrd.

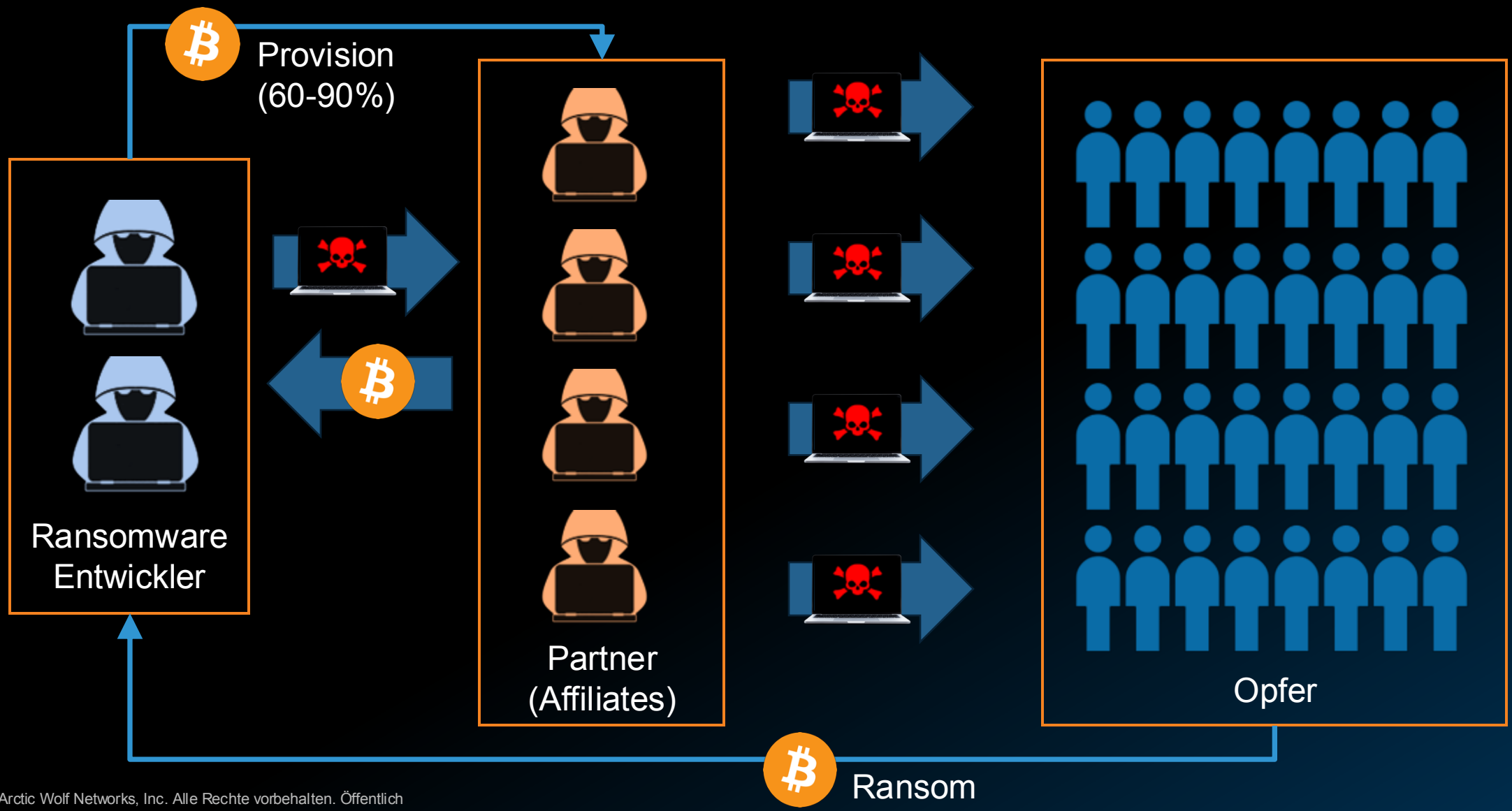
JÄHRLICHER ANSTIEG DER AUSGABEN:
11 %

Quellen: IC3, Gartner, It-Harvest

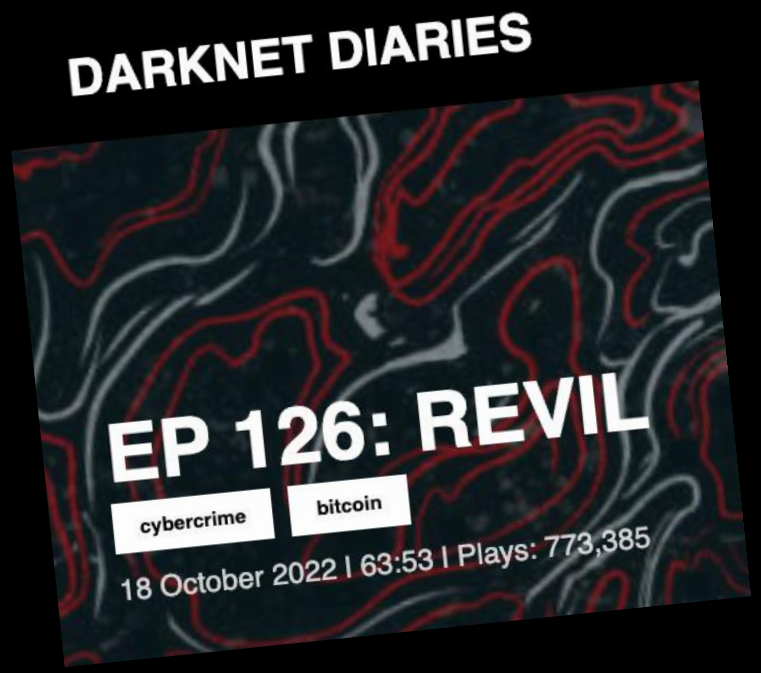
Warum?

#1: Geld regiert die Welt!

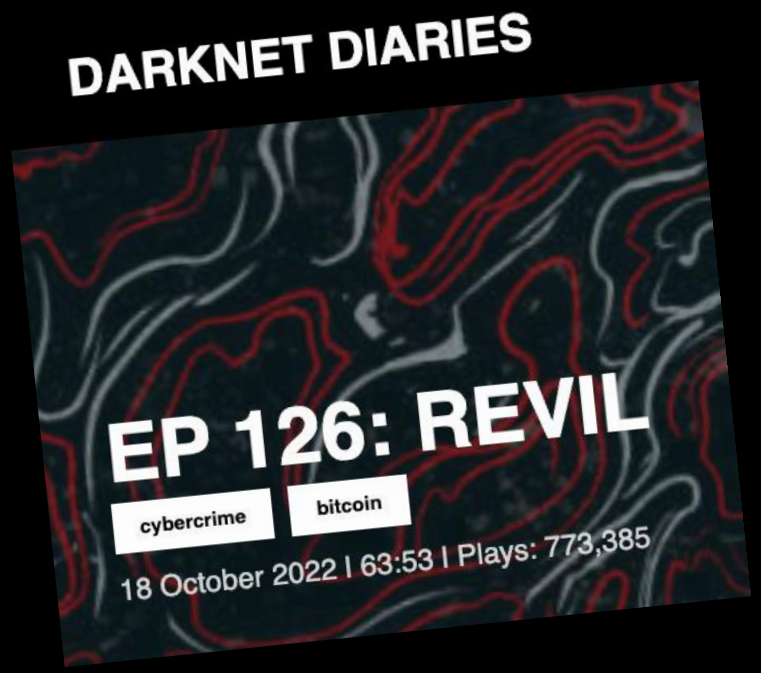
Ransomware as a Service (RaaS)

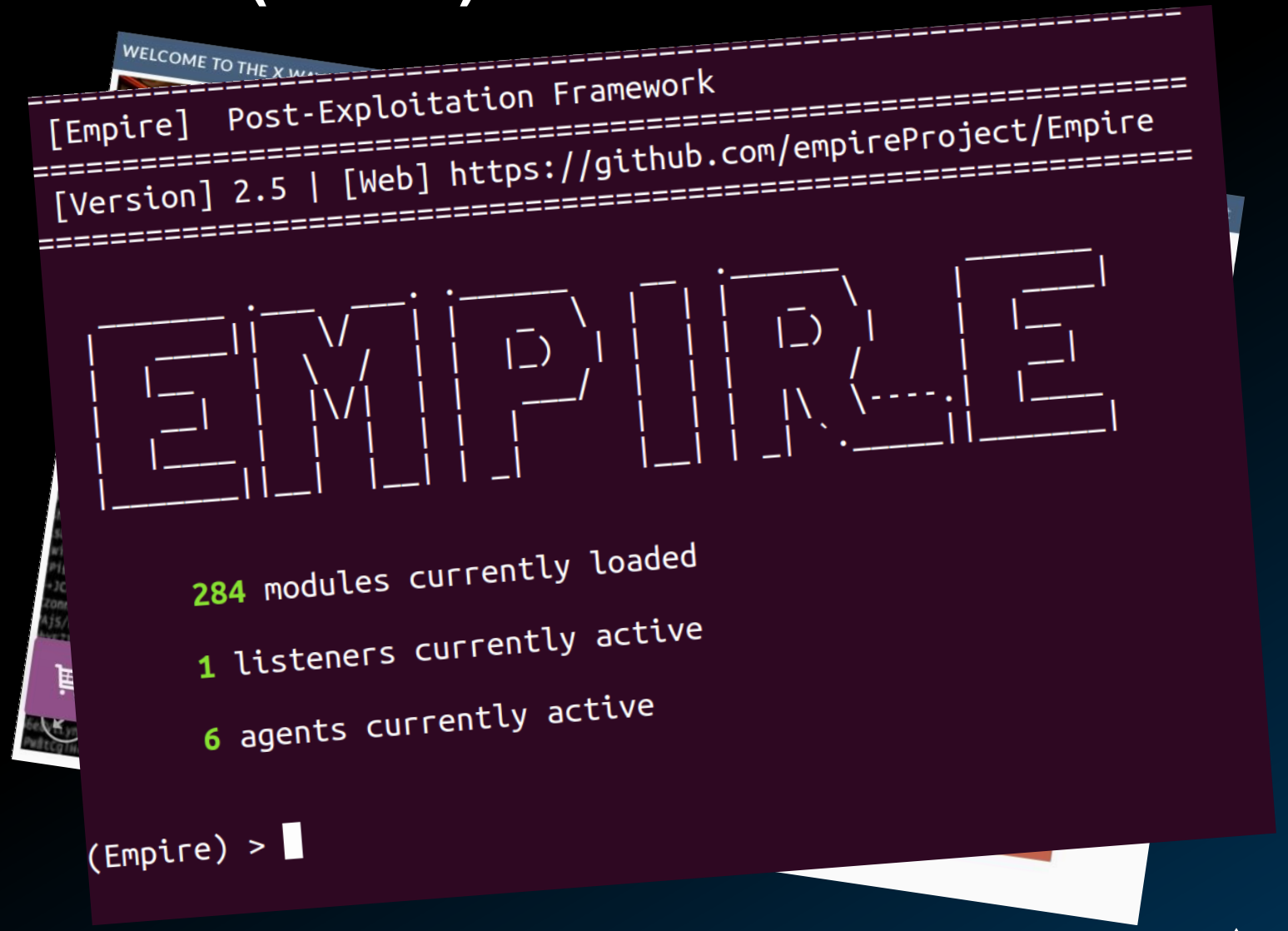


Ransomware as a Service (RaaS)

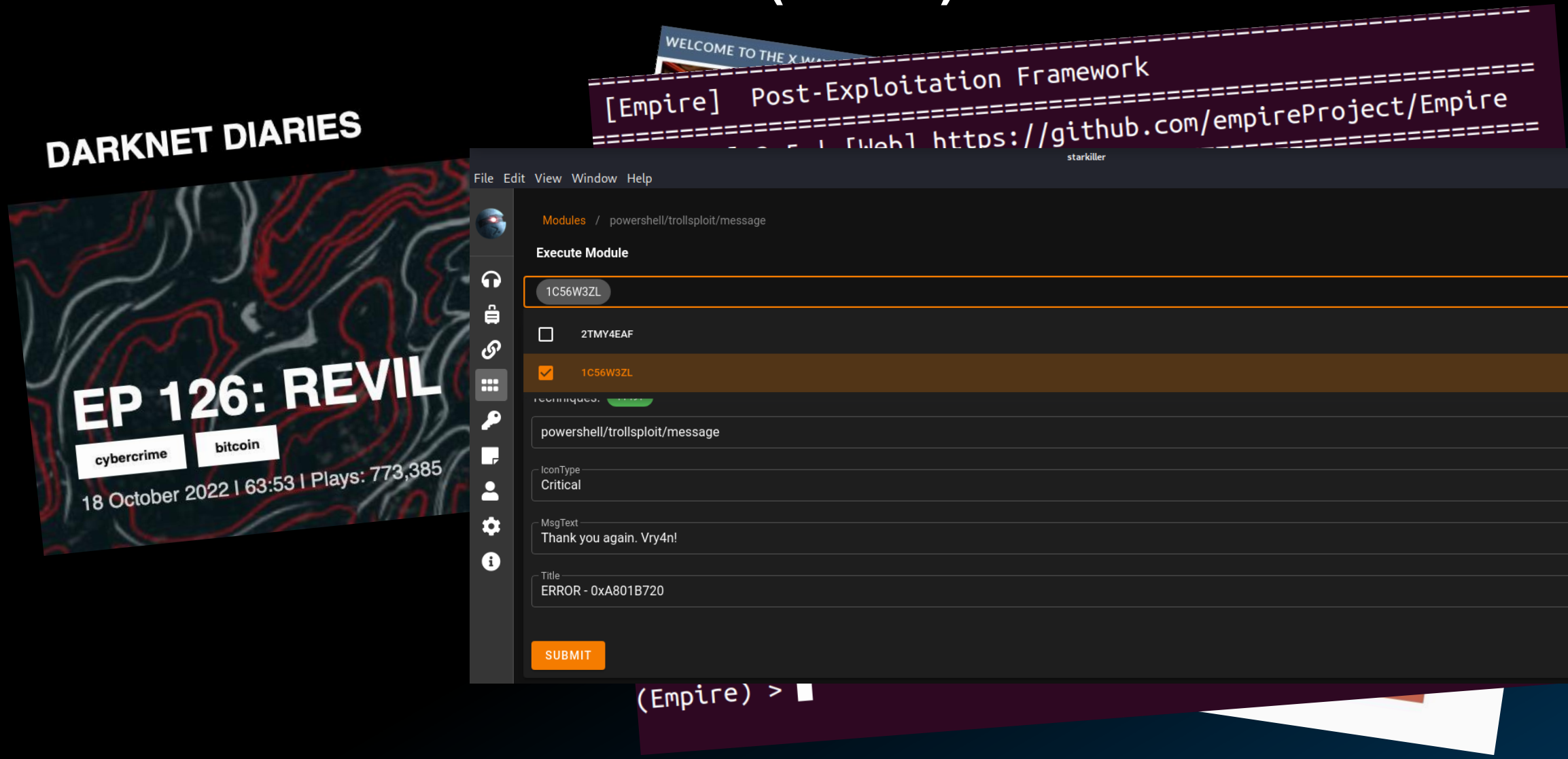


Ransomware as a Service (RaaS)





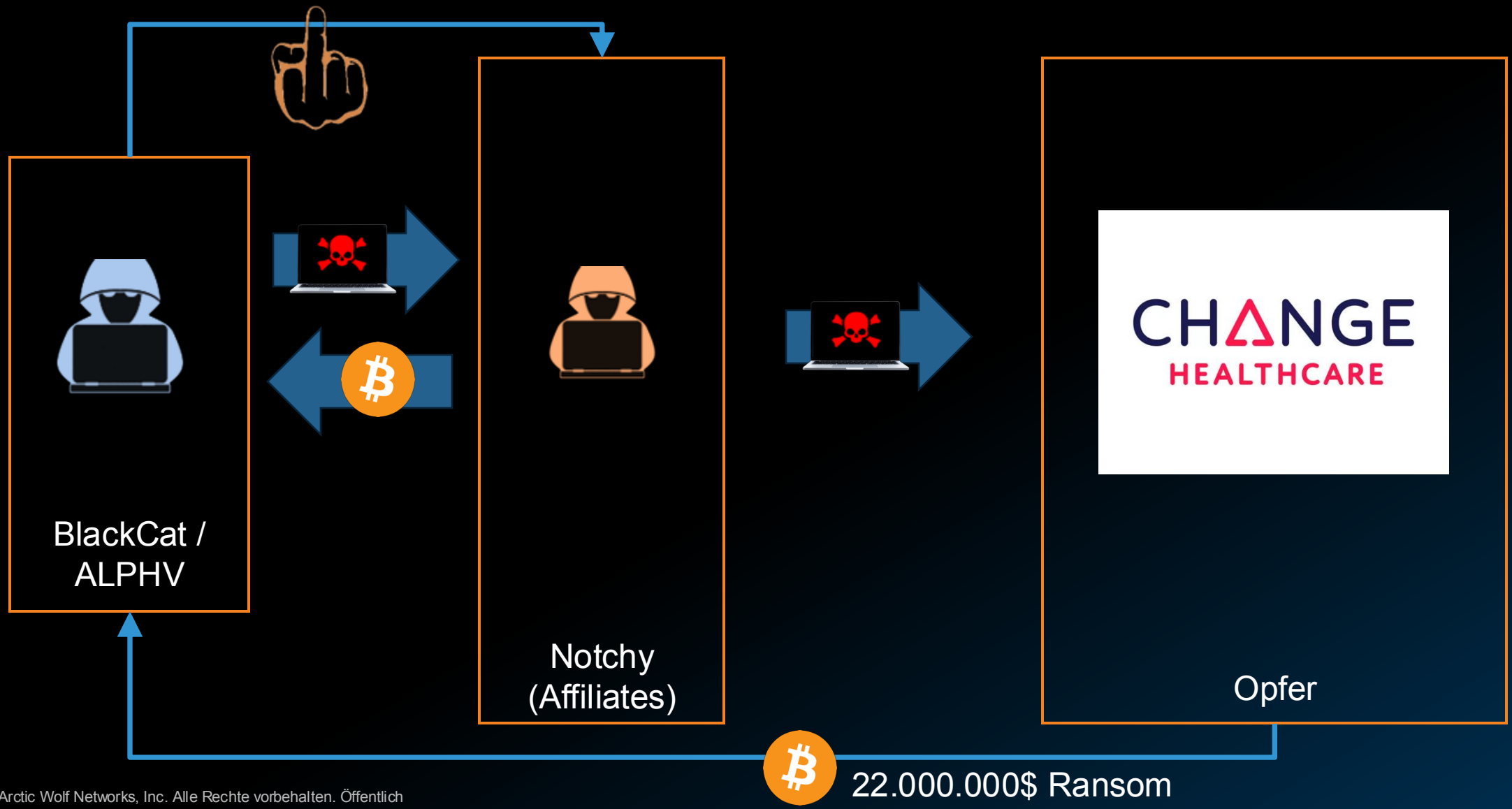
Ransomware as a Service (RaaS)



Change Healthcare (Februar 2024)

Anbieter eines Zahlungssystems, innerhalb des US-amerikanischen Gesundheitssystems.

Ransomware as a Service (RaaS)



Auf dem neuesten Stand bleiben

https://www.ransomware.live/map/DE

https://konbriefing.com/de-topics/hackerangriff-deutschland.html

#2: Es ist einfach!

War hat in den letzten 12 Monaten?

- DKMI, SPF, DMARC für Email konfiguriert?
- Scan von außen durchgeführt? Welche Dienste sind ohne VPN erreichbar und „verwundbar“?
- Ein AD Kerberos Assessment durchgeführt und das Golden Ticket zurückgesetzt?
- Analysiert, wie Powershell im Unternehmen eingesetzt wird und ein Berechtigungskonzept dazu entwickelt?
- NTLM überprüft und eingeschränkt (Print Nightmare)
- CIS Benchmarking auf Server und Clients durchgeführt?
- Schachstellenmanagement eingeführt und das patchen priorisiert?

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | country:"DE" product:"Remote Desktop Protocol" | Account

TOTAL RESULTS

190,442

TOP CITIES

Frankfurt am Main	66,673
Falkenstein	25,593
Berlin	23,452
Düsseldorf	23,358
Nürnberg	18,716

More...

TOP PORTS

3389	189,670
3388	554
33889	218

TOP ORGANIZATIONS

Contabo GmbH	38,292
Hetzner Online GmbH	30,585
Deutsche Telekom AG	12,211
IONOS SE	10,017
1&1 IONOS SE	9,279

More...

View Report | Browse Images | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

62.171.164.98

vmi1460062.contaboserver.net

Contabo GmbH

Germany, Frankfurt am Main

self-signed

SSL Certificate

Issued By:

|- Common Name:

vmi1460062

Issued To:

|- Common Name:

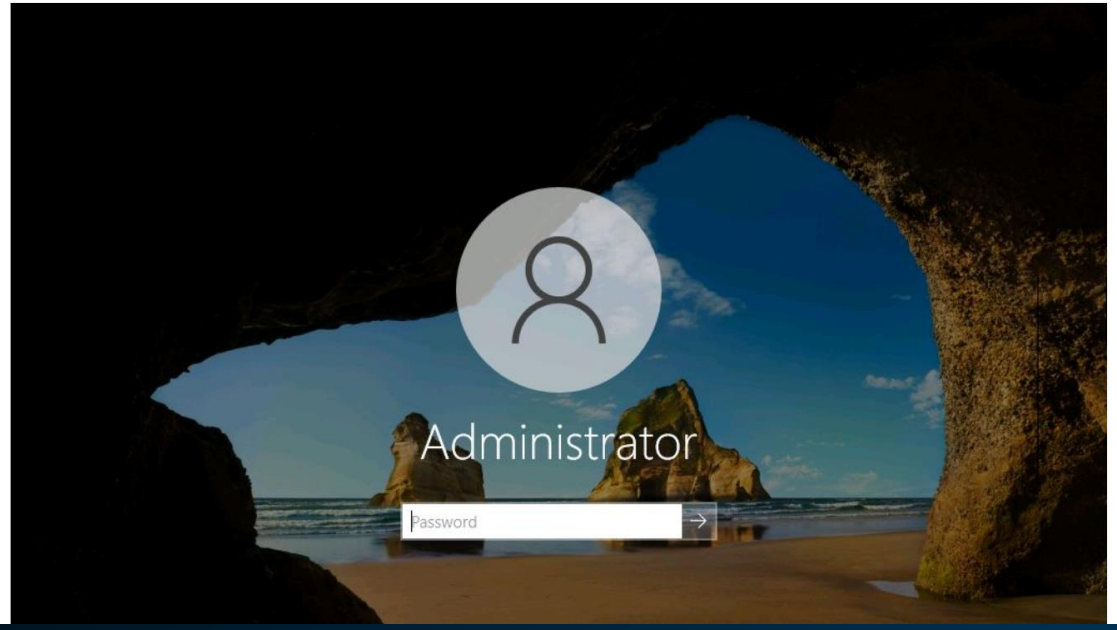
vmi1460062

Supported SSL Versions:

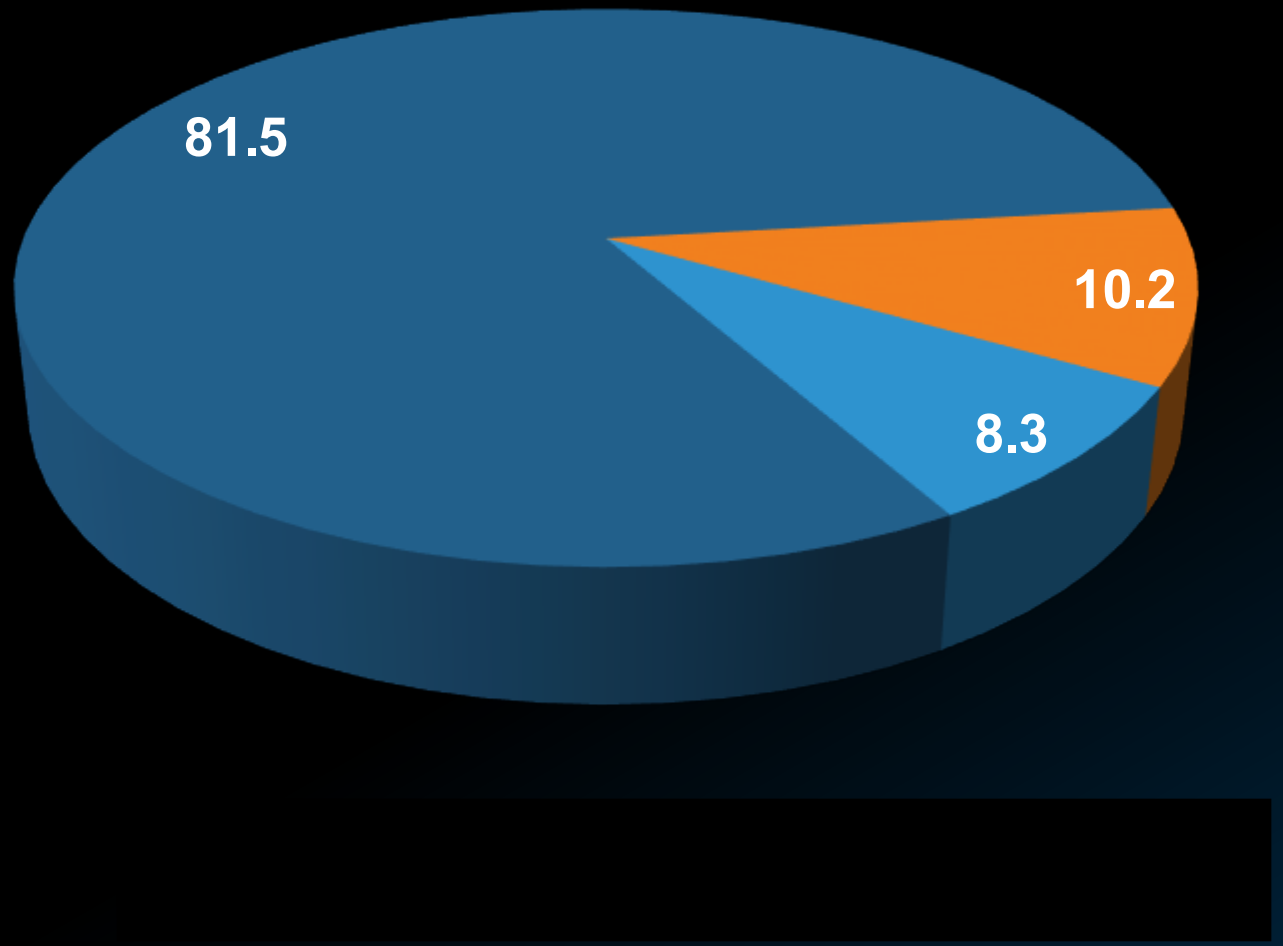
TLSv1, TLSv1.1, TLSv1.2

2024-11-13T07:49:27.929998

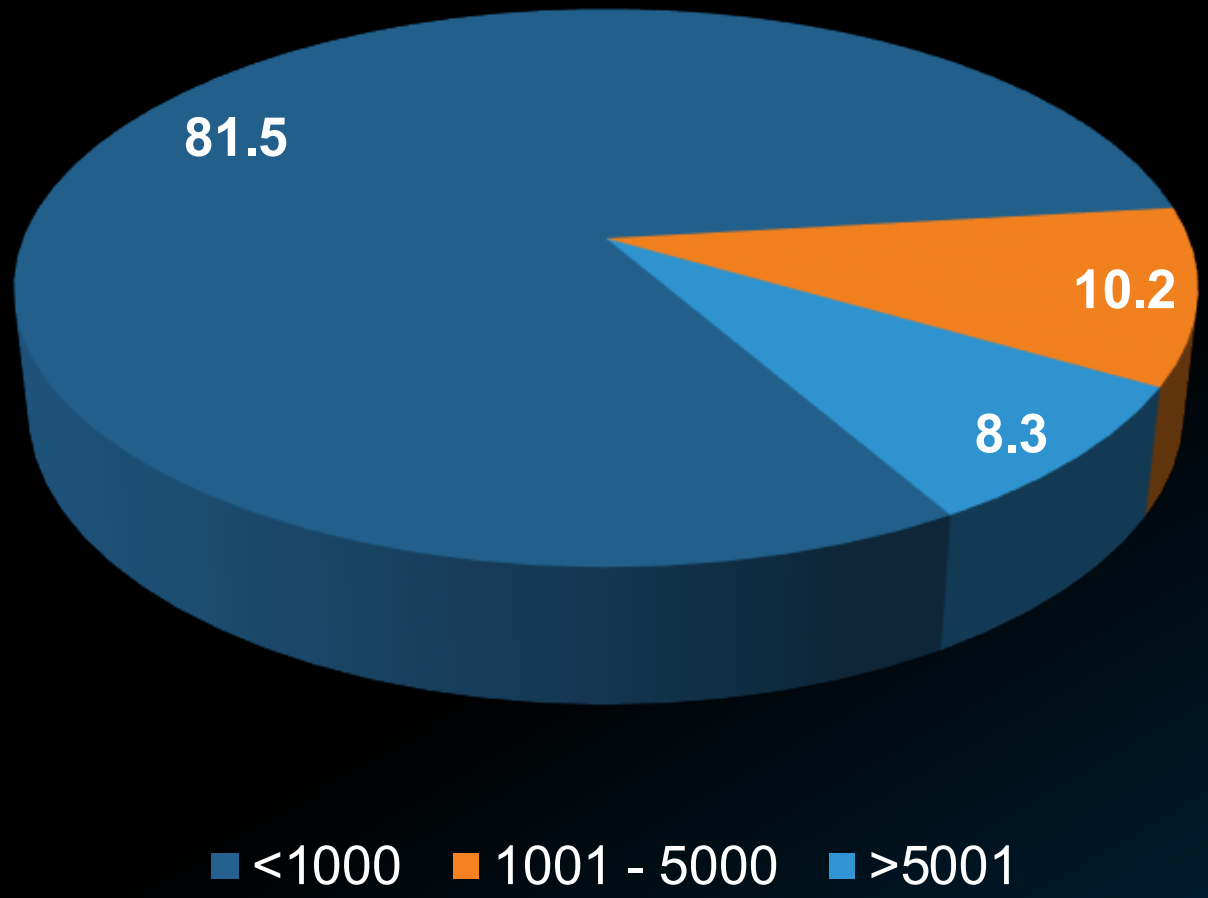
```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows Server 2022
  OS Build: 10.0.20348
  Target Name: VMI1460062
  NetBIOS Domain Name: VMI1460062
  NetBIOS Computer Name: VMI1460062
  DNS Domain Name: ...
```



Betroffene Unternehmen



Betroffene Unternehmen



Antworten der Industrie?!?

Marketing und Buzzwords

SOC

SIEM

XDR

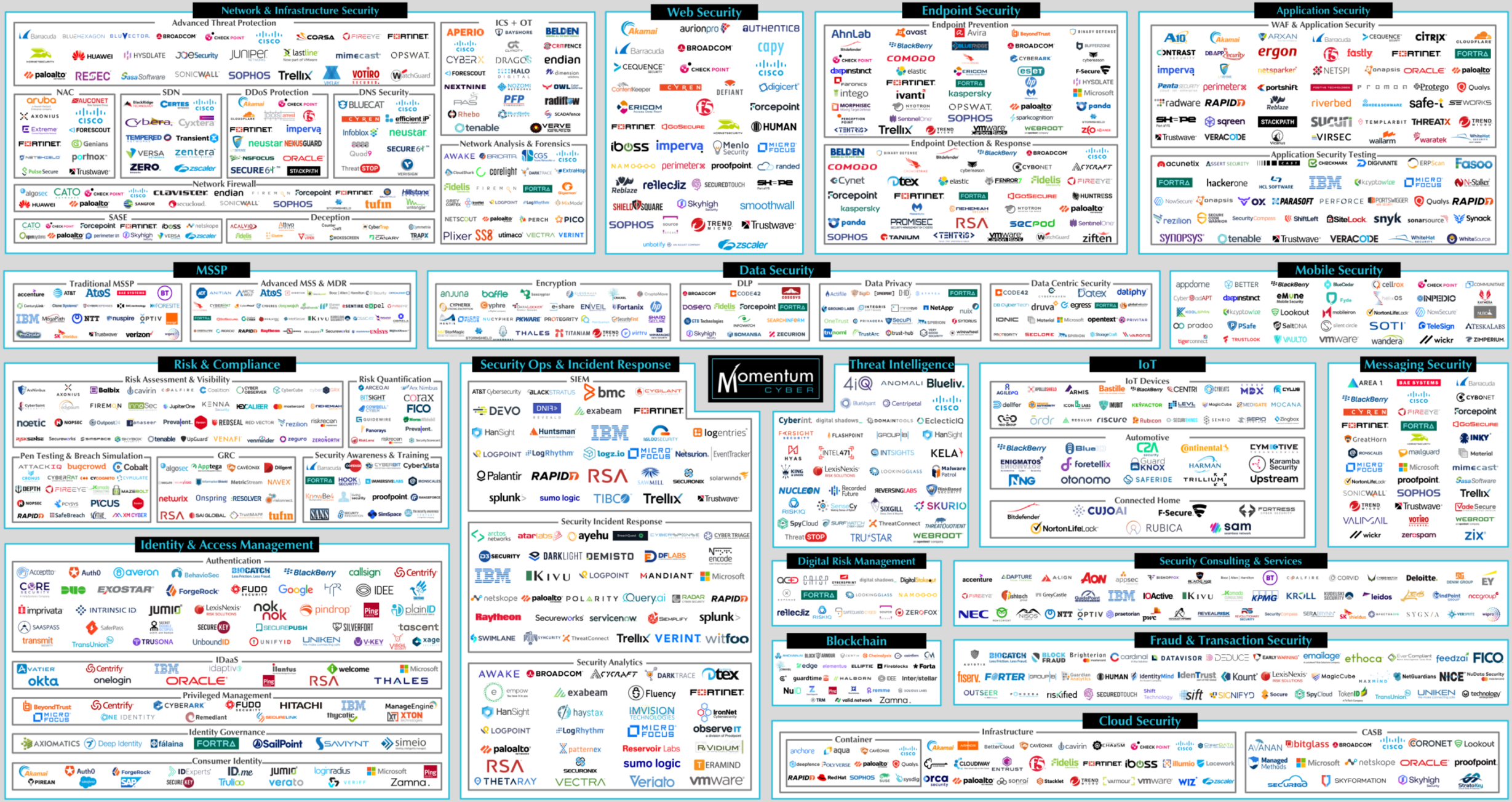
MDR

MXDR

EDR

Plattform

CYBER SCAPE 2023



Marketing und Buzzwords

SOC

SIEM

XDR

MDR

ML (Machine Learning)

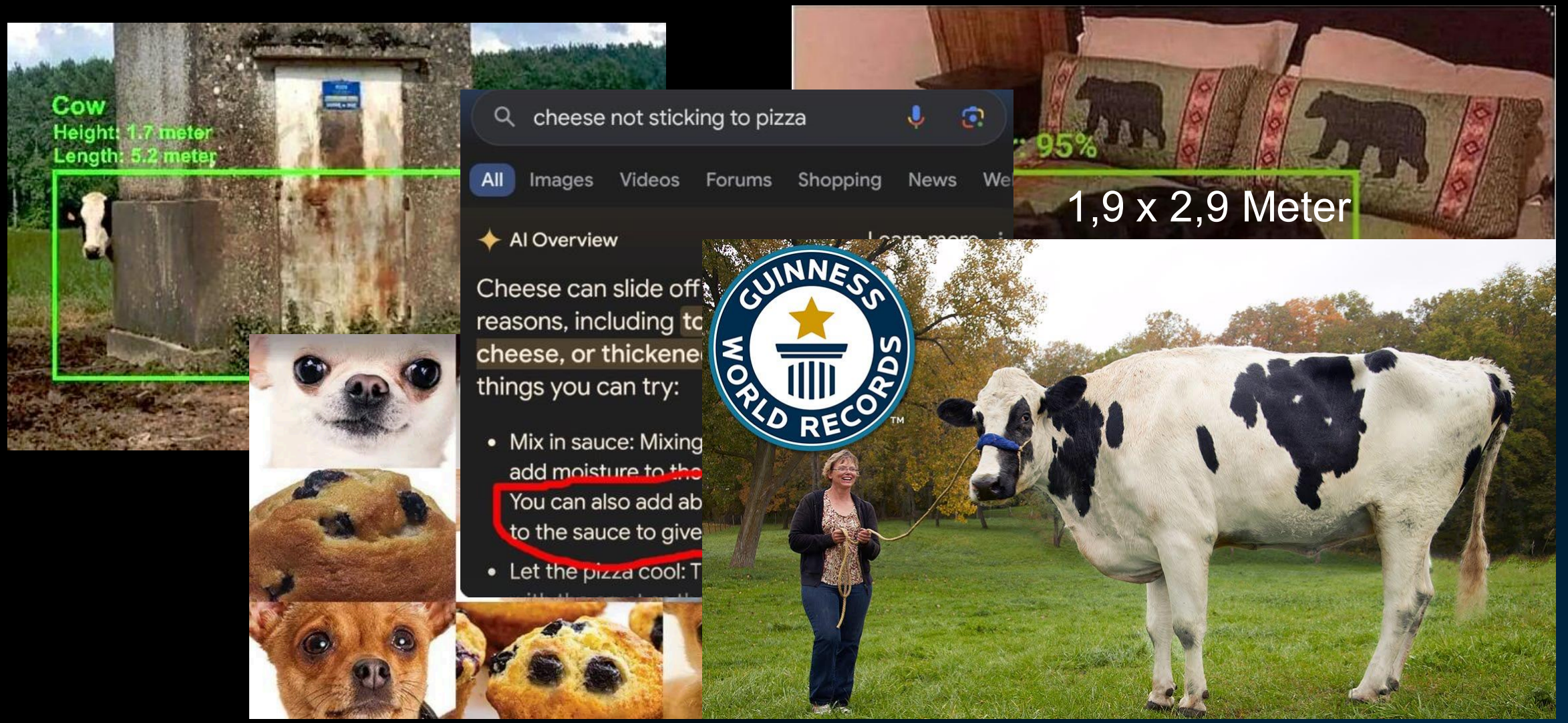
MXDR

KI (AI)

EDR

Plattform

AI&ML kann den Mensch nicht ersetzten



AI&ML kann den Mensch nicht ersetzten

Der Kontext ist der Schlüssel!

In Cybersecruity bezieht sich “Kontext” auf die spezifischen Umstände, Bedingungen und Informationen, die eine Sicherheitsmaßnahme, einen Vorfall oder eine Bedrohung umgeben. Die Analyse sowie die Reaktion werden damit maßgeblich beeinflusst.

Wie helfen wir als Security Operations Partner?

Worauf es wirklich ankommt!

Bundesamt für Sicherheit in der Informationstechnik

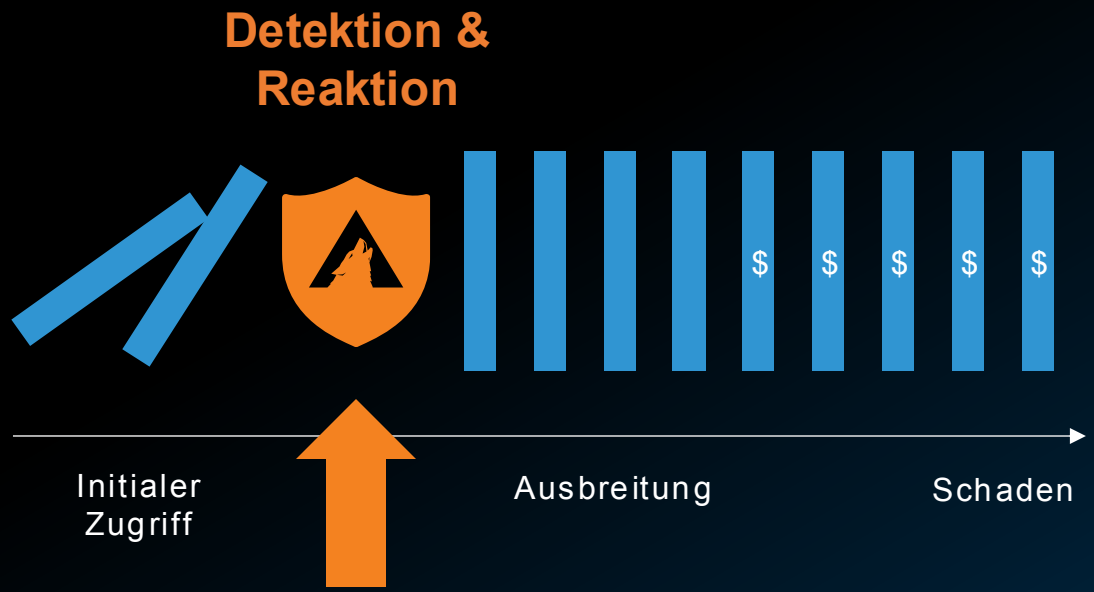
BSI IT Grundschutz

MDR / Managed SOC = Reaktion

> 90% [2]
Reduzierte Auswirkungen

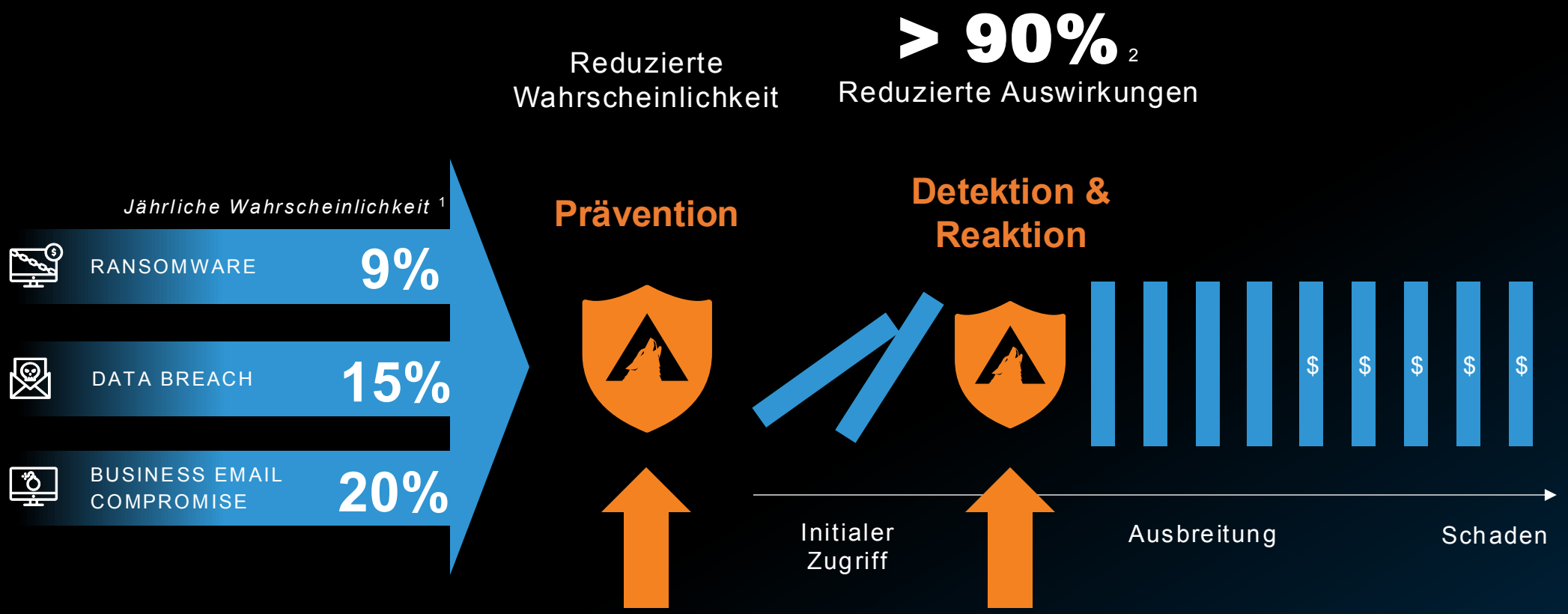
Jährliche Wahrscheinlichkeit [1]

RANSOMWARE	9%
DATA BREACH	15%
BUSINESS EMAIL COMPROMISE	20%



[1] ACAMS, 2022; IBM, 2019; TechStrong Group, 2023
[2] Forrester, 2023

Arctic Wolf = Prävention + Reaktion



[1] ACAMS, 2022; IBM, 2019; TechStrong Group, 2023
[2] Forrester, 2023

SECURITY OPERATIONS PARTNER

2012
gegründet

750+
Security Engineers

24x7
Deutsch und Englisch

98%
Zufriedene Kunden in Europa

7.500+
SOP Kunden weltweit

ERPROBT, GETESTET UND BEWÄHRT

IDC
2X LEADER
MDR MarketScape

Gartner Peer Insights™
AM STÄRKSTEN EMPFOHLEN
MDR, Schwachstellenanalyse und Security Awareness

CNBC DISRUPTOR 50
3-FACHER GEWINNER
Einziges Cybersecurity-Unternehmen überhaupt

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE
AICPA SOC
ZERTIFIZIERT

Die Kombination aus Technologie und Menschen

TECHNOLOGIE

Security Journey

Strukturierte Begleitung für die Verbesserung der Abwehrstrategien

Plattform

Die technologische Basis für unsere Prozesse und Services

Concierge Delivery Model

MENSCHEN

Deployment

Sicherstellen, dass Ihre Umgebung eingerichtet und einsatzbereit ist

Concierge Security Team

Feste Ansprechpartner für die strategische Beratung und regelmäßige Security Workshops

SOC

24x7 Überwachung

Begleitung bei Sicherheitsvorfällen mit Handlungsanweisungen

ARCTIC WOLF LABS

Threat Intelligence
Threat Research
Detection Improvement

Arctic Wolf Security Journey

Onboarding Team & Kunde

CST und Kunde

Phase 1

Onboarding

Ca. 30 Tage

Erbracht durch das Onboarding Team

- Projekt Kick Off & Technical Kick Off
- Vorstellung des Portals
- Sensoren werden verschickt
- Konfiguration der Log-Quellen, ausrollen des Agenten

Phase 2

Die ersten 90 Tage

Go Live

Das Concierge Security Team übernimmt den Service zum Kunden

- Häufige Meetings
- Der Service wird auf die Anforderungen des Kunden angepasst

Kundenspezifische Anpassung

Überprüfung von

- Log-Quellen
- Firewalls
- Active Directory
- Endgeräte

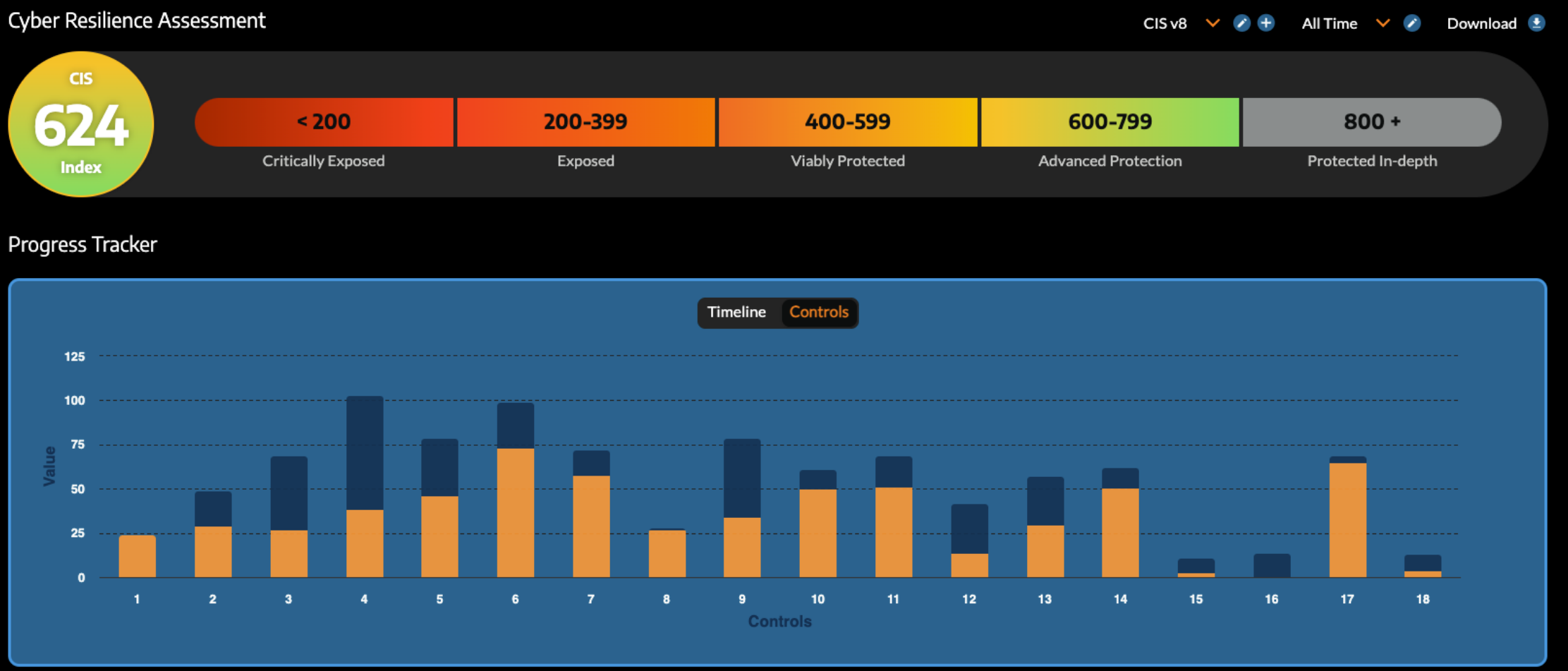
Kennenlernen, Businessprozesse verstehen

Finetuning der Plattform

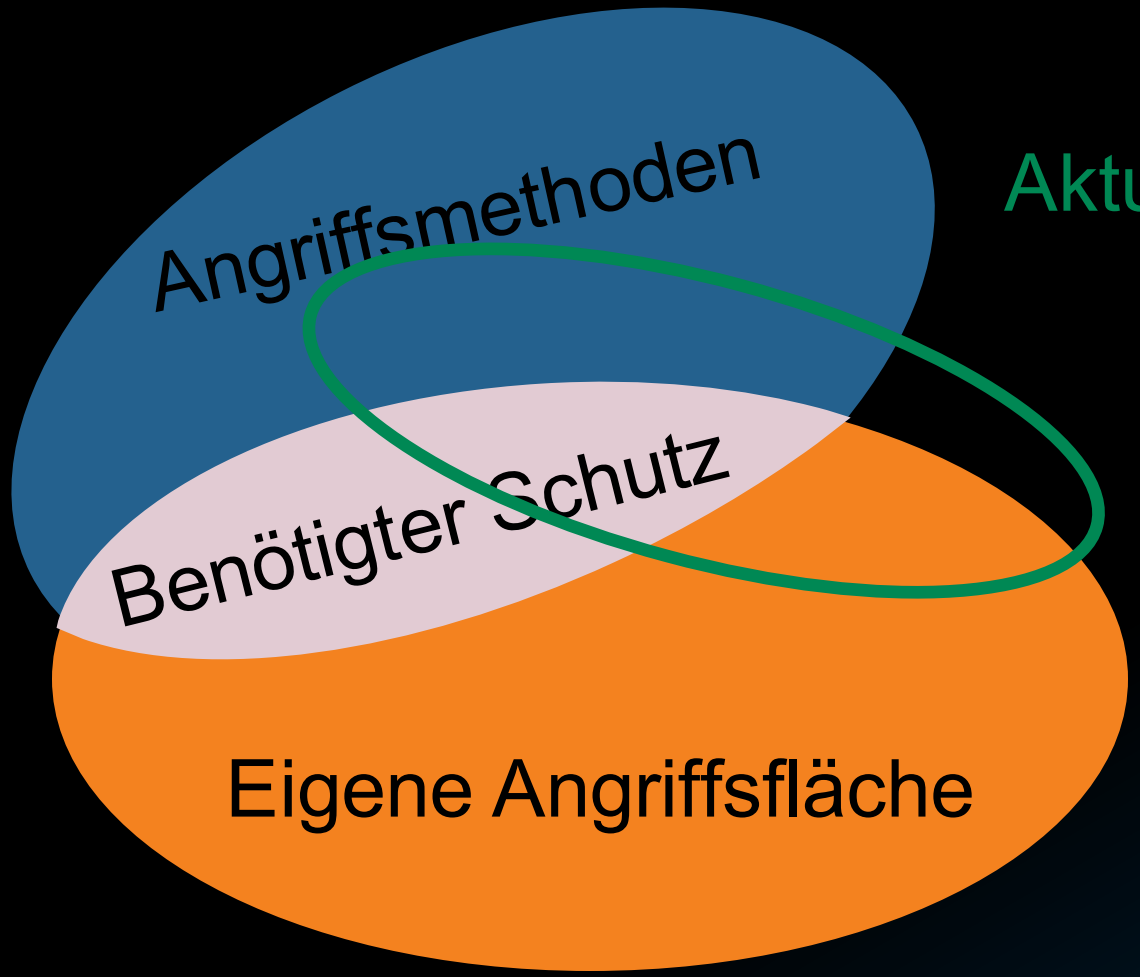
Cyber Resilience Assessment

Phase 3

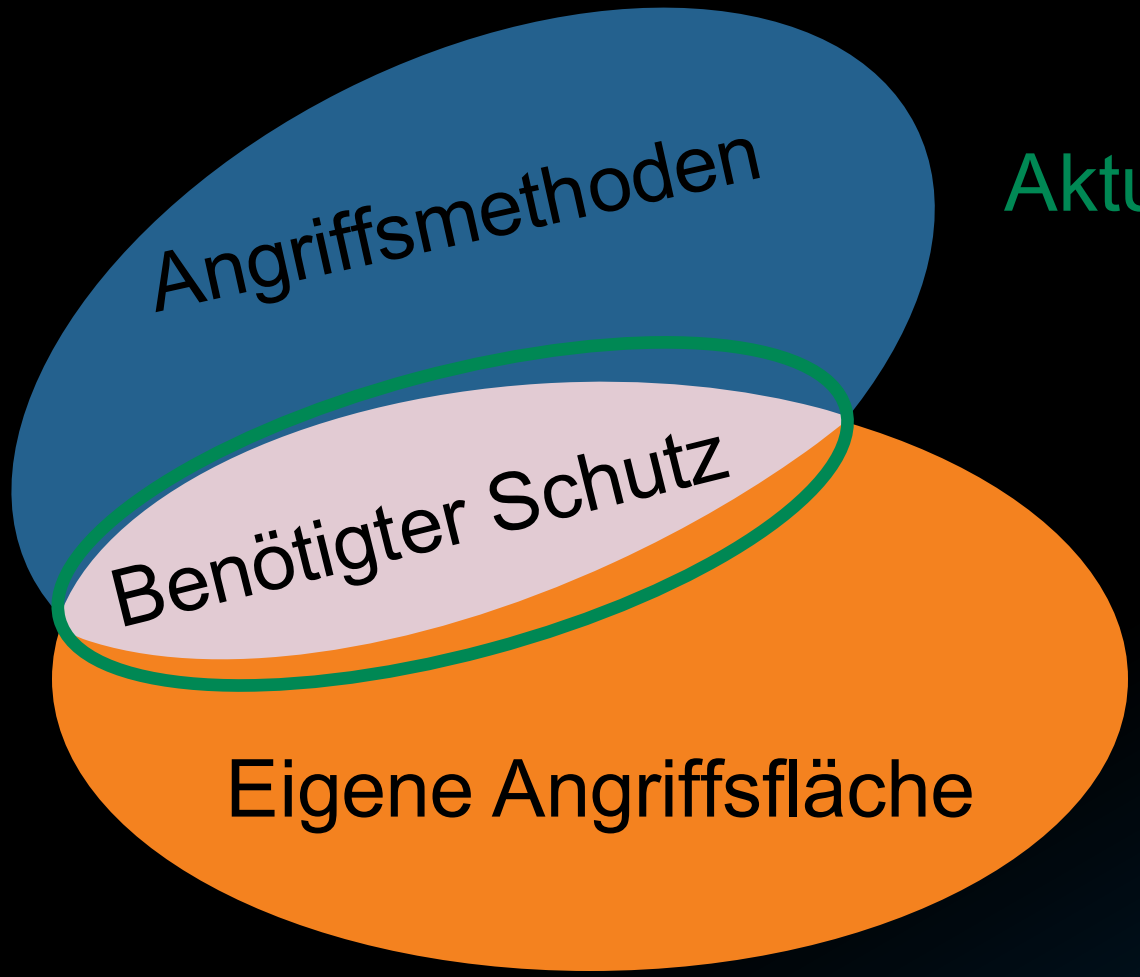
Cyber Resilience Assessment – CIS v8



Anpassung an den erforderlichen Umfang



Anpassung an den erforderlichen Umfang



Aktueller Schutz

Das Concierge Security Team hilft mit

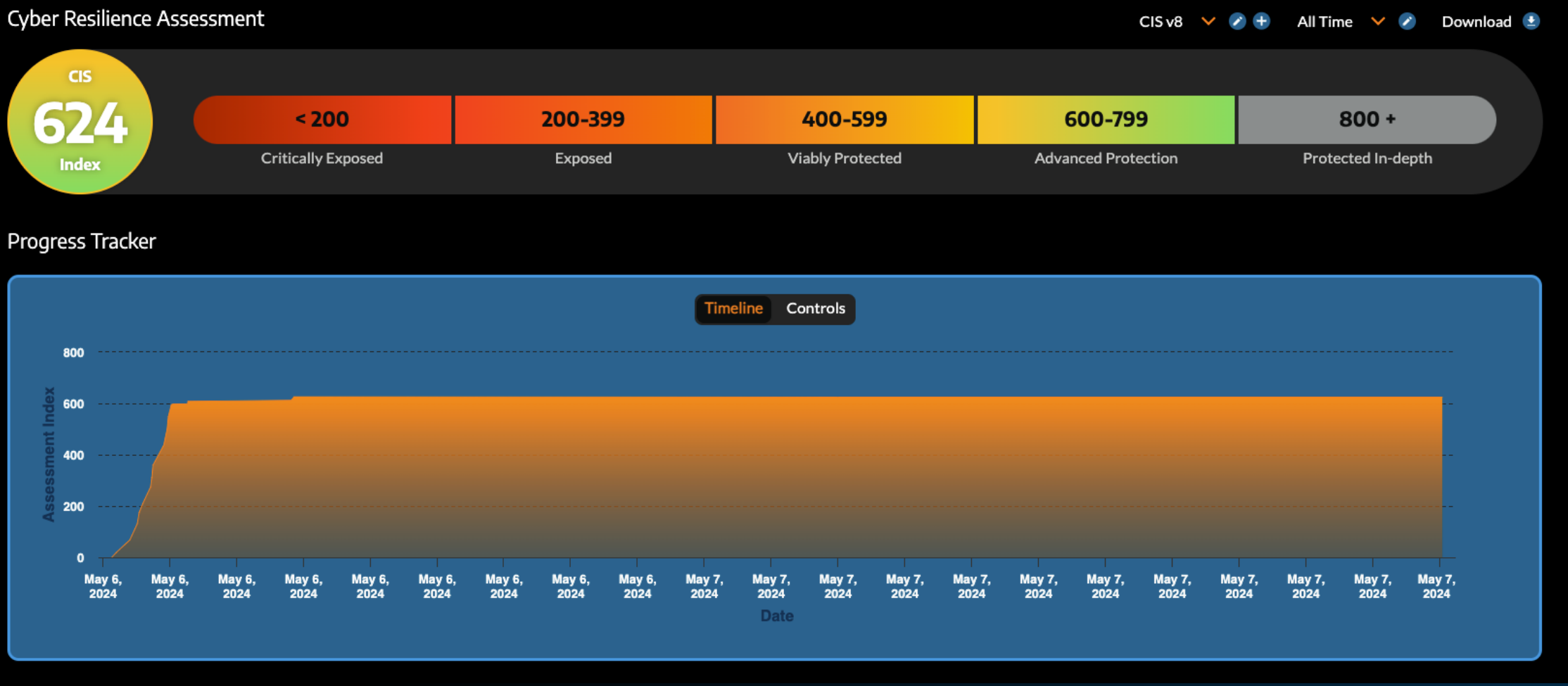
- Fachwissen
- Best Practices
- Kontinuierliche Überprüfungen
- Dokumentation

Ein paar Beispiele

PROAKTIV das Risiko senken

- External Assessment
- FW Assessment (Basic)
- FW Assessment (Advanced)
- O365 Security Recommendations
- Identity and Lifecycle Management
- Patch and Vulnerability Management
- O365 Mail Forwarding Review
- Phishing and Employee Awareness Training
- Ransomware and Malware Hardening
- Group Policy Management Hardening
- Anomalous Traffic Analysis
- Backup Recommendations
- PowerShell Review
- Email Gateways
- AD Attack Vectors
- Architecture and Visibility Assessment
- DNS Security Assessment
- Kerberos Assessment - Kerberoasting
- AD Audit Policy Review
- Credential Access - DCSync Attack
- MS NTLM Assessment
- Supply Chain Risk Best Practice
- Insider Threat Risk Best Practice
- Cloud ID Foundation Review
- CIS Benchmarking
- Email Trust and Authentication Assessment
- Endpoint Security Review
- PsExec Utility Assessment
- Asset Classification and Criticality Review
- Vulnerability Prioritization and Asset Baseline Review
- Threat Landscape and Prioritizations Review
- Customer Incident and Pentest Report
- Pre-Pentest Prep

Cyber Resilience Assessment – CIS v8



Arctic Wolf Security Journey

Onboarding Team & Kunde

CST und Kunde

Phase 1

Onboarding
Ca. 30 Tage

Erbracht durch das Onboarding Team

- Projekt Kick Off & Technical Kick Off
- Vorstellung des Portals
- Sensoren werden verschickt
- Konfiguration der Log-Quellen, ausrollen des Agenten

Phase 2

Die ersten 90 Tage
Go Live

Das Concierge Security Team übernimmt den Service zum Kunden

- Häufige Meetings
- Der Service wird auf die Anforderungen des Kunden angepasst

Kundenspezifische Anpassung

Überprüfung von

- Log-Quellen
- Firewalls
- Active Directory
- Endgeräte

Kennenlernen, Businessprozesse verstehen

Finetuning der Plattform

Cyber Resilience Assessment

Phase 3

Dauerzustand
Fokus nach Kundenwunsch

Regelmäßige Termine

#1 #2 #3 #...

Monatlich **Externe Vulnerability Assessments** und **Darkweb Scans**

Security Bulletins & Threat Hunting bei Mega Events

Security Touchpoints

- Bewertung – Lücken/Risken
- Konfigurations-Checks (z.B. FW, AD)
- Best Practice – Empfehlungen

Unlimitiertes Reporting

Die Kombination aus Technologie und Menschen

TECHNOLOGIE

Security Journey

Strukturierte Begleitung für die Verbesserung der Abwehrstrategien

Plattform

Die technologische Basis für unsere Prozesse und Services

Concierge Delivery Model

MENSCHEN

Deployment

Sicherstellen, dass Ihre Umgebung eingerichtet und einsatzbereit ist

Concierge Security Team

Feste Ansprechpartner für die strategische Beratung und regelmäßige Security Workshops

SOC

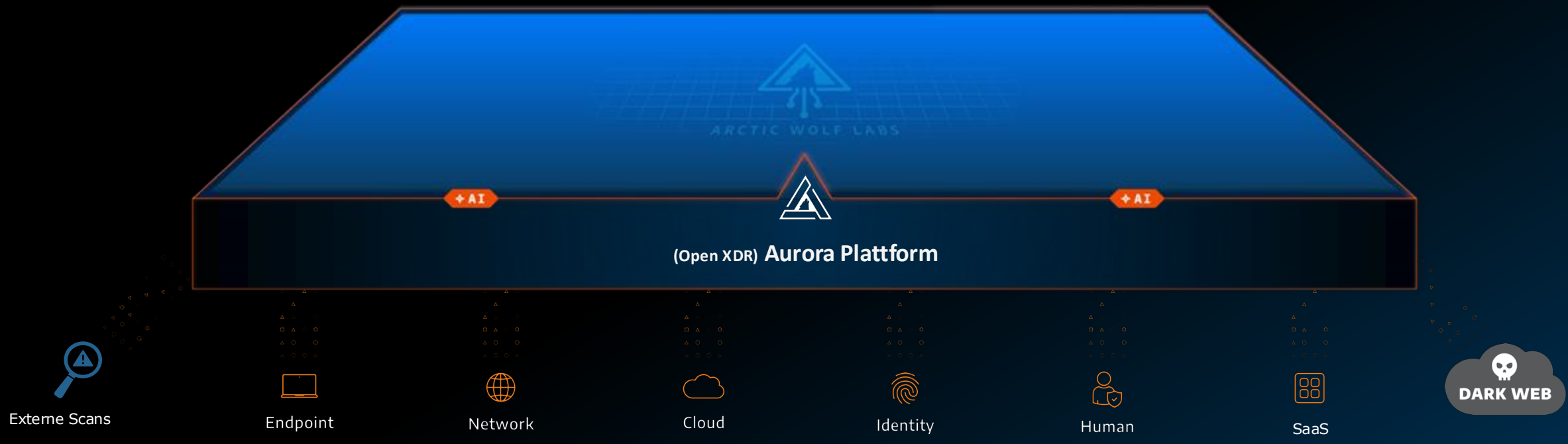
24x7 Überwachung

Begleitung bei Sicherheitsvorfällen mit Handlungsanweisungen

ARCTIC WOLF LABS

Threat Intelligence
Threat Research
Detection Improvement

SECURITY OPERATIONS PARTNER



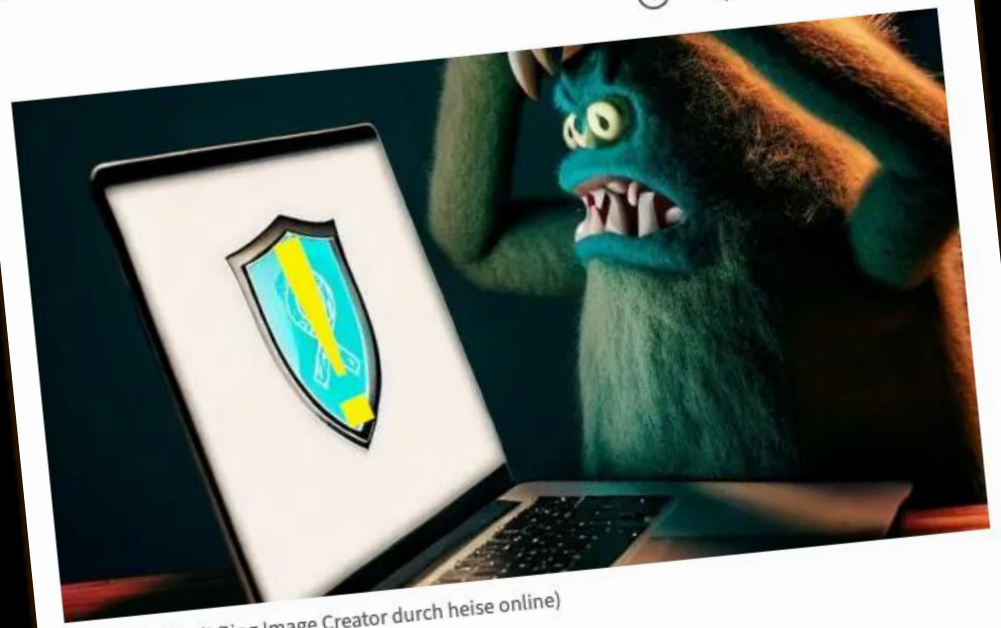
Open XDR = Herstellerneutral

Jedes Tool kann versagen

Microsoft Defender: Der Erkennung mit Komma entgehen

Ein IT-Forscher hat entdeckt, dass sich die Erkennung des Microsoft Defenders mit einem Komma austricksen lässt.

106



(Bild: Erstellt mit Bing Image Creator durch heise online)

UPDATE 12.02.2024, 12:59 Uhr Lesezeit: 2 Min. | Security

Von Dirk Knop

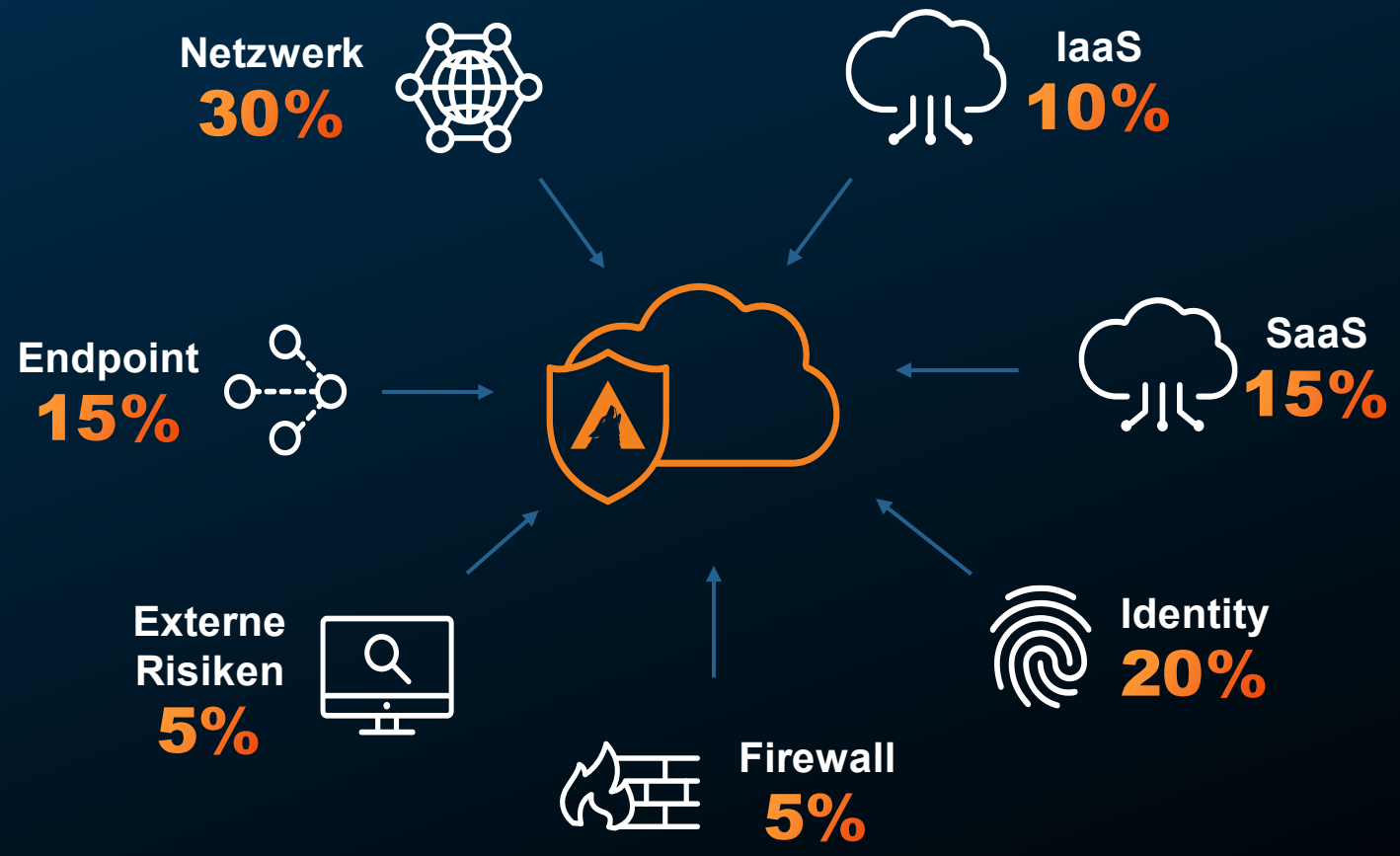
https://www.heise.de/news/Microsoft-Defender-Der-Erkennung-mit-Komma-entgehen-9625770.html

Abdeckung aller Angriffsvektoren

83%

aller Tickets stammen aus Arctic Wolf Erkennungen und wurden von vorhandenen Tools nicht erkannt

Bestätigte Fälle, basierend auf den ersten IOC



Schwarmintelligenz durch ARCTIC WOLF LABS

Threat Intelligence und Security Research

Detection & Response Engineering

KI und Datenwissenschaft

Security Posture Engineering

SECURITY OPERATIONS PARTNER

Open XDR = Herstellerneutral

SECURITY OPERATIONS PARTNER

Open XDR = Herstellerneutral

Ransomware Chat

Ransomware.live - Negotiatic

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

Darkweb-Scanning für ATO-Risk

1

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

Thank you!

Is it possible to share what means initial access? Which username (I assume

Ransomware.live - Negotiatic

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

SP-AUTH-065

Kerberos Assessment

2

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

Thank you!

Is it possible to share what means initial access? Which username (I assume

Ransomware.live - Negotiatic

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

3

Thank you!

Is it possible to share what means initial access? Which username (I assume

24x7x365
MDR

Ransomware.live - Negotiatio

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

4

Awareness Training

Thank you!

Is it possible to share what means initial access? Which username (I assume

Ransomware.live - Negotiatio

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

SP-RISK-049

Password Policies, Password Managers

5

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

Thank you!

Is it possible to share what means initial access? Which username (I assume

Ransomware.live - Negotiatic

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

Concierge Security Team

Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

6

Thank you!

Is it possible to share what means initial access? Which username (I assume

Ransomware.live - Negotiatio

ransomware.live/nego/akira/20231209

Managed Bookmarks | DHL | flammi.home | AWN | Cyber Security | Excel Tips | Amazon.de - Rück... | DeepL | AnyImage.io | Private | Scripting | Flammi Wiki.js | AWN Demo | Zoom Tim | Threat Event Inves... | SE Depot | medocino files 5C... | DACH - KPI | Sales... | Event-Planer

RANSOMWARE.LIVE

Search...

- Recent victims
- Cyberattacks in the press
- Ransomware Groups
- Negotiation Chats
- Ransom Notes
- Statistics
- Victims by country
- Cartography
- Intel...
- API
- About

I will provide in an hour.

[redacted]_dellog.txt // 2.54 MB

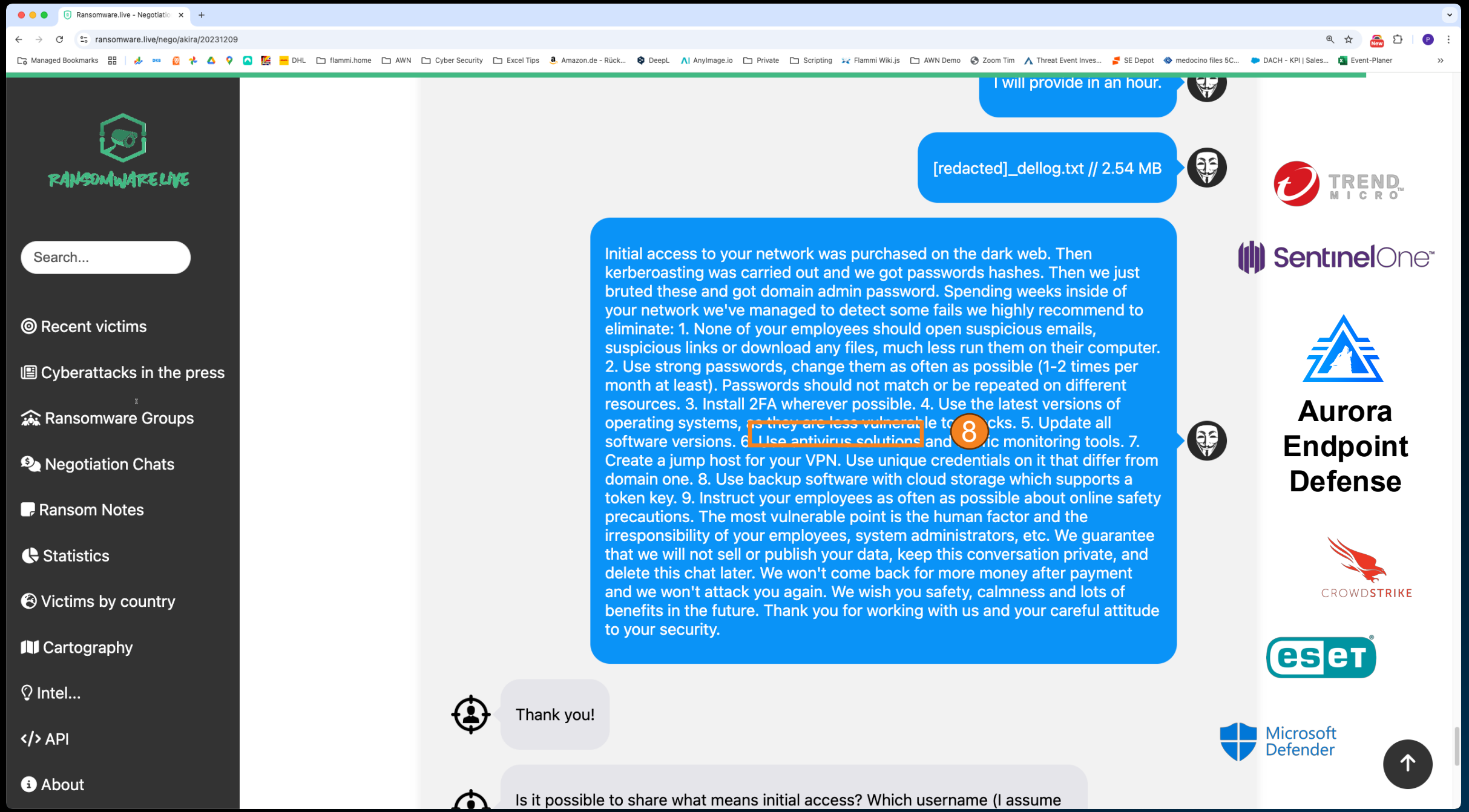
Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.

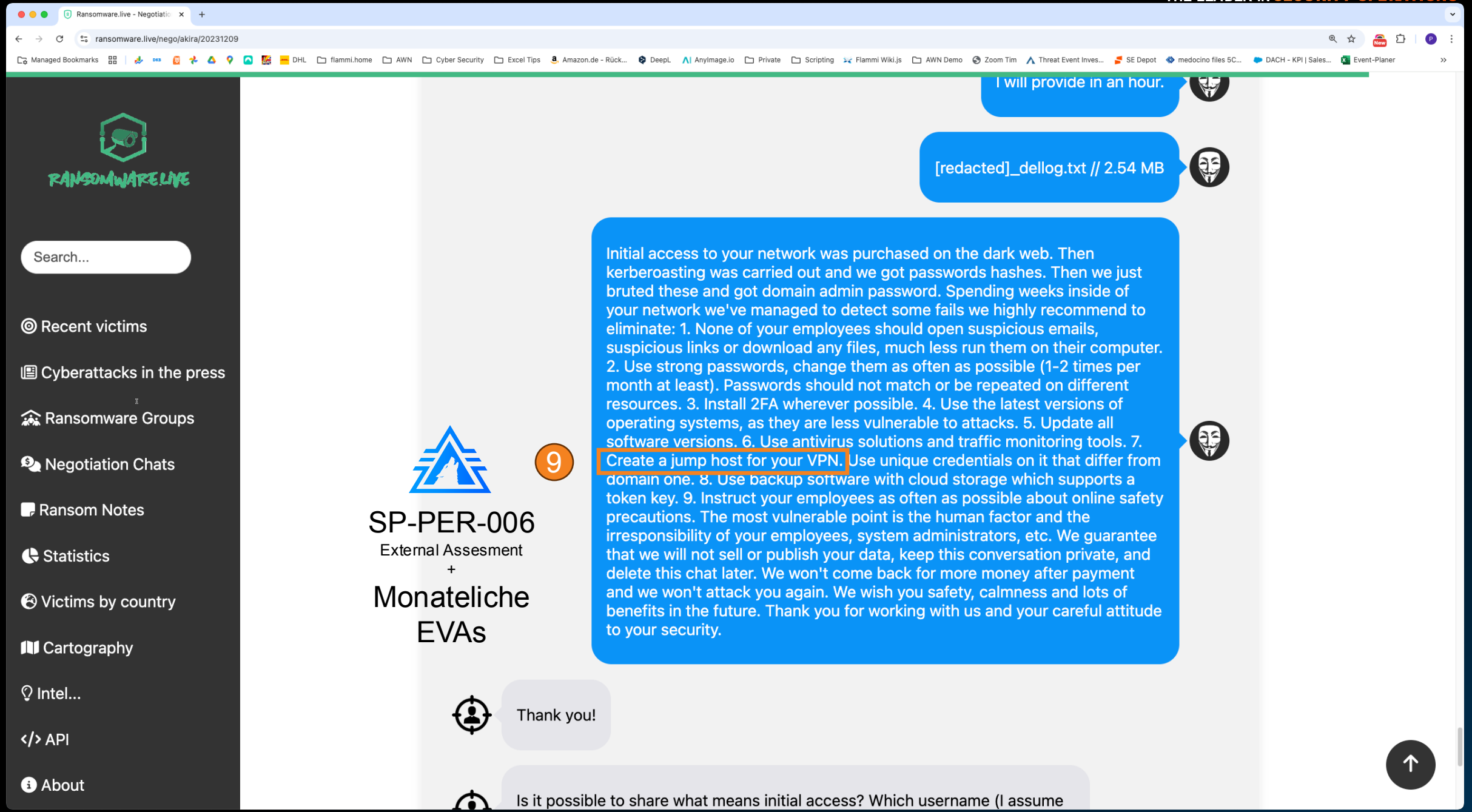
7

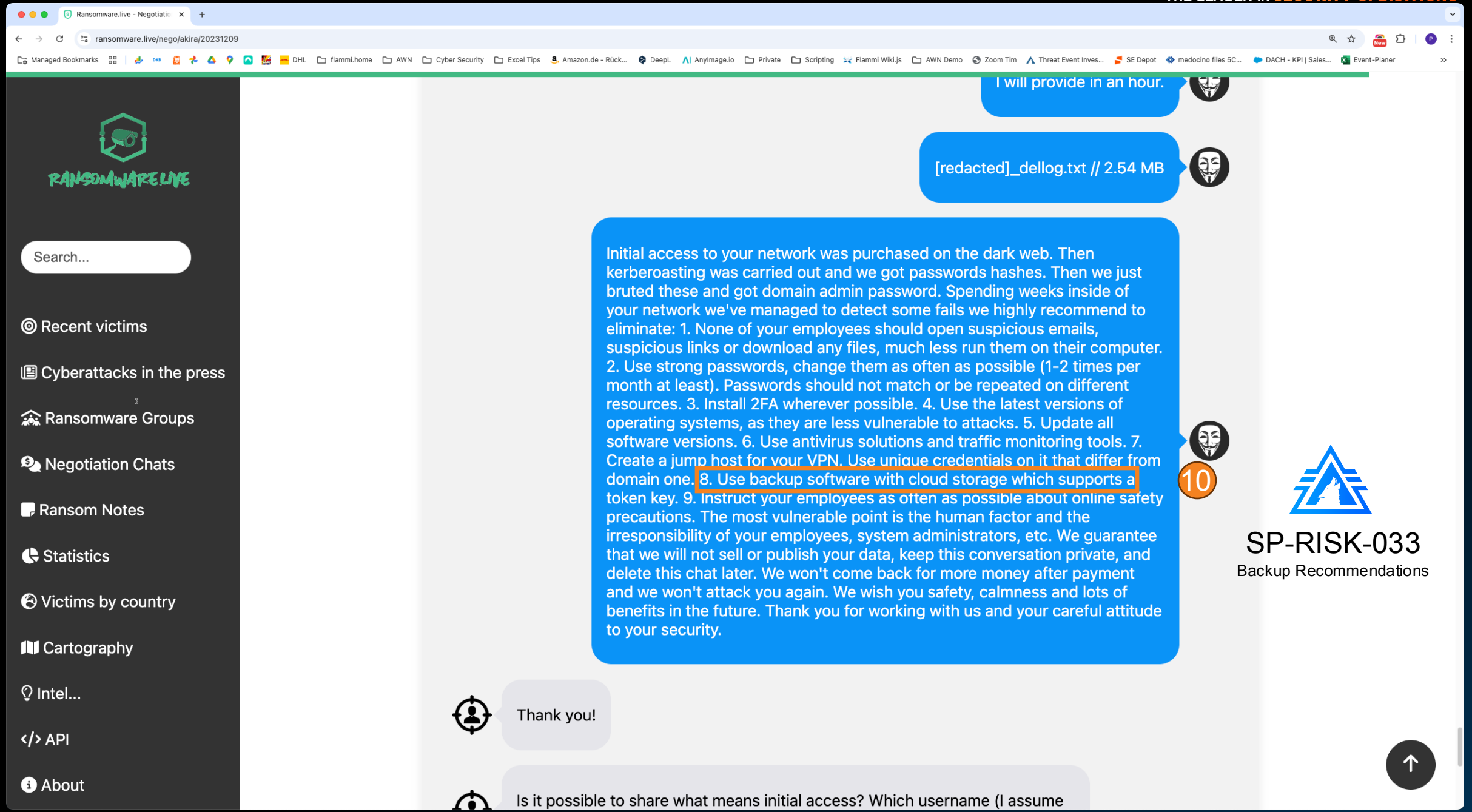
Managed Risk

Thank you!

Is it possible to share what means initial access? Which username (I assume


Ransomware.live - Negotiatio
ransomware.live/nego/akira/20231209
RANSOMWARE.LIVE
Search...
Recent victims
Cyberattacks in the press
Ransomware Groups
Negotiation Chats
Ransom Notes
Statistics
Victims by country
Cartography
Intel...
API
About
I will provide in an hour.
[redacted]_dellog.txt // 2.54 MB
Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and heuristic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.
8
Thank you!
Is it possible to share what means initial access? Which username (I assume
TREND MICRO
SentinelOne
Aurora Endpoint Defense
CROWDSTRIKE
eset
Microsoft Defender


Ransomware.live - Negotiatic
ransomware.live/nego/akira/20231209
RANSOMWARE.LIVE
Search...
Recent victims
Cyberattacks in the press
Ransomware Groups
Negotiation Chats
Ransom Notes
Statistics
Victims by country
Cartography
Intel...
API
About
I will provide in an hour.
[redacted]_dellog.txt // 2.54 MB
Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate: 1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer. 2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources. 3. Install 2FA wherever possible. 4. Use the latest versions of operating systems, as they are less vulnerable to attacks. 5. Update all software versions. 6. Use antivirus solutions and traffic monitoring tools. 7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one. 8. Use backup software with cloud storage which supports a token key. 9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc. We guarantee that we will not sell or publish your data, keep this conversation private, and delete this chat later. We won't come back for more money after payment and we won't attack you again. We wish you safety, calmness and lots of benefits in the future. Thank you for working with us and your careful attitude to your security.
9
SP-PER-006
External Assesment
+
Monateliche
EVAs
Thank you!
Is it possible to share what means initial access? Which username (I assume



SP-RISK-033

Backup Recommendations

Danke!

Backup

Südwestfalen IT Hack

- Cisco ASA nicht gepatcht - CVE-2023-20269 seit Sep. 2023 bekannt
  (Geeignet für Brute-Force-Angriffe gegen Passwörter und Benutzernamen)
- Schwaches Passwort
- Kein MFA

- Keine Detektion
  (über 300 fehlgeschlagene anonyme SMB-Login-Versuche auf 190 Systeme am 18. Oktober)
- Angreifer waren min. 12 Tage im System

- Über 960 Systeme verschlüsselt

Südwestfalen-IT

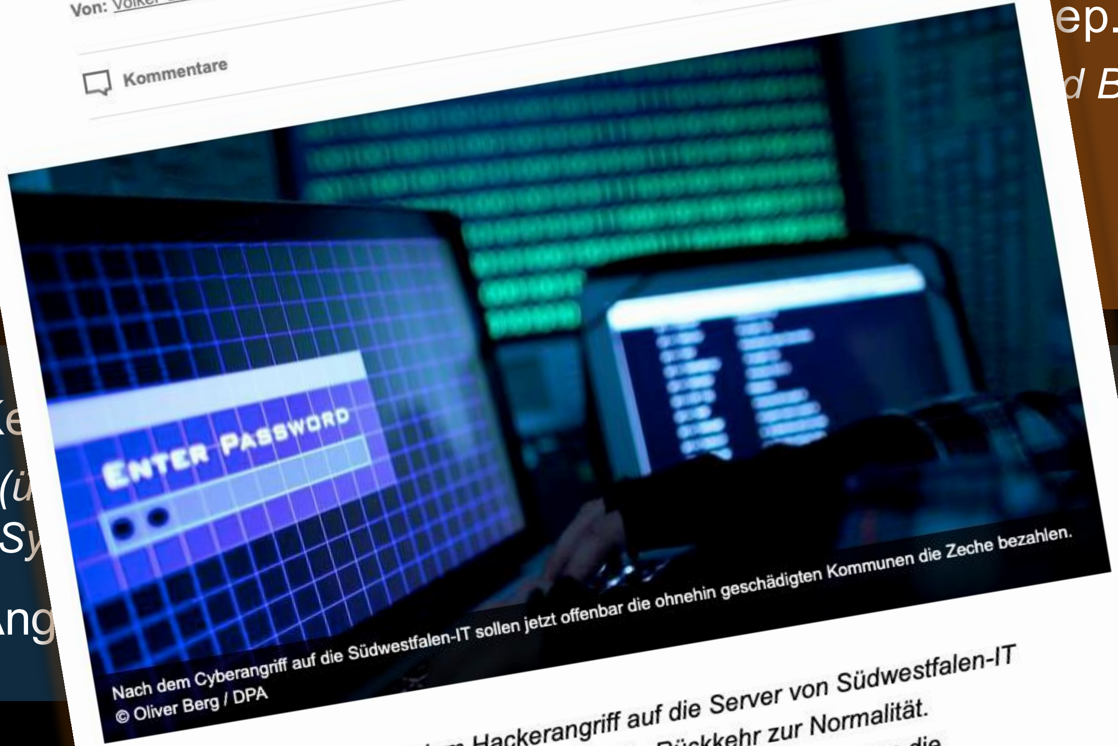
- …ep. 2023 bekannt
  …d Benutzernamen)
- …
- K…
- Ke…
  (ü… Sy… …auf 190
- Ang…
- Über…

Zurück im „Normalmodus“: Südwestfalen-IT bittet Kommunen zur Kasse

09.10.2024, 19:00 Uhr
Von: Volker Griese

Drucken Teilen

Kommentare



Nach dem Cyberangriff auf die Südwestfalen-IT sollen jetzt offenbar die ohnehin geschädigten Kommunen die Zeche bezahlen.
© Oliver Berg / DPA

Fast ein Jahr nach dem Hackerangriff auf die Server von Südwestfalen-IT meldet der kommunale Dienstleister die Rückkehr zur Normalität. Allerdings bitte er offensichtlich die Kommunen zur Kasse, um die finanziellen Folgen der Attacke zu bewältigen.

Marco Pinske „Elf Monate nach dem Angriff können wir nun in den Normalmodus übergehen, um auch die letzten verbliebenen Themen abzuschließen.“

Prävention

Reaktion

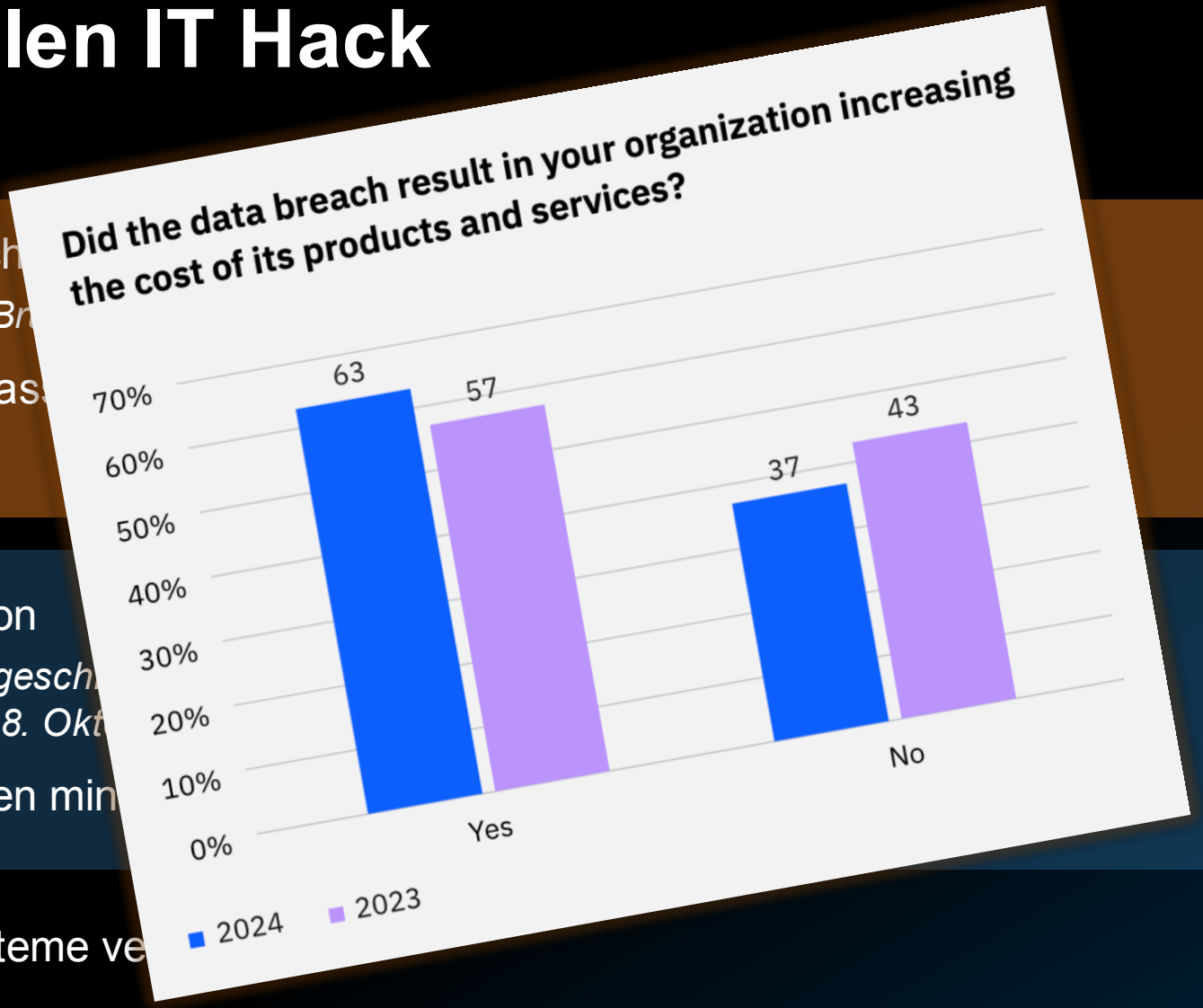
https://www.come-on.de/lennetal/werdohl/zurueck-im-normalmodus-suedwestfalen-it-bittet-kommunen-zur-kasse-93346047.html

Südwestfalen IT Hack

- Cisco ASA nich
  (Geeignet für Br
- Schwaches Pas
- Kein MFA

- Keine Detektion
  (über 300 fehlgesch
  Systeme am 18. Okt
- Angreifer waren min

- Über 960 Systeme ve



https://www.come-on.de/lennetal/werdohl/zurueck-im-normalmodus-suedwestfalen-it-bittet-kommunen-zur-kasse-93346047.html

Preiserhöhungen nach einem Cybervorfall

Risiken & Statiskiken

Bei 63% der Unternehmen, führte ein Cyber-Vorfall (Breach) zu Preiserhöhungen, die an Kunden weitergegeben werden musste

Quelle: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52913

Wo stehen Sie?

Angestrebtes Sicherheitslevel

Lücke

BASIS

Passwörter / AD

Patch Management

Backups

PERIMETER

Firewalls

SPAM / Web Filters

WAF / Proxy

ERWEITERTE VERTEIDIGUNG

Endpoint (NGAV, EDR)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

WIEDERSTANDS-FÄHIGKEIT

Kontinuierliche Verbesserung

Regulatorische Anforderungen (NIS 2, ISO, etc)

Versicherbarkeit

Ruhig schlafen

ARCTIC WOLF

SECURITY OPERATIONS PARTNER