WARUM BRAUCHT ES EIN SECURITY OPERATIONS CENTER?

first frame networkers
IT, die Sie weiterbringt

HERZLICH WILLKOMMEN

first frame networkers
IT, die Sie weiterbringt

Vielen Dank, dass Sie sich die Zeit für uns nehmen!

Was Sie heute erwartet:

Ein spannendes Referat über die Wichtigkeit eines Security Operation Centers.

JÖRG KOCH
Leiter Marketing
first frame networkers ag

DER HEUTIGE REFERENT

first frame networkers
IT, die Sie weiterbringt

PHILIPPE HIRZEL
Projektleitung Security Services
first frame networkers ag

- Seit Mai 2023 zurück bei der first frame networkers ag, nachdem er bereits sechs Jahre hier gearbeitet hatte.
- Seine neue Aufgabe ist es, die Managed Security Services auf- und auszubauen.
- Aktuell studiert er am SANS Technology Institute für den Master of Science in Information Security Engineering.
- Neben der Arbeit kocht Philippe Hirzel gerne und ist Jugend- und Sport-Leiter (Ski).

AGENDA

first frame networkers
IT, die Sie weiterbringt

- 11:00 Begrüssung, Jörg Koch
- 11:05 Warum braucht es ein SOC?, Philippe Hirzel
- 11:35 Fragen & Antworten

Kein technischer Deep Dive!

Fragen können mit der Chatfunktion gestellt werden.

Das Webinar wird in Schweizerdeutsch gehalten.

WAS IST EIN SECURITY OPERATIONS CENTER?

first frame networkers
IT, die Sie weiterbringt

Security Operations Center

WAS IST EIN SECURITY OPERATIONS CENTER?

first frame networkers
IT, die Sie weiterbringt

WAS IST EIN SECURITY OPERATIONS CENTER?

first frame networkers
IT, die Sie weiterbringt

Security Operations Center

WAS IST EIN SECURITY OPERATIONS CENTER?

first frame networkers
IT, die Sie weiterbringt

SOC-BESTANDTEILE

first frame networkers
IT, die Sie weiterbringt

Personen

– Zertifizierte Spezialisten

Prozesse

– ISO-Zertifizierungen

Technologien

– Marktführende Hersteller

Personen, die anhand definierter Prozesse modernste Technologien überwachen.

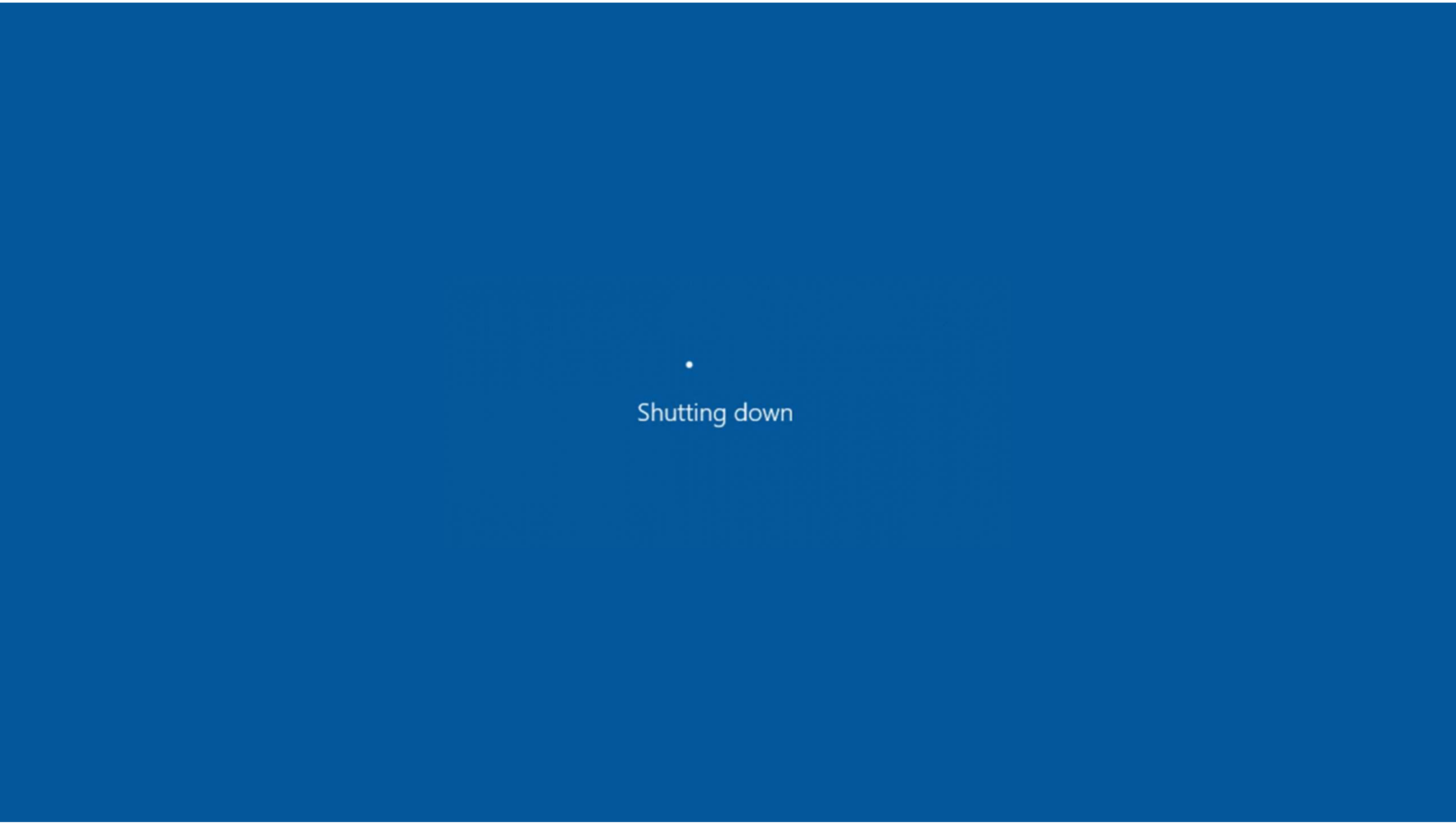
SOC-AUFGABEN

first frame networkers
IT, die Sie weiterbringt

- Systeme überwachen
- Auffälliges Verhalten erkennen
- Reagieren bei Vorfällen
- Verfügbarkeit der Systeme sicherstellen
- Blockieren ist nicht immer möglich
- Es braucht menschliche Interaktion

Eine Alarmanlage geht los – und niemand hört hin


Dear Customer:
It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your c
If you don't use the printed INVOICE, then be sure to refer to the imp
reference numbers below in all correspondence. In return you will rece
- a renewal software package with easy-to-follow, complete instruction
- an automatic, self-installing diskette that anyone can apply in minu
Important reference numbers: A5599796-2695577-
The price of 365 user applications is US$189. The price of a lease for
lifetime of your hard disk is US$378. You must enclose a bankers draf
cashier's check or international money order payable to PC CYBORG CORP
for the full amount of $189 or $378 with your order. Include your name
company, address, city, state, country, zip or postal code. Mail your
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.
Press ENTER to continue
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
ALL YOUR IMPORTANT
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.
Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information
data of any company.
You can provide us accounting data for the access to any company, for example, login a
Open our letter at your email. Launch the provided virus on any computer in your company
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
ve problems with gates, use direct connection:
load TOR Browser from http://torproject.org
Tor Browser open the http://bs7aygotd2rnjl4o.onion
t this server is available via Tor Browser only. Retry in 1 hour if site is not
llowing public key in the input form on server:
BF36-WBJBC-8TYKH-NAMB8-N5GCF-W27NM-NFHGV-XWPUH-JWHT6-FE2YI-XHFQF
50WX-AVB26-C7RW5-GGA5Q-P3GEE-R3JWH-RE530-PBD4F-G21FY-ONKVU-KYP7U
KHQ2G-A5XV8-RG8EQ-C2WQS-JZBUI-ZDN6S-M4P30-AYTXV-TSF1A-XE8YH-534EA-EX3KK-C7K8B-MCNRJ
4JRIW-KYZWI-AYD4D-1BCA2-XZHPS-2Y5QJ-31D1B-P4KC0-6MWAG-6Z8IM-7Q2T0-ZD4YN-C0RI0-3N77U
AN0ED-E2QXG-8SSUC-5G5DV-TJ8NV-WMJ2H-BJ8JN-3EE5Z-U2378-M3E6U-CMNWK-KED2Z-BZJ30-EA46S
2SGAK-MRIFQ-UKGSX-5RJYD-YFYW7-5E4PH-KD0RJ-X6MDH-XCP35-2UXNK-V7YA5-XVMXZ
Copy Public Key to Clipboard


Shutting down

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

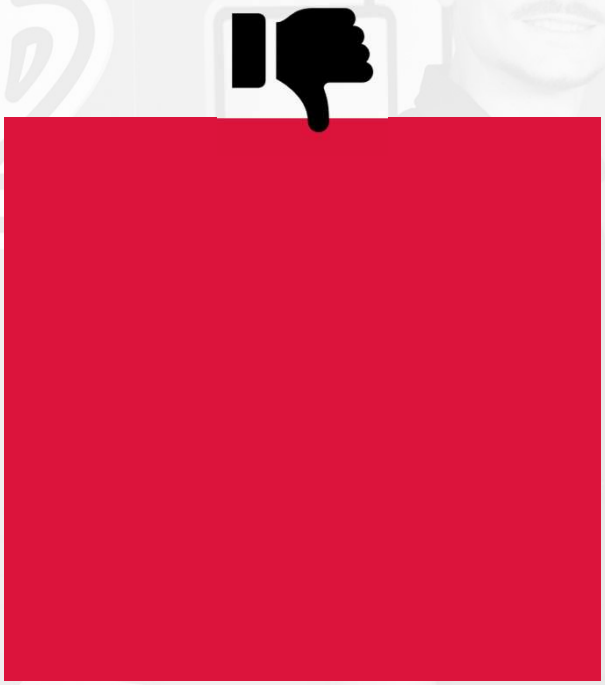
Important reference numbers: A5599796-2695577-

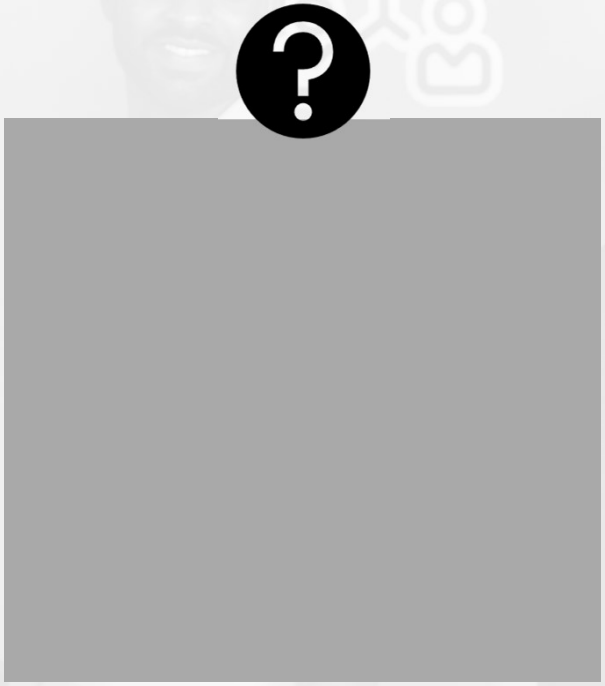
The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

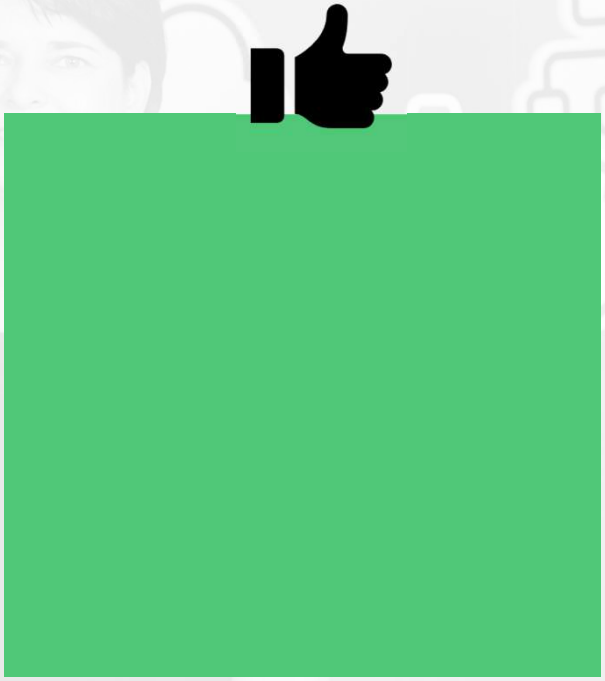
Press ENTER to continue

WIE VERÄNDERN SICH ANGRIFFE?

first frame networkers
IT, die Sie weiterbringt

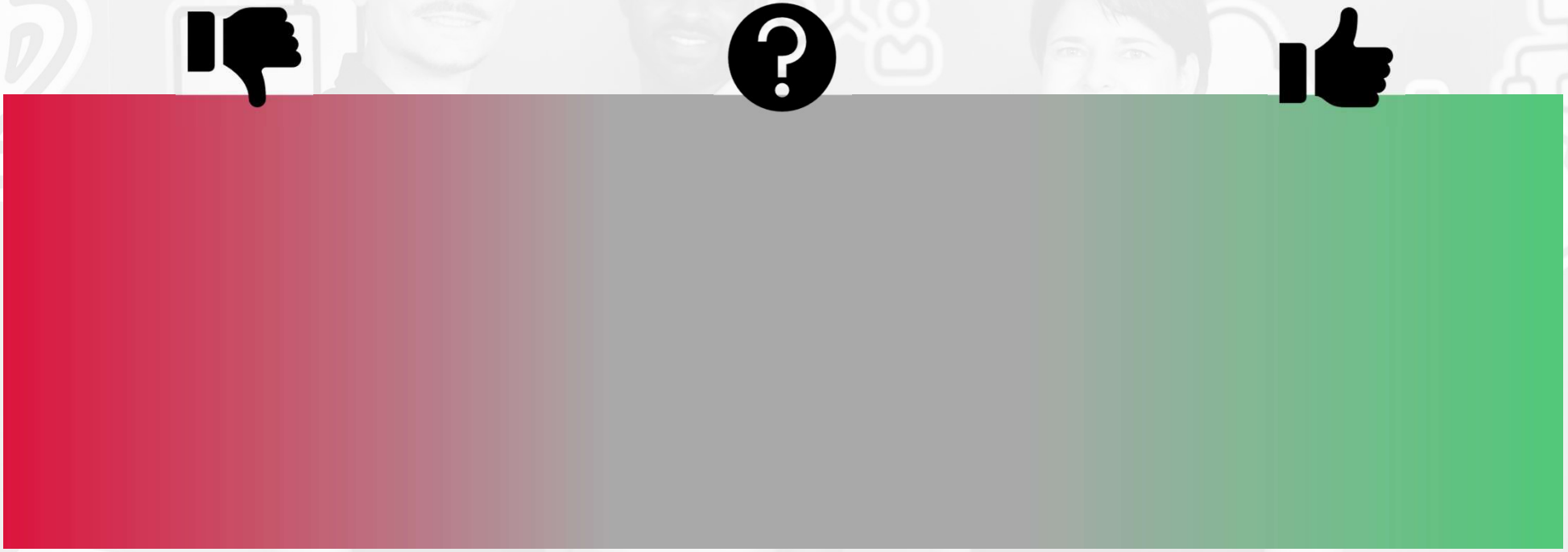






WIE VERÄNDERN SICH ANGRIFFE?

first frame networkers
IT, die Sie weiterbringt



WIE VERÄNDERN SICH ANGRIFFE?

first frame networkers
IT, die Sie weiterbringt

WIE WEHREN WIR DAS AB?

first frame networkers
IT, die Sie weiterbringt

Anti-Virus oder EDR

SPAM-Filter und Sandbox

Multi Faktor Authentifizierung

WIE WEHREN WIR DAS AB?

first frame networkers
IT, die Sie weiterbringt

Anti-Virus oder EDR

SPAM-Filter und Sandbox

Multi Faktor Authentifizierung

WIE WEHREN WIR DAS AB?

first frame networkers
IT, die Sie weiterbringt

Anti-Virus oder EDR

SPAM-Filter und Sandbox

Multi Faktor Authentifizierung

WAS MACHT DIE FIRST FRAME NETWORKERS AG?

first frame networkers
IT, die Sie weiterbringt

Personen

- Zertifizierte Spezialisten
- Kontinuierliche Weiterbildungen
- SOC-Betriebsteam

Prozesse

- ISO-Zertifizierungen
- Messen und verbessern anhand etablierter Standards (SOC-CMM)

Technologien

- XDR als Grundlage

WAS MACHT DIE FIRST FRAME NETWORKERS AG?

first frame networkers
IT, die Sie weiterbringt

Personen

- Zertifizierte Spezialisten
- Kontinuierliche Weiterbildungen
- SOC-Betriebsteam

Prozesse

- ISO-Zertifizierungen
- Messen und verbessern anhand etablierter Standards (SOC-CMM)

Technologien

- XDR als Grundlage

Zusammenarbeit zwischen Teams und Technologien verbessern!

WAS MACHT XDR?

first frame networkers
IT, die Sie weiterbringt

Anti-Virus oder EDR

SPAM-Filter und Sandbox

Multi Faktor Authentifizierung

MICROSOFT DEFENDER XDR

first frame networkers
IT, die Sie weiterbringt

INTEGRATION MIT SIEM

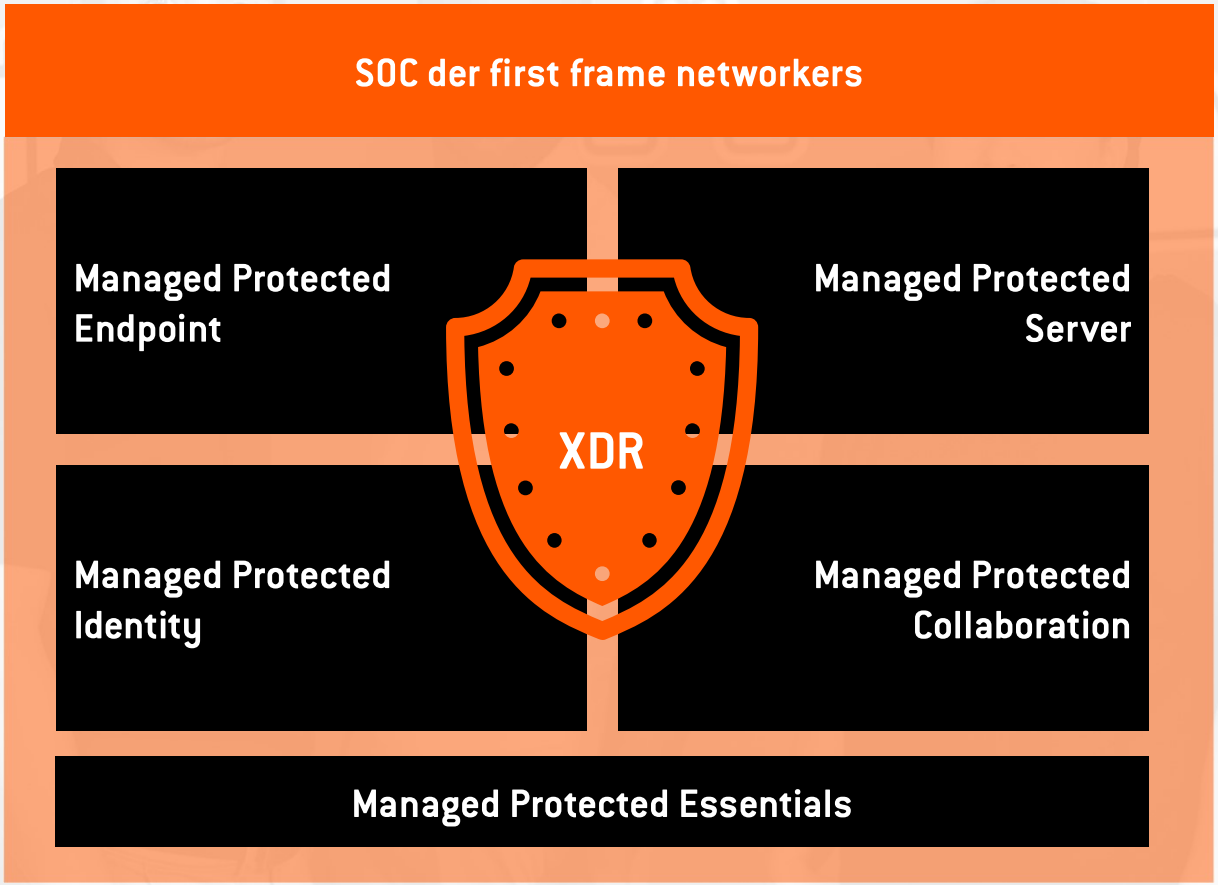
first frame networkers
IT, die Sie weiterbringt

INTEGRATION MIT SIEM

first frame networkers
IT, die Sie weiterbringt

WIE SIEHT DAS FÜR MICH ALS KUNDEN AUS?

first frame networkers
IT, die Sie weiterbringt



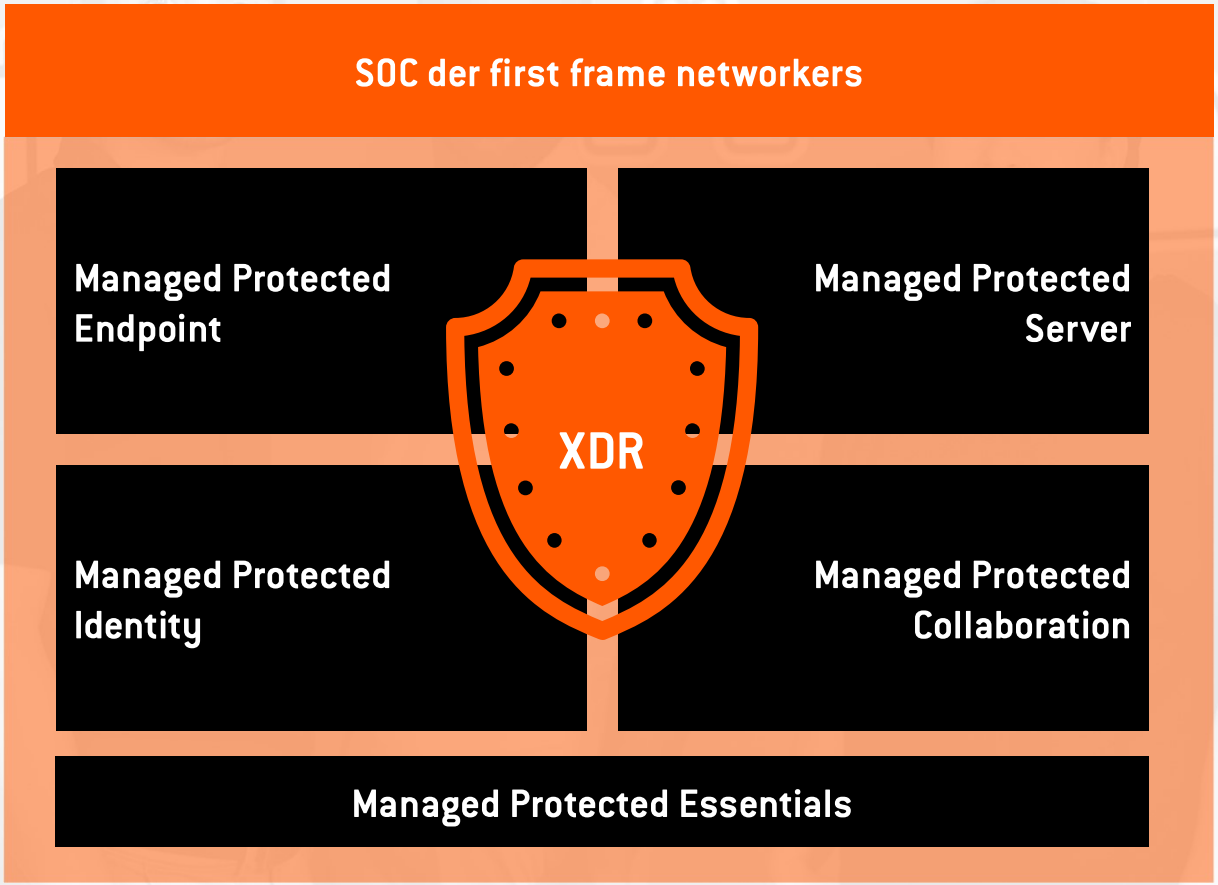
MANAGED PROTECTED ENDPOINT

first frame networkers
IT, die Sie weiterbringt

- Basiert auf Microsoft Defender for Endpoint P2
- Optionaler 24/7 Betrieb durch Sophos MDR
- Zusätzliche Leistungen von first frame
  - Reagieren auf Incidents
  - Definierte Prozesse für die Handhabung von Incidents
  - Hinweise zu Einstellungsoptionen, um weitere solcher Incidents zu verhindern (Umsetzung nicht im Service enthalten)
  - Kontinuierliche Verringerung der Angriffsfläche durch anpassen der "Attack Surface Reduction" Einstellungen

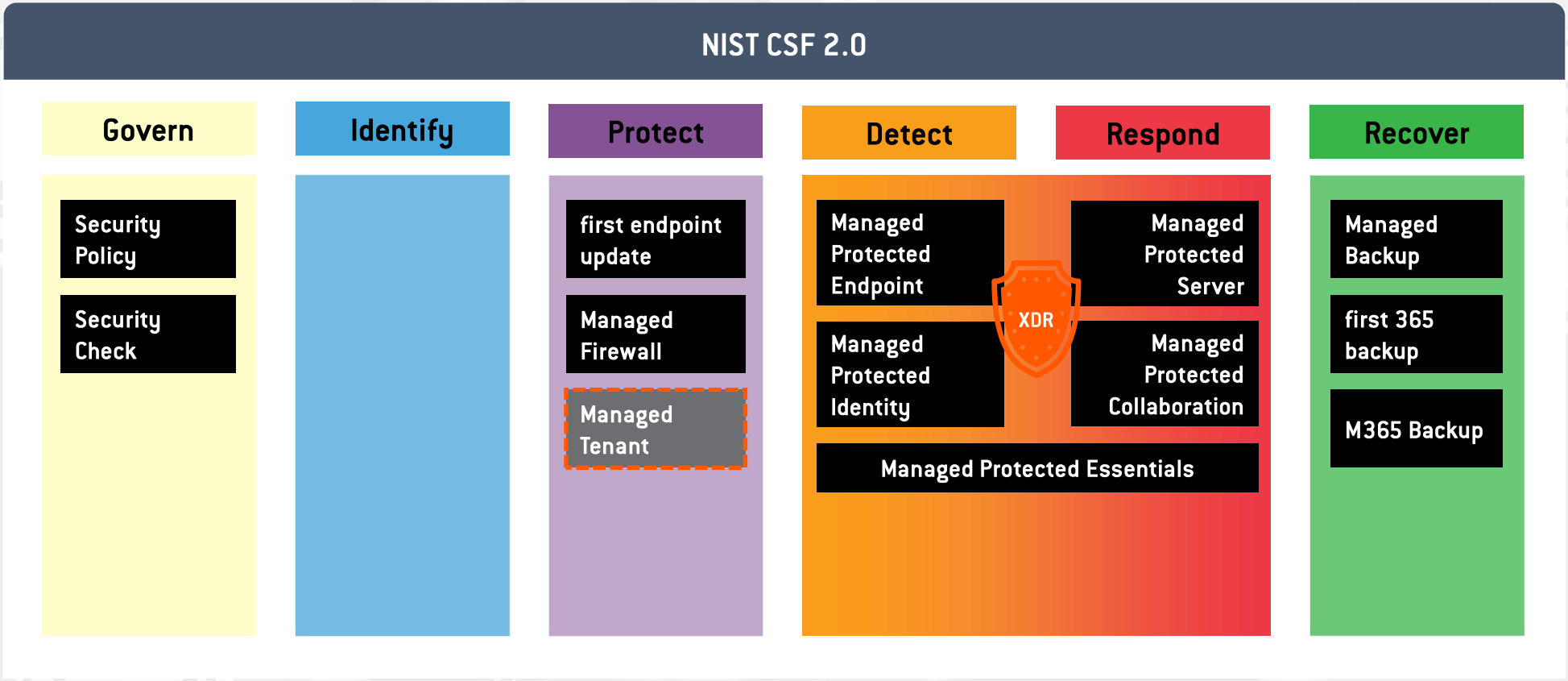
WIE SIEHT DAS FÜR MICH ALS KUNDEN AUS?

first frame networkers
IT, die Sie weiterbringt



GESAMTES SECURITY PORTFOLIO

first frame networkers
IT, die Sie weiterbringt



WO FANGE ICH AN?

first frame networkers
IT, die Sie weiterbringt

- Security ist ein Prozess und kein Produkt
- «Security-Journey» über die nächsten Jahre
- Managed Services für alle Kundengrössen

SECURITY JOURNEY, KAPITEL 1

first frame networkers
IT, die Sie weiterbringt

MANAGED TENANT

first frame networkers
IT, die Sie weiterbringt

- Absichern vom Microsoft/Office 365 Tenant
- Security Best Practices anwenden
- Security Best Practices überwachen
- Security Best Practices verfeinern
- Administrative Logins überwachen
- Management für Microsoft & Office 365 Lizenzen

Absichern Ihres „Zuhauses“ in der Cloud.

FIRST ENDPOINT UPDATE

first frame networkers
IT, die Sie weiterbringt

- Regelmässige Aktualisierung von Windows und Applikationen
- Regelmässige Prüfung von Firmware und BIOS/UEFI inkl. Update
- Zentrale Anlaufstelle und schnelle Hilfe bei Problemen im Zusammenhang mit der Aktualisierung
- Monatliche Berichte

Datenschutzverordnung (DSV) - seit September 2023 in Kraft:

…Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit)…

Schnelle Installation von Updates ist entscheidend.

MANAGED PROTECTED ESSENTIALS

first frame networkers
IT, die Sie weiterbringt

Schutz der Computer

- AV
- Webfilter für unterwegs
- EDR bei einem Vorfall
- AI-Basierte Angriffsunterbrechung

Schutz der E-Mails

- SPAM-Filter
- Safe Link
- Safe Attachments für Outlook, Teams, Sharepoint & OneDrive

Schutz der Logins

- Conditional Access
- Self-service password reset (SSPR)
- Defender for Identity Add-On möglich

SECURITY JOURNEY, KAPITEL 1

first frame networkers
IT, die Sie weiterbringt

MANAGED PROTECTED ESSENTIALS

FIRST ENDPOINT UPDATE

MANAGED TENANT

NEXT STEPS

first frame networkers
IT, die Sie weiterbringt

Let's Talk!

- Mit Ihrem Account Manager
- Mit Philipp Hirzel: philippe.hirzel@firstframe.net oder +41 41 768 08 60

Weitere Infos

- https://lp.firstframe.net/securtity-services
- https://lp.firstframe.net/endpoint-sicherheit

first frame networkers

IT, die Sie weiterbringt

first frame networkers

IT, die Sie weiterbringt

firstframe.net

Herzlichen Dank

first frame networkers
IT, die Sie weiterbringt