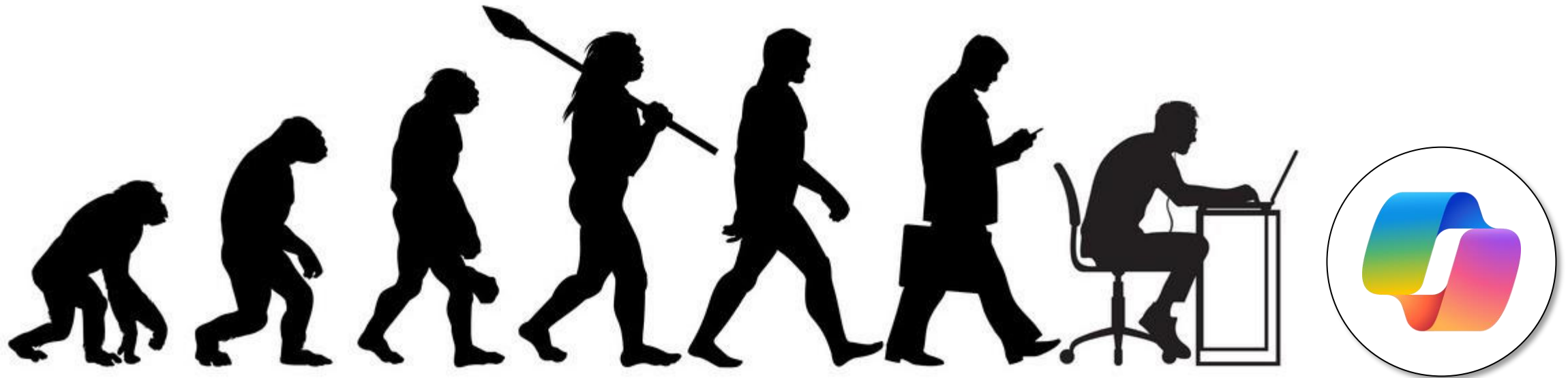


Von der Firewall zum Copiloten – Willkommen im Zeitalter der KI

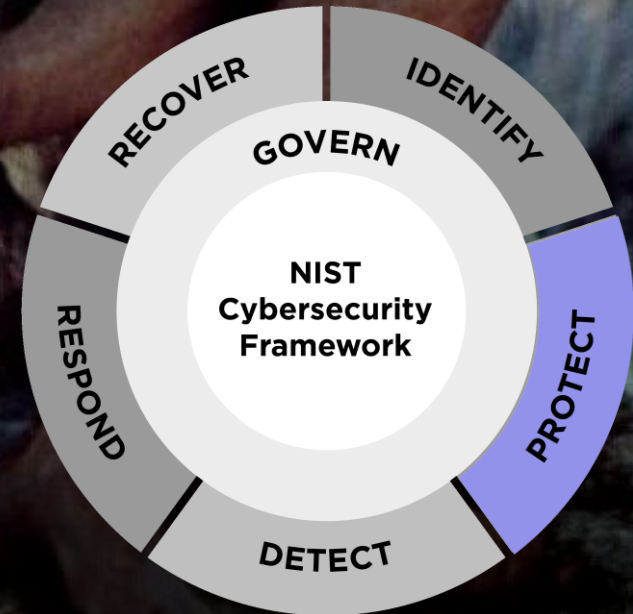


eine kleine Reise durch die Epochen der Cyber Security Geschichte

Firewalls
Antivirus

Am Anfang war das Feuer.

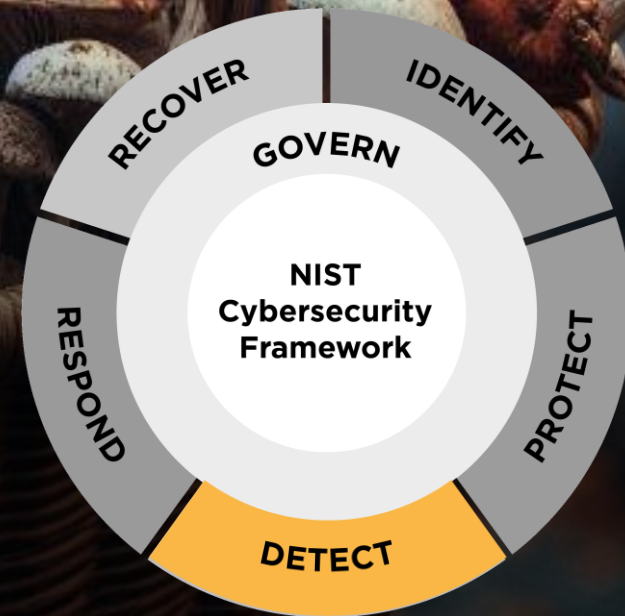
1990er



SIEM
SOAR

Dann kamen die Sammler

2000er



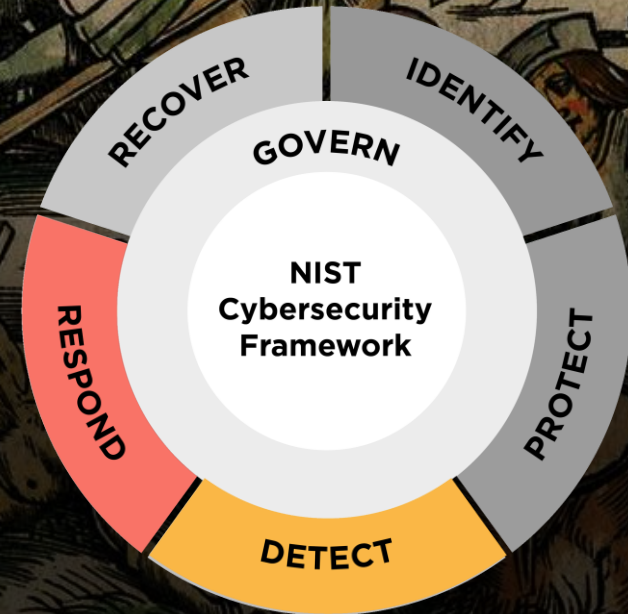


und sammelten bis ins dunkle Mittelalter

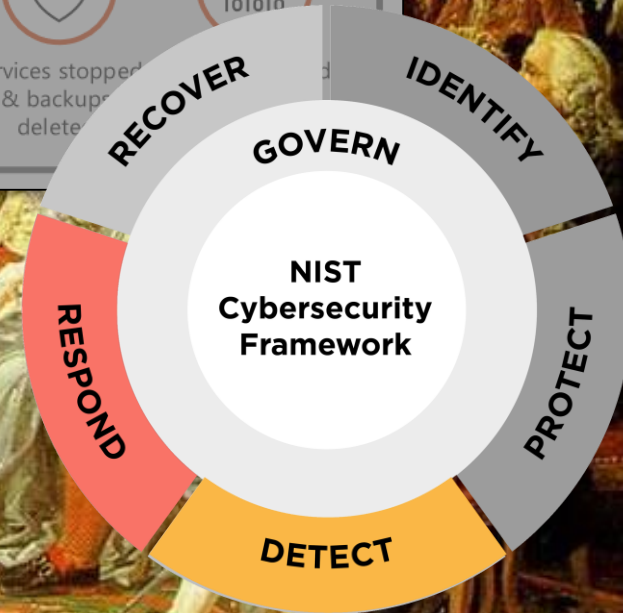
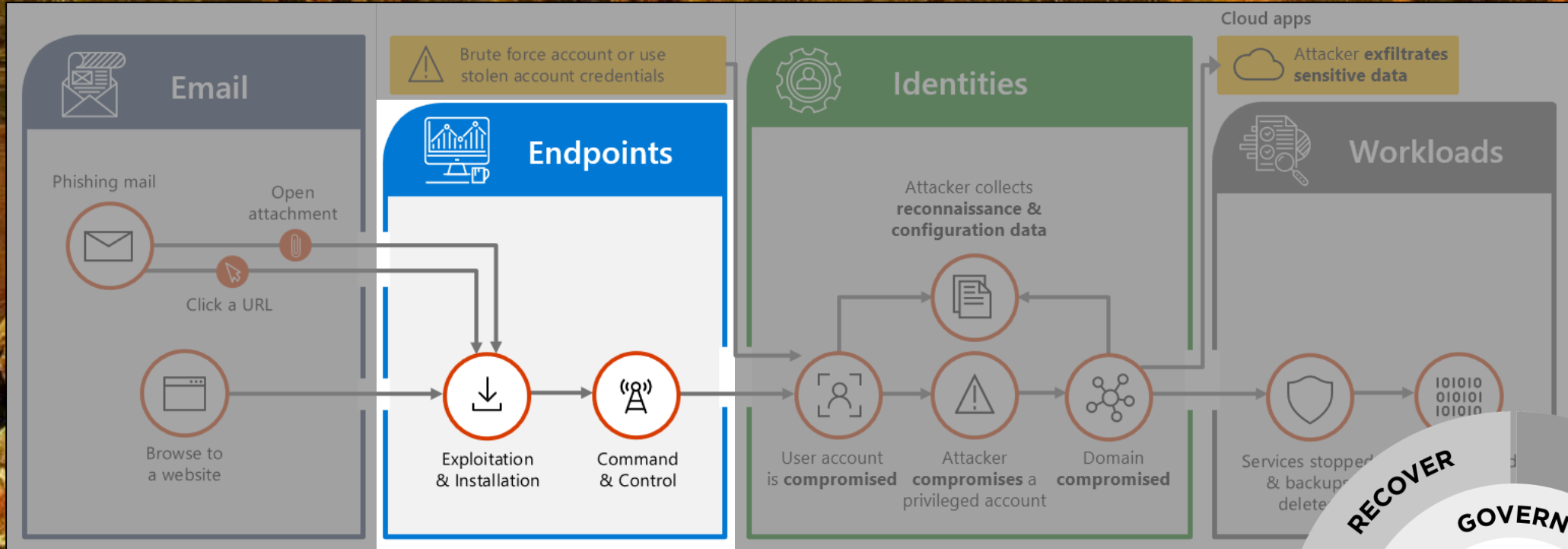


bis EDR etwas Licht
in die Dunkelheit brachte

2010er



Aufklärung: XDR erweitert den Horizont 2020er



DUDEN

Gegenwart, die

Wortart: Substantiv, feminin

für Microsoft 365

für Dynamics

für GitHub



für Power Plattform

für XYZ

für Security
(GA seit 01.04.2024)

Ladies & Gentlemen,
Hier spricht ihr Copilot.
Willkommen im **Zeitalter der KI.**

Der Copilot **unterstützt** die Spezialisten.

Er ersetzt weder den Piloten, noch die Flugbegleiter, noch das Bodenpersonal und auch nicht die Zollabfertigung.

Copilot for Security gibt es entweder im "Standalone Modus"

Microsoft Security Copilot Preview

Continue your last session

Tell me about Defender incident 20259.

The customer inquired about the Defender incident 20259 with Medium severity. The incident involved a medium-severity alert for an unfamiliar sign-in attempt from IP address '136.49.226.136' in the United States. The incident was detected on 2023-11-02 18:36:24 UTC and involved an user named 'lvandenende'. The incident was at the Initial Access stage of the kill chain. The user was affected by the attempted sign-in and the incident is still ongoing. The incident was reported to the customer by the agent. The customer was asked to provide a summary of the incident. The agent provided a summary of the security incident.

Updated less than a minute ago

Explore with Copilot

- Featured prompts
- Promptbooks

Threat actor profile

Get a report profiling a known actor with suggestions for protecting against common tools and tactics.

Microsoft Security · 5

Vulnerability impact assessment

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security · 6

Ask anything about security, or type / for suggestions or * for promptbooks

Microsoft Sentinel incident investigation

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

Sentinel Incident ID

Prompts (7)

- Summarize Sentinel incident <SENTINEL_INCIDENT_ID>
- Tell me about the entities associated with that incident.
- What are the reputation score for the IPv4 addresses on that incident?
- Show the authentication methods setup for each user involved in that incident. Especially indicate whether they have MFA enabled.
- If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies.
- If any devices are listed in the previous output, show details from Intune on the one that checked in most recently. Especially indicate if it is current on all operating system updates.
- Write an executive report summarizing this investigation. It should be suited for a non-technical audience.

Usecase: Incident Summary

Attack story Recommended actions (22) Alerts (12) Assets (7) Investigations (3) Evidence and Response (16) Summary Similar incidents

Alerts

0/12 Active alerts Unpin all Show all

- Oct 16, 2023 3:53 PM Resolved
Suspicious URL clicked
parkcity-win10d.parkcity.alpineskihouse.co leeg
- Oct 16, 2023 3:53 PM Resolved
**User accessed link in ZAP-
quarantined email**
Lee Gu
- Oct 16, 2023 3:56 PM Resolved
**A potentially malicious URL click
was detected**
Lee Gu Lee Gu
- Oct 16, 2023 3:59 PM Resolved
Anonymous IP address
Lee Gu
- Oct 16, 2023 4:07 PM Resolved
Activity from a Tor IP address
Lee Gu
- Oct 16, 2023 4:07 PM Resolved
**Suspicious behavior: Activity from
infrequent country or region**
Lee Gu Lee Gu
- Oct 16, 2023 4:14 PM Resolved
Activity from a Tor IP address
Lee Gu
- Oct 16, 2023 4:14 PM Resolved
Suspicious inbox manipulation rule
Lee Gu
- Oct 16, 2023 4:14 PM Resolved
BEC financial fraud

Incident graph Layout Group similar nodes

— Communication ... Association



Incident summary

Nov 9, 2023 9:45 PM

The security incident occurred between 2023-10-16 13:53:06 UTC and 2023-10-16 14:48:02 UTC, involving BEC Fraud and Credential Phishing with a high severity. The incident began with user 'leeg' clicking a suspicious URL on their Windows 10 device 'parkcity-win10d'. The URL was accessed from a quarantined email, and the user's email address is 'leeg@parkcity.alpineskihouse.co'.

An anonymous IP address (185.220.101.21) from Germany attempted to sign in, followed by suspicious activity from an infrequent country or region (IP 89.58.41.156). User 'leeg' accessed a Tor IP address and created a suspicious inbox rule named ITCleanup, moving messages to a folder named RSS Feeds.

The user then sent a suspicious email to 'nestorw@parkcity.alpineskihouse.co' with the subject 'Re: October project update - project maximus oasis is on hold for now'. Finally, email messages containing the malicious URL were removed after delivery, impacting users 'pattif' and 'leeg'.

AI generated. Verify for accuracy.

Mit "Guided Response"

Attack story Recommended actions (22) Alerts (12) Assets (7) Investigations (3) Evidence and Response (16) Summary Similar incidents

Alerts

0/12 Active alerts

Unpin all

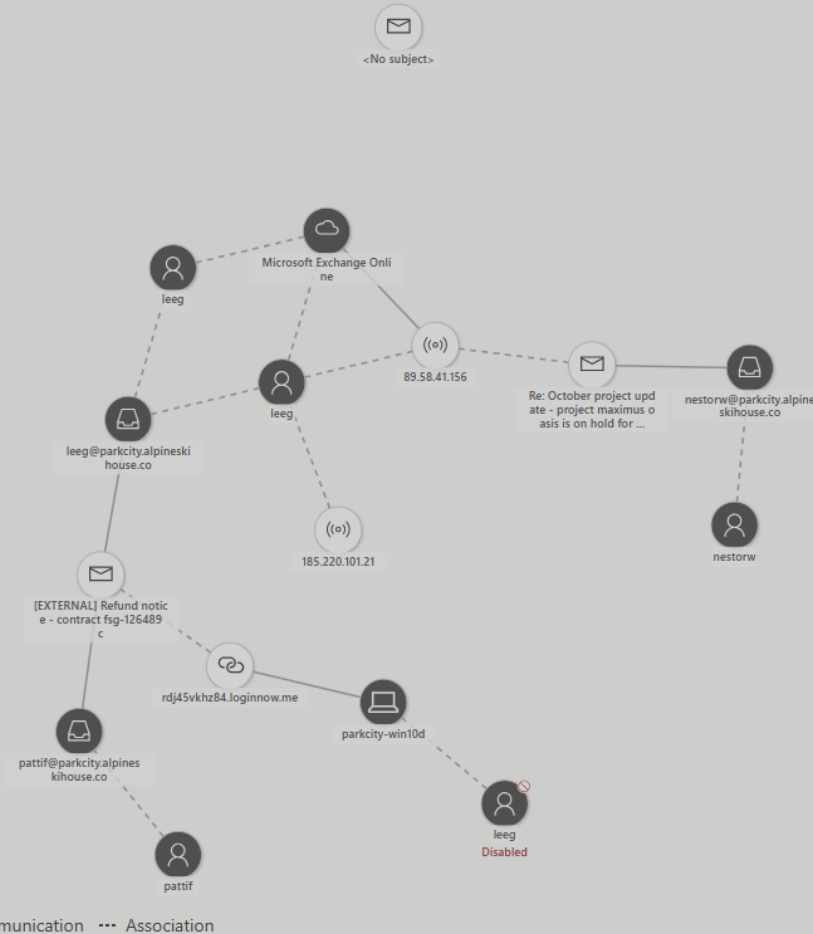
Show all

Incident graph

Layout

Group similar nodes

- Oct 16, 2023 3:53 PM Resolved
Suspicious URL clicked
parkcity-win10d.parkcity.alpineskihouse.co leeg
- Oct 16, 2023 3:53 PM Resolved
User accessed link in ZAP-quarantined email
Lee Gu
- Oct 16, 2023 3:56 PM Resolved
A potentially malicious URL click was detected
Lee Gu Lee Gu
- Oct 16, 2023 3:59 PM Resolved
Anonymous IP address
Lee Gu
- Oct 16, 2023 4:07 PM Resolved
Activity from a Tor IP address
Lee Gu
- Oct 16, 2023 4:07 PM Resolved
Suspicious behavior: Activity from infrequent country or region
Lee Gu Lee Gu
- Oct 16, 2023 4:14 PM Resolved
Activity from a Tor IP address
Lee Gu
- Oct 16, 2023 4:14 PM Resolved
Suspicious inbox manipulation rule
Lee Gu
- Oct 16, 2023 4:14 PM Resolved
BEC financial fraud



Recommended actions

Aug 01, 2023 2:41 AM

All (7)

Unfinished



Triage



Contain



Active

Isolate device cont-jonathan.pc

This action will isolate the device from the network. It will remain connected to the Microsoft Defender for Endpoint service.

Isolate device

View device details

Investigate



Remediate



Active

Resolve incident and generate report to ServiceNow



Resolve and generate report

- BEC Fra
- M
- REC
- Phis
- View
- reco
- O
- REC
- BEC
- View
- inve
- step
- O
- REL
- Thre
- 25 impacted assets

Other organizations tend to classify similar

Usecase: Incident Report erstellen

Incident report

Mar 31, 2024 4:10 PM

Incident title

Human-operated ransomware attack was launched from a compromised asset (attack disruption)

Incident details

Analysts	AlpineSkiHouse - AlpineSkiH... Analyst@domain.com
Time created	03/21/2024 19:05:32
First log	03/21/2024 20:11:33
Last log	03/31/2024 13:28:30
Time closed	03/31/2024 12:43:22

Incident summary

The high severity incident 'Human-operated ransomware attack was launched from a compromised asset' occurred between 2023-03-21 19:05:32 UTC and 2023-03-21 20:16:16 UTC. It was tagged as Attack Disruption and Ransomware, triggering an automatic Attack Disruption action.

- The incident began at 2023-03-21 19:05:32 UTC with potential human-operated malicious activity on the device 'Device1' (Windows10). The activity involved 7 files, including 'subtler.doc' and 'subtler.doc.lockbit', 2 IPs 11.111.11.111 and 111.222.33.444, and 9 processes, including 'powershell.exe' (running as SYSTEM), impacting users 'Account name 1' and 'Account name 2'.

Classification

True positive - Other

The incident was classified as "TruePositive" due to the detection of malicious activities such as ransomware-like behavior, suspicious remote activity, and lateral movement attempts. These activities were linked to a compromised user account and several devices within the organization. The involvement of an external actor was confirmed through the user associated with the compromised account.

Investigation actions

1. An investigation package was collected from the device identified as 'Device5'.
2. An antivirus scan was initiated on the device 'Device5'.
3. An investigation revealed that only the mentioned assets were affected and certain scripts had not been run in the organization in the last 30 days.

Remediation actions

1. The user account associated with Account name 2 was disabled by the automation system, Attack disruption.
2. The machine identified as WindowsServer1 was contained by the automation system, Attack disruption.
3. The user account linked to Account name 2 was contained by the automation system, Attack disruption.
4. The playbook "isolate-all-devices-immediately" was run as part of the response to the incident.
5. All devices were cleaned from potential malware.
6. Passwords for all users were reset.

Follow-up actions

1. A post-mortem review was scheduled with management to discuss the incident.
2. A reminder was set to export a PDF report for the meeting.
3. A security training session focusing on User Awareness

Incident summary

- Activity log
- Ask Defender Experts
- Generate incident report**
- Export incident as PDF

messages to a folder named RSS Feeds.

The user then sent a suspicious email to 'nestorw@parkcity.alpineskihouse.co' with the subject 'Re: October project update - project maximus oasis is on hold for now'. Finally, email messages containing the malicious URL were removed after delivery, impacting users 'pattif' and 'leeg'.

AI generated. Verify for accuracy.

Guided response

Apr 24, 2024 10:21 AM

Triage

Confirm this is a 'true positive'

Other organizations tend to classify similar incidents as a 'true positive'

Nochmals: der Copilot **unterstützt** die Spezialisten.

Typische Usecases sind:



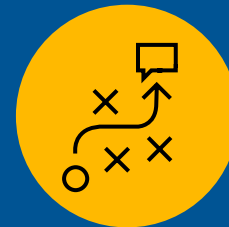
Incident summarization



Impact analysis



Reverse engineering of scripts



Guided response

- Suche Tags Agenda Mobile Digitale Schweiz IT-Security Bildung & Karriere Künstliche Intelligenz
- Cloud Social Media Infrastrukturen Telekommunikation Wirtschaft

Kinderspital beider Basel ersetzt bestehende Sicherheitsplattformen durch Microsoft Copilot für Security

Verfasst von **ictk** am Di, 23. April 2024 - 15:06



Das Universitäts-Kinderspital beider Basel (UKBB) ersetzt seine bestehenden Sicherheitsplattformen durch die KI-gestützte Lösung "Copilot für Security" des Softwareriesen Microsoft. Die Implementierung der neuen Lösung erfolge im Rahmen eines Pilotprojekts, das die Patientenversorgung und -sicherheit auf ein neues Level heben und die Arbeit des ICT-Personals erleichtern soll, heisst es in einer Mitteilung dazu.

Am UKBB sollen aber noch weitere KI-gestützte Lösungen wie der Microsoft 365 Copilot evaluiert werden. Das UKBB will damit auch seine Rolle als digitaler Pionier im Spitalbereich weiter festigen, wird in der Aussendung betont. Sebastien Dez, Leiter ICT im UKBB: "Jährlich werden hier über 100.000 Menschen ambulant oder stationär behandelt und wir haben die Vision, das Kinderkrankenhaus im Interesse der Patienten und des Personals zu digitalisieren und aktiv Innovationen zu realisieren." So habe sich das UKBB zum Ziel gesetzt, die Digitalisierung und telemedizinischen Dienste systematisch auszubauen, um jederzeit und an jedem Ort eine ganzheitliche Versorgung zu gewährleisten.



<https://ictk.ch/inhalt/kinderspital-beider-basel-ersetzt-bestehende-sicherheitsplattformen-durch-microsoft-copilot>

Kinderspital nutzt fortschrittliche Digitalisierungslösungen, um die Patientenversorgung zu verbessern - Microsoft Switzerland News Center

- Suche
- Tags
- Agenda
- Mobile
- Digitale Schweiz
- IT-Security
- Bildung & Karriere
- Künstliche Intelligenz
- Cloud
- Social Media
- Infrastrukturen
- Telekommunikation
- Wirtschaft

Kinderspital beider Basel ~~ersetzt~~ bestehende Sicherheitsplattformen ~~durch~~ Microsoft Copilot für Security **ergänzt** **mit** **als erstes Spital in der Schweiz**

Verfasst von **ictk** am Di, 23. April 2024 - 15:06



Das Universitäts-Kinderspital beider Basel (UKBB) ersetzt seine bestehenden Sicherheitsplattformen durch die KI-gestützte Lösung "Copilot für Security" des Softwareriesen Microsoft. Die Implementierung der neuen Lösung erfolge im Rahmen eines Pilotprojekts, das die Patientenversorgung und -sicherheit auf ein neues Level heben und die Arbeit des ICT-Personals erleichtern soll, heisst es in einer Mitteilung dazu.

Am UKBB sollen aber noch weitere KI-gestützte Lösungen wie der Microsoft 365 Copilot evaluiert werden. Das UKBB will damit auch seine Rolle als digitaler Pionier im Spitalbereich weiter festigen, wird in der Aussendung betont. Sebastien Dez, Leiter ICT im UKBB: "Jährlich werden hier über 100.000 Menschen ambulant oder stationär behandelt und wir haben die Vision, das Kinderkrankenhaus im Interesse der Patienten und des Personals zu digitalisieren und aktiv Innovationen zu fördern." So habe sich das UKBB zum Ziel gesetzt, die Digitalisierung und telemedizinischen Dienste systematisch auszubauen, um jederzeit und an jedem Ort eine ganzheitliche Versorgung zu gewährleisten.



Und wie
geht es
weiter?



Die Angreifer werden die KI (noch besser) nutzen



- Gezielte Angriffe
 - KI um detaillierte Profile von Personen aus Social Media Daten zu erstellen -> gezieltes Phishing
 - Phishing Mails haben keine Rechtschreibfehler mehr...
 - KI-Suche nach Vulnerabilities bei Zielsystemen
- Angriffe durch Imitation
 - Deepfakes, Sprachnachrichten, Videos
- Automatisierte Angriffe
 - AI powered botnets für noch bessere DDoS Attacks

Und wir werden die KI Systeme weiter ausbauen



- Die KI muss weiterhin "sicher gemacht" werden
 - "AI for Security" vs "Security for AI"
- KI wird nicht nur empfehlen, sondern auch selber durchführen
 - KI wird mehr Skills bekommen
 - Weitere Umsysteme werden eingebunden
 - Automatic attack disruption (schon jetzt, wird weiter ausgebaut)
- Neben "post-breach" kommt auch "pre-breach"
 - Exposure Management (*in preview*)
 - Vulnerabilities
 - Cloud Security Posture
 - Exposure Mgmt
 - Attack Path Analysis



[Security Exposure Management \(youtube.com\)](#)

[Microsoft Security Exposure Management documentation](#)



Fragen?

Urs Achermann

Health Industry Enterprise Security Executive

urs.achermann@microsoft.com

