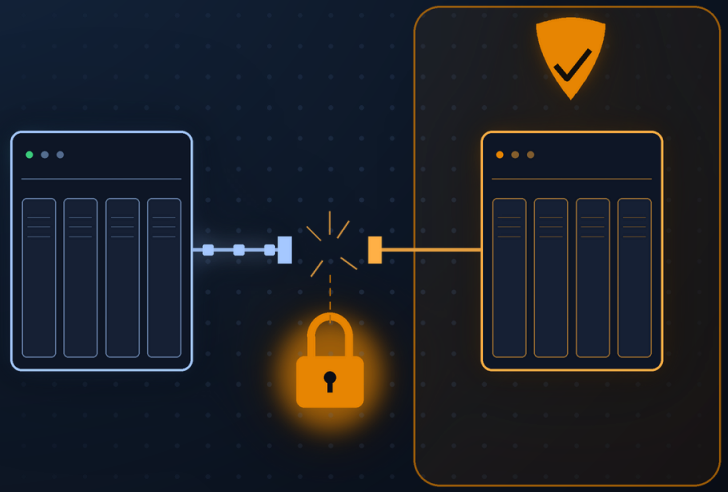
Nie wpuszczaj ransomware do backupu



Kacper Kaźmierczak
Junior Presales Engineer
+48 510 044 724
kacper.kazmierczak@fen.pl



Kopia off-line

AirGap+

Czego potrzebujemy do AirGap+?

QNAP Routers

QHora-321
QHora-322

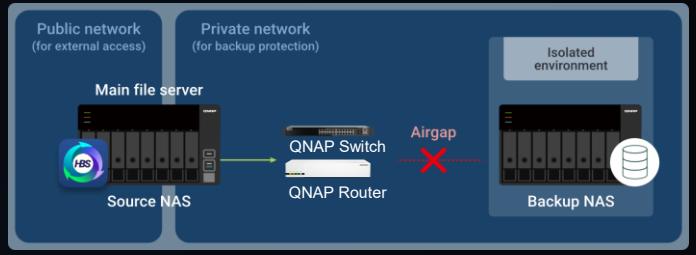
QNAP Airgap+

QNAP Switches

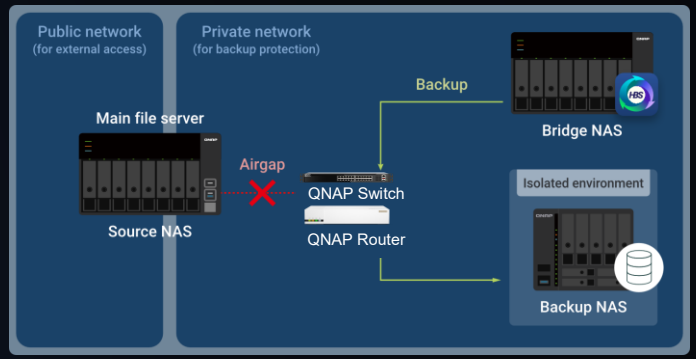
QSW-M7308R-4X
QSW-M3224-24T
QSW-M3212R-8S4T
QSW-M3216R-8S8T
QSW-IM3216R-8S8T

NEW

Standard Config



Advanced Config

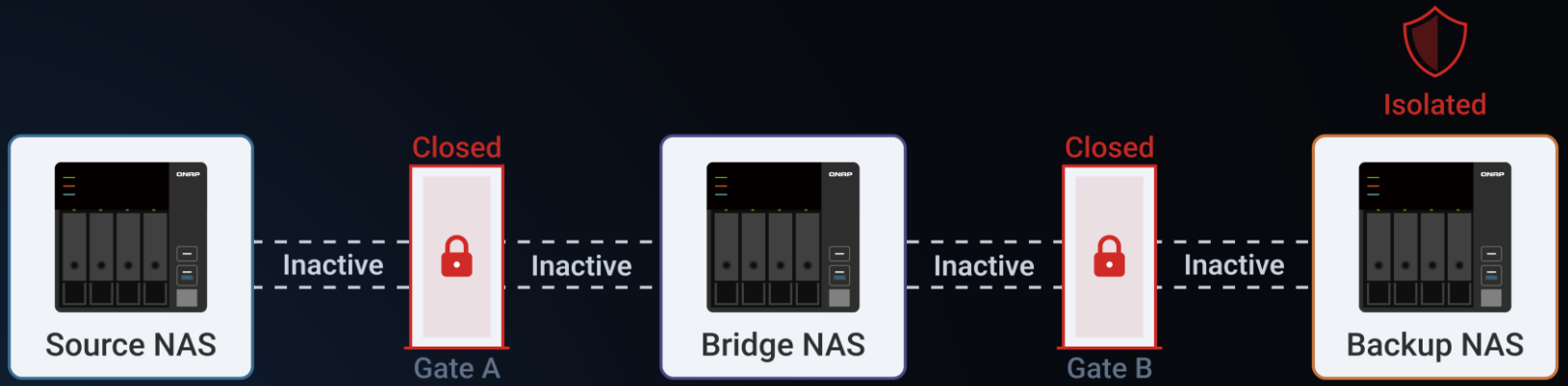


Zasada airlock:

5-stopniowa izolacja

1. Tryb gotowości
2. Otwieranie bramy zewnętrznej
3. Dane umieszczone na moście serwera NAS
4. Otwieranie bramy wewnętrznej
5. Powrót do izolacji

1. Tryb gotowości



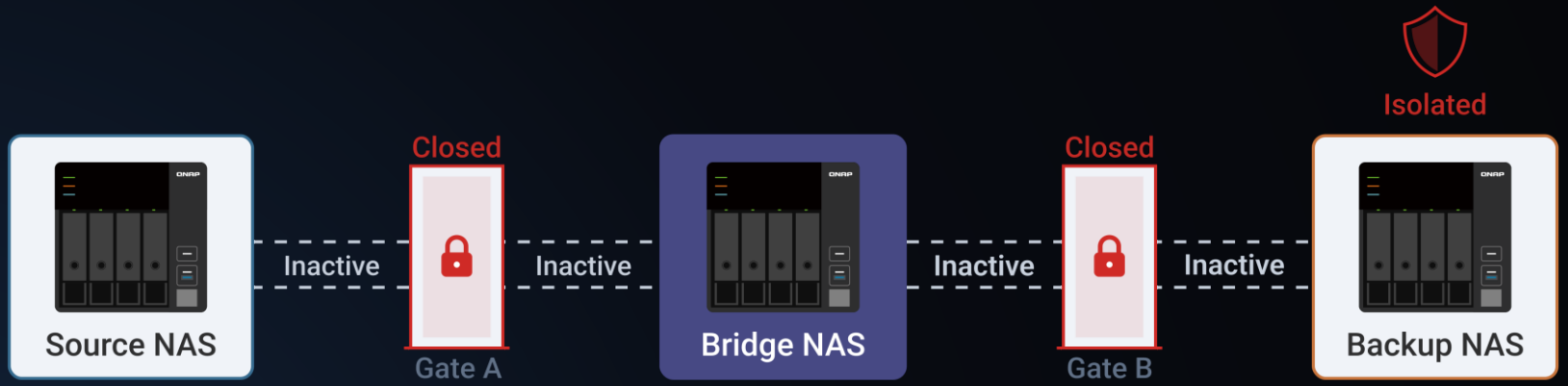
1 2 3 4 5

2. Otwieranie bramy zewnętrznej



1 — 2 — 3 — 4 — 5

3. Dane umieszczone na moście serwera NAS

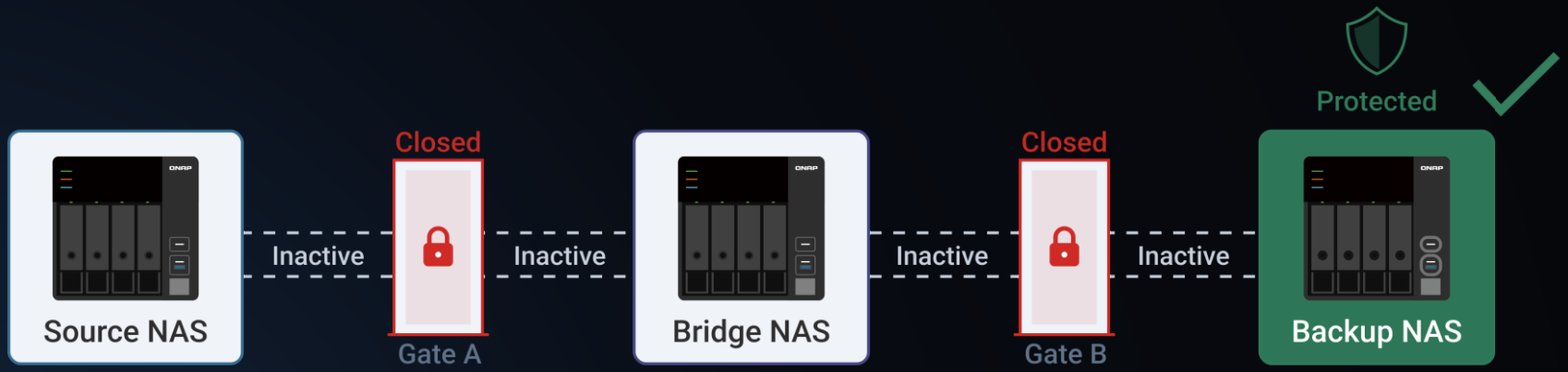


4. Otwieranie bramy wewnętrznej

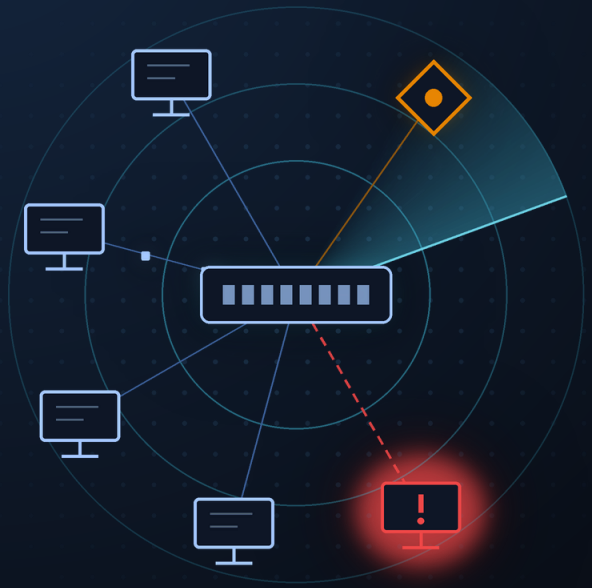


1 — 2 — 3 — 4 — 5

5. Powrót do izolacji



1 — 2 — 3 — 4 — 5



ADRA NDR

Strażnik sieci LAN

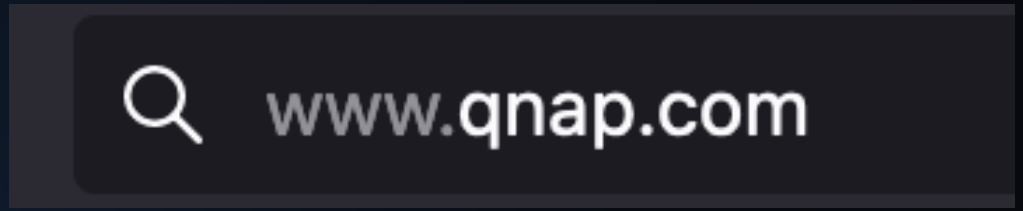
ADRA NDR – wykrywanie zagrożeń



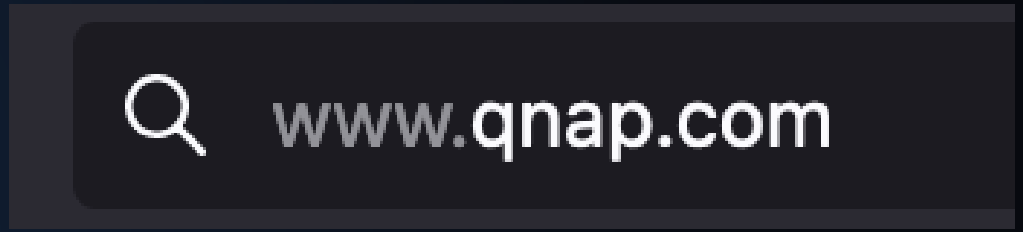
Po co mi NDR?

Przykład prostego ataku

Który adres jest poprawny?



czy



??????

Po co mi NDR?

Przykład prostego ataku

Który adres jest poprawny?

www.qnap.com

czy ??????

www.qnap.com

Po co mi NDR?

Przykład prostego ataku

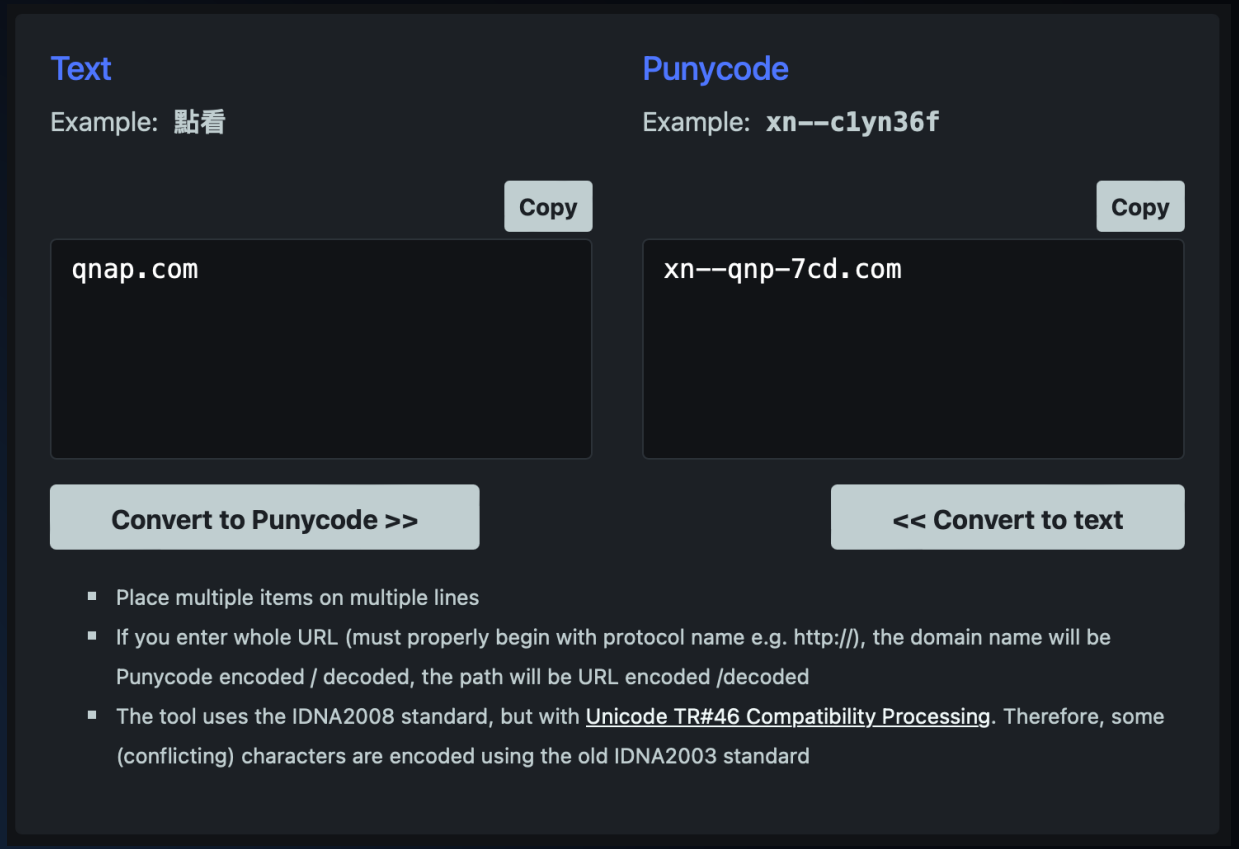
Wygląda podobnie…



Unicode Character “a” (U+0430)

Unicode Character “a” (U+0061)

Po co mi NDR?


Text
Example: 點看
Copy
qnap.com
Convert to Punycode >>
Punycode
Example: xn--c1yn36f
Copy
xn--qnp-7cd.com
<< Convert to text
Place multiple items on multiple lines
If you enter whole URL (must properly begin with protocol name e.g. http://), the domain name will be Punycode encoded / decoded, the path will be URL encoded /decoded
The tool uses the IDNA2008 standard, but with Unicode TR#46 Compatibility Processing. Therefore, some (conflicting) characters are encoded using the old IDNA2003 standard

Po co mi NDR?

Przykład prostego ataku

Atak phishingowy Punnycode

zamiana liter w domenie podobnymi znakami

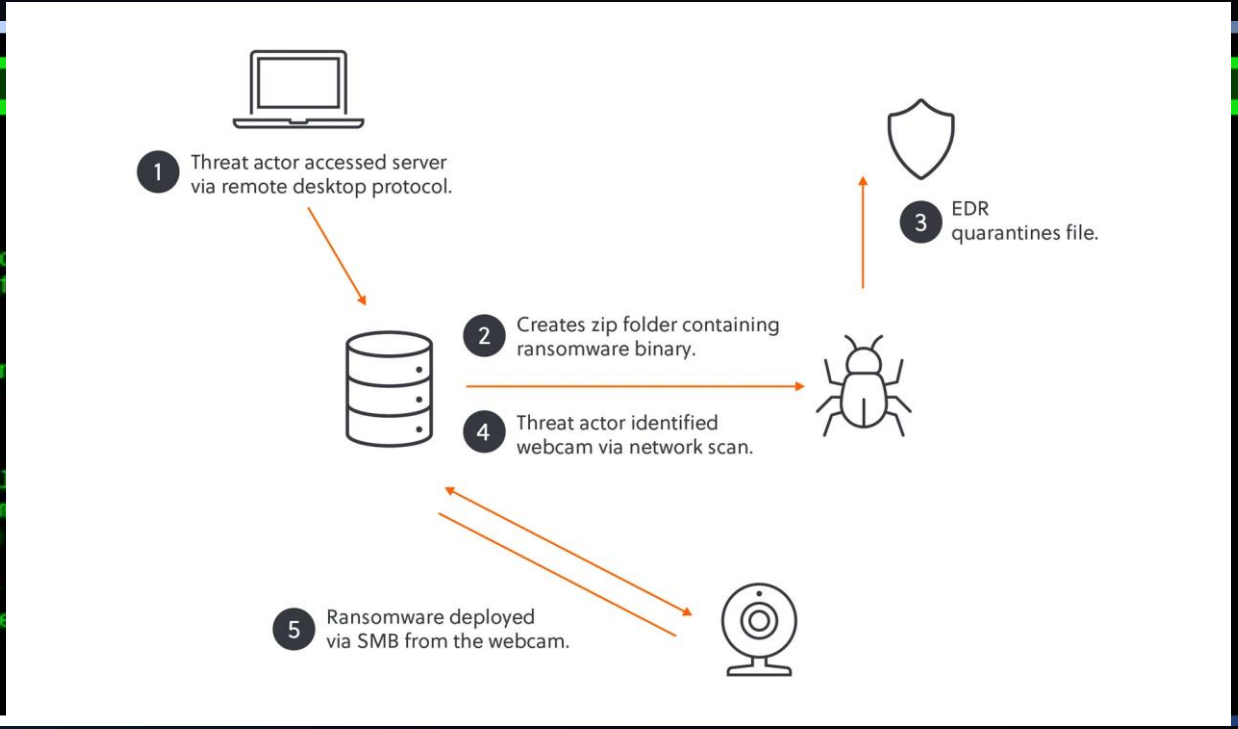
* Microsoft	->	microsoft.com	->	mìcrosoft[.]com
* Paypal	->	paypal.com	->	paypal[.]com
* Coinbase	->	coinbase.com	->	ćoinbase[.]name
* Blockchain	->	blockchain.com	->	blóckchäin[.]com
* Twitter	->	twitter.com	->	twittër[.]com
* Rolex	->	rolex.com	->	rołex.com.

Po co mi NDR?


HACKER TIMELINE
PLANNING
Target Selection
Research
Attack Vector
ENUMERATION
Who Am I?
Where Am I?
Where Can I Go?
Who Do I Need To Be?
COMPLETE OBJECTIVE
Steal IP
Data Exfil
Deploy Ransomware
Destroy Network
DAY 1
90+ DAYS
Spear-phishing
Insider Threat
0-day
Exploit
INTRUSION
To Steal Data
To Establish Persistence
To Hunt Users
To Distribute Toolset/Malware
LATERAL SPREAD

Od jednej kamery do całej sieci





ADRA NDR

Po co mi NDR?

2023/05/17 11:02:59	Pułapka: port usług	Średnie	212.112.120.218	-	10.26.82.101	A trap has detected a potential attack. Trap: internal trap, Instance: 1 (QNAP-NAS-1), IP: 10.26.82.101, TCP: 3389	
2023/05/17 10:57:21	Korelacja zagrożeń	Wysokie	37.46.113.220	-	-	One or more traps have detected the source IP performing a network scan.	
2023/05/17 10:57:21	Korelacja zagrożeń	Wysokie	195.181.170.237	-	-	One or more traps have detected the source IP performing a network scan.	
Operacja						01.101.200.222 placed	

Jakie zagrożenia może wykryć ADRA?

Kategoria	Zawartość
Skanowanie	• Skanowanie urządzeń/sieci • Skanowanie TCP/UDP/ICMP/ARP
Niestandardowe działanie	• Powódź sieciowa • Atak na flagę TCP • Nieznane żądania domeny • Wyłudzanie danych uwierzytelniających
Luki w zabezpieczeniach	• Ataki zero-day, luki CVE • Ataki zero-day na program Microsoft Active Protections • Ataki typu zero-day na „Patch Tuesday”
Podejrzane działanie Malware/Ransomware *	• C&C call back • Wykrycie pakietu exploit • Spoofing sieciowy • DDoS

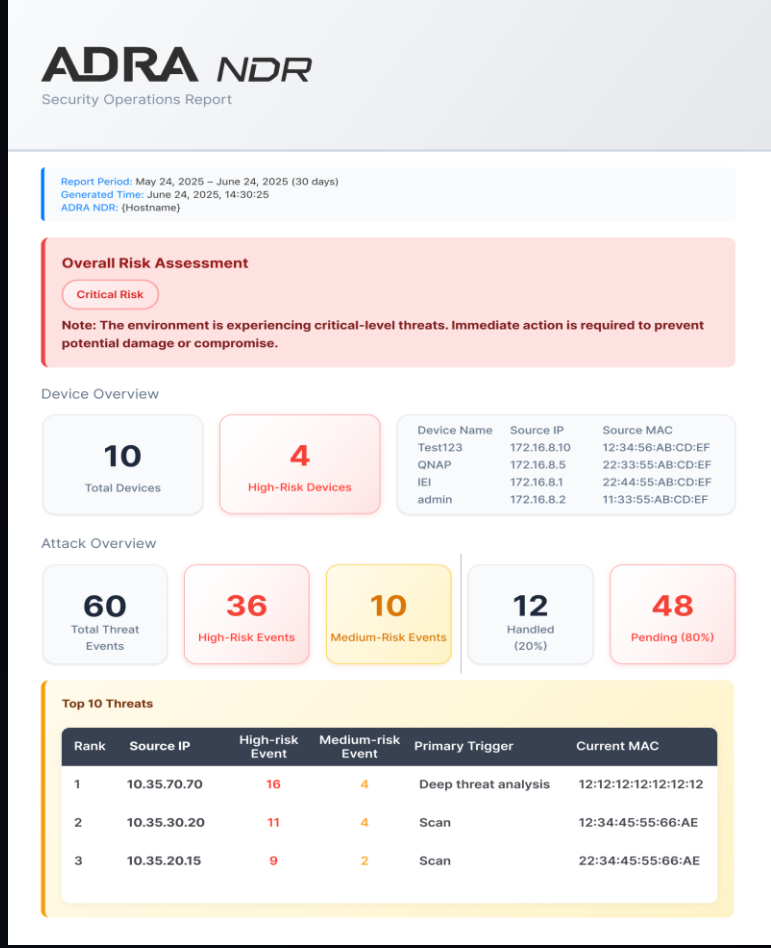
ADRA NDR

Automatyczne miesięczne raporty bezpieczeństwa

- Zaprojektowane, aby wspierać zgodność z wymogami audytu cyberbezpieczeństwa,
- ADRA automatycznie generuje raporty PDF na podstawie określonego przedziału czasowego,
- Pomaga nietechnicznemu zarządowi szybko zrozumieć ryzyka systemowe i skuteczność zastosowanych środków zaradczych

Co zawiera raport?

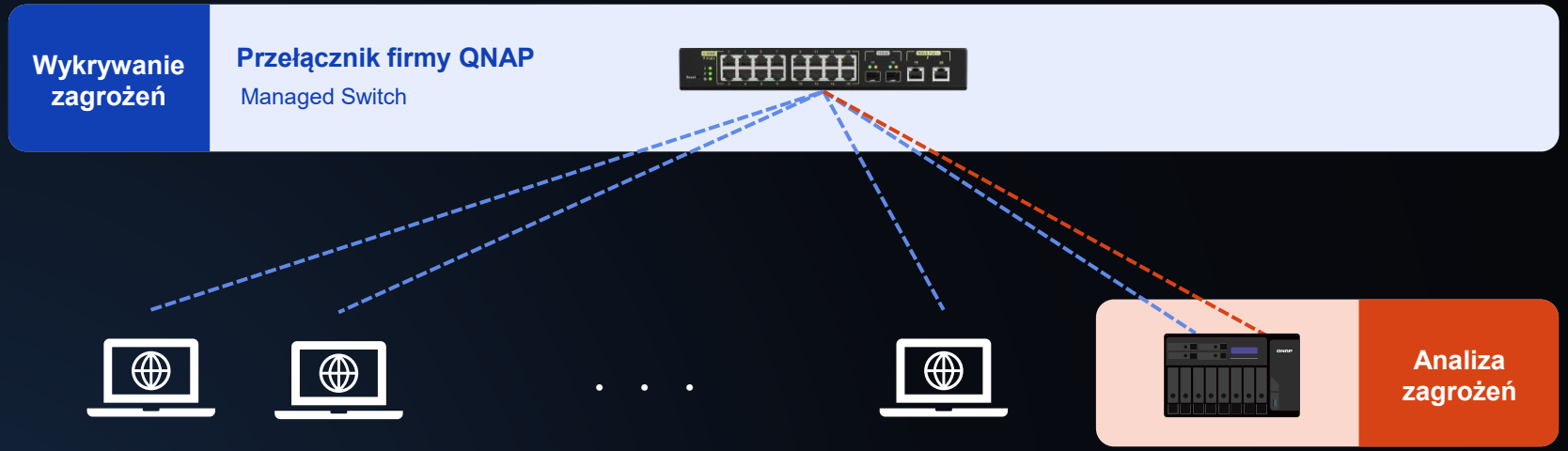
- Statystyki dotyczące wysokiego/średniego ryzyka
- Analiza i ranking źródeł ryzyka
- Postęp i stan udoskonaleń w obsłudze incydentów stanowiących zagrożenie



ADRA NDR

ADRA NDR na serwerze NAS

ADRA NDR Standalone



ADRA NDR

NDR Porównanie dostępnych rozwiązań

Tak, jest za darmo!!!

	Fortinet FortiNDR	Cisco Secure Network Analytics	QNAP ADRA NDR Standalone
Funkcjonalność	★★★★★	★★★★★	★★★
Użyteczność	★★★	★★★	★★★★★
Łatwość wdrożenia	★★★	★★★	★★★★★
Efektywność	★★★★★	★★★★★	★★★★★
TCO	$$$$$ (Subscription)	$$$$$ (Subscription)	$ (No Subscription Fee)

ADRA NDR to idealne, przyjazne dla budżetu rozwiązanie z zakresu cyberbezpieczeństwa dla małych i średnich firm.

Dziękuję za uwagę!

Nie wpuszczaj ransomware do backupu



Kacper Kaźmierczak
Junior Presales Engineer
+48 510 044 724
kacper.kazmierczak@fen.pl