

Offensive AI

Marcus “selle” Sellebjerg

WhoAmI

Marcus “Selle” Sellebjerg

Offensive Security Consultant

Security Researcher

Graduated from AU@2023

Just curious about technology

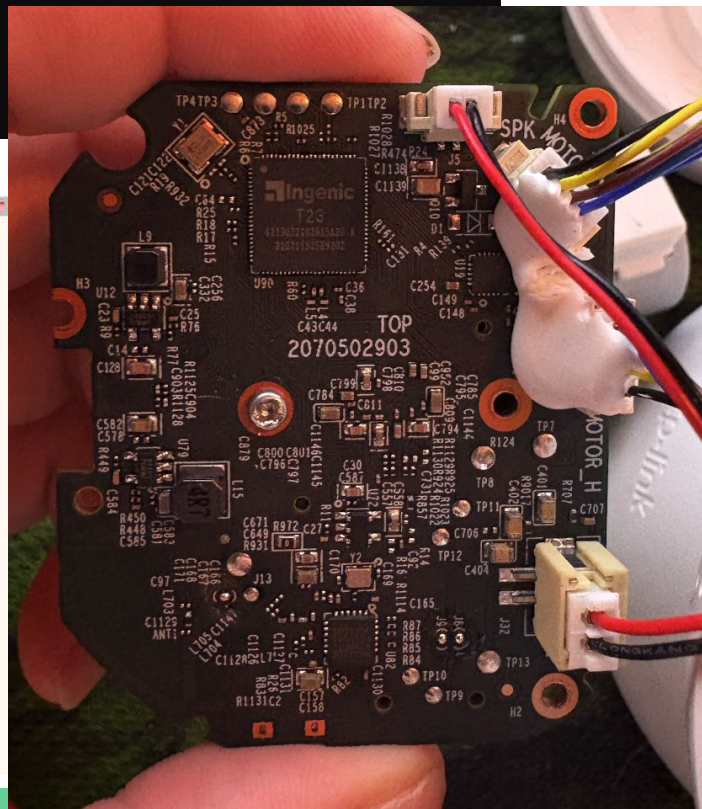
Mac enjoyer



My daily life

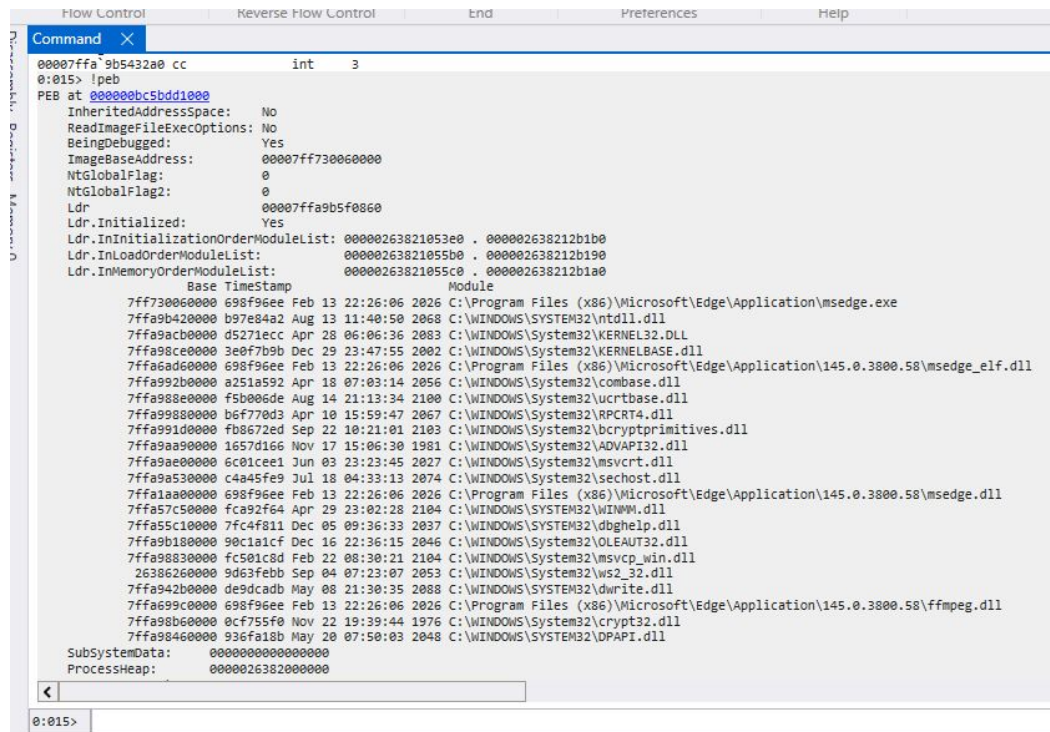
```
Windows PowerShell
PS C:\Users\selleri\Downloads> ./cat.exe output.txt
[i] You're all good, no virtualization here!
[i] Reading NTDLL from disk!
[i] Fetching ptr NTDLL from current process
[i] Replacing the .text section from current session with that from disk
[i] Success!
[+] FREEEEEEDOM!
[+] Trying to call the PE exec
```

00007FF8E1508260	4C:8BDC	mov r11,rsp	AmsiScanBuffer
00007FF8E1508263	49:895B 08	mov qword ptr ds:[r11+8],rbx	
00007FF8E1508267	49:896B 10	mov qword ptr ds:[r11+10],rbp	
00007FF8E150826B	49:8973 18	mov qword ptr ds:[r11+18],rsi	
00007FF8E150826F	57	push rdi	
00007FF8E1508270	41:56	push r14	
00007FF8E1508272	41:57	push r15	
00007FF8E1508274	48:83EC 70	sub rsp,70	
00007FF8E1508278	4D:8BF9	mov r15,r9	
00007FF8E150827B	41:88F8	mov edi,r8d	
00007FF8E150827E	48:88F2	mov rsi,rdx	
00007FF8E1508281	48:88D9	mov rbx,rcx	
00007FF8E1508284	48:88D0 75DD0000	mov rcx,qword ptr ds:[7FF8E1516000]	
00007FF8E1508288	48:8D05 6EDD0000	lea rax,qword ptr ds:[7FF8E1516000]	
00007FF8E1508292	48:88AC24 B8000000	mov rbp,qword ptr ss:[rsp+88]	
00007FF8E150829A	4C:8BB424 B0000000	mov r14,qword ptr ss:[rsp+80]	
00007FF8E15082A2	48:38C8	mov rcx,rax	
00007FF8E15082A5	< 74 23	je amsi.7FF8E15082CA	
00007FF8E15082A7	< 6F41 1C 04	test byte ptr ds:[rcx+1C],4	
00007FF8E15082A8	< 74 1D	je amsi.7FF8E15082CA	
00007FF8E15082AD	48:8849 10	mov rcx,qword ptr ds:[rcx+10]	
00007FF8E15082B1	4C:88CB	mov r9,rbx	
00007FF8E15082B4	49:896B B0	mov qword ptr ds:[r11-50],rbp	
00007FF8E15082B8	4D:8973 A8	mov qword ptr ds:[r11-58],r14	
00007FF8E15082BC	44:894424 28	mov dword ptr ss:[rsp+28],r8d	
00007FF8E15082C1	49:8953 98	mov qword ptr ds:[r11-68],rdx	
00007FF8E15082C5	E8 66070000	call amsi.7FF8E1508A30	
00007FF8E15082CA	48:85F6	test rsi,rsi	
00007FF8E15082CD	< 74 68	je amsi.7FF8E1508337	
00007FF8E15082CF	85FF	test edi,edi	



My focus

- Malware development
- AI assisted hacking
- Hacking agentic AI
- Nation state APT replication
- Offensive Software Engineering



```
00007ffa9b5432a0 cc int 3
0:015> !peb
PEB at 00000bc5bdd1000
InheritedAddressSpace: No
ReadImageFileExecOptions: No
BeingDebugged: Yes
ImageBaseAddress: 00007ff730060000
NtGlobalFlag: 0
NtGlobalFlag2: 0
Ldr: 00007ffa9b5f0860
Ldr.Initialized: Yes
Ldr.InInitializationOrderModuleList: 0000263821053e0 . 00002638212b1b0
Ldr.InLoadOrderModuleList: 0000263821055b0 . 00002638212b190
Ldr.InMemoryOrderModuleList: 0000263821055c0 . 00002638212b1ae
Base TimeStamp Module
7ff730060000 698f96ee Feb 13 22:26:06 2026 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
7ffa9b420000 b97e84a2 Aug 13 11:40:50 2068 C:\WINDOWS\SYSTEM32\ntdll.dll
7ffa9acb0000 d5271ecc Apr 28 06:06:36 2083 C:\WINDOWS\System32\KERNEL32.DLL
7ffa98ce0000 3e0f7b9b Dec 29 23:47:55 2002 C:\WINDOWS\System32\KERNELBASE.dll
7ffa6ad60000 698f96ee Feb 13 22:26:06 2026 C:\Program Files (x86)\Microsoft\Edge\Application\145.0.3800.58\msedge_elf.dll
7ffa992b0000 a251a592 Apr 18 07:03:14 2056 C:\WINDOWS\System32\combase.dll
7ffa988e0000 f5b006de Aug 14 21:13:34 2100 C:\WINDOWS\System32\ucrtrbase.dll
7ffa99880000 b6f770d3 Apr 10 15:59:47 2067 C:\WINDOWS\System32\RPCRT4.dll
7ffa991d0000 fb8672ed Sep 22 10:21:01 2103 C:\WINDOWS\System32\bcryptprimitives.dll
7ffa9aa90000 1657d166 Nov 17 15:06:30 1981 C:\WINDOWS\System32\ADVAPI32.dll
7ffa9ae00000 6c01cee1 Jun 03 23:23:45 2027 C:\WINDOWS\System32\msvcrt.dll
7ffa9a530000 c4a45fe9 Jul 18 04:33:13 2074 C:\WINDOWS\System32\sechost.dll
7ffa1aa00000 698f96ee Feb 13 22:26:06 2026 C:\Program Files (x86)\Microsoft\Edge\Application\145.0.3800.58\msedge.dll
7ffa57c50000 fca92f64 Apr 29 23:02:28 2104 C:\WINDOWS\SYSTEM32\WINMM.dll
7ffa55c10000 7fc4f811 Dec 05 09:36:33 2037 C:\WINDOWS\SYSTEM32\dghelp.dll
7ffa9b180000 90c1a1cf Dec 16 22:36:15 2046 C:\WINDOWS\System32\OLEAUT32.dll
7ffa98830000 fc501c8d Feb 22 08:30:21 2104 C:\WINDOWS\System32\msvc_p_win.dll
26386260000 9d63febb Sep 04 07:23:07 2053 C:\WINDOWS\System32\ws2_32.dll
7ffa942b0000 de9dcadb May 08 21:30:35 2088 C:\WINDOWS\SYSTEM32\dwwrite.dll
7ffa699c0000 698f96ee Feb 13 22:26:06 2026 C:\Program Files (x86)\Microsoft\Edge\Application\145.0.3800.58\ffmpeg.dll
7ffa98b60000 0cf755f0 Nov 22 19:39:44 1976 C:\WINDOWS\System32\crypt32.dll
7ffa98460000 936fa18b May 20 07:50:03 2048 C:\WINDOWS\SYSTEM32\DPAPI.dll

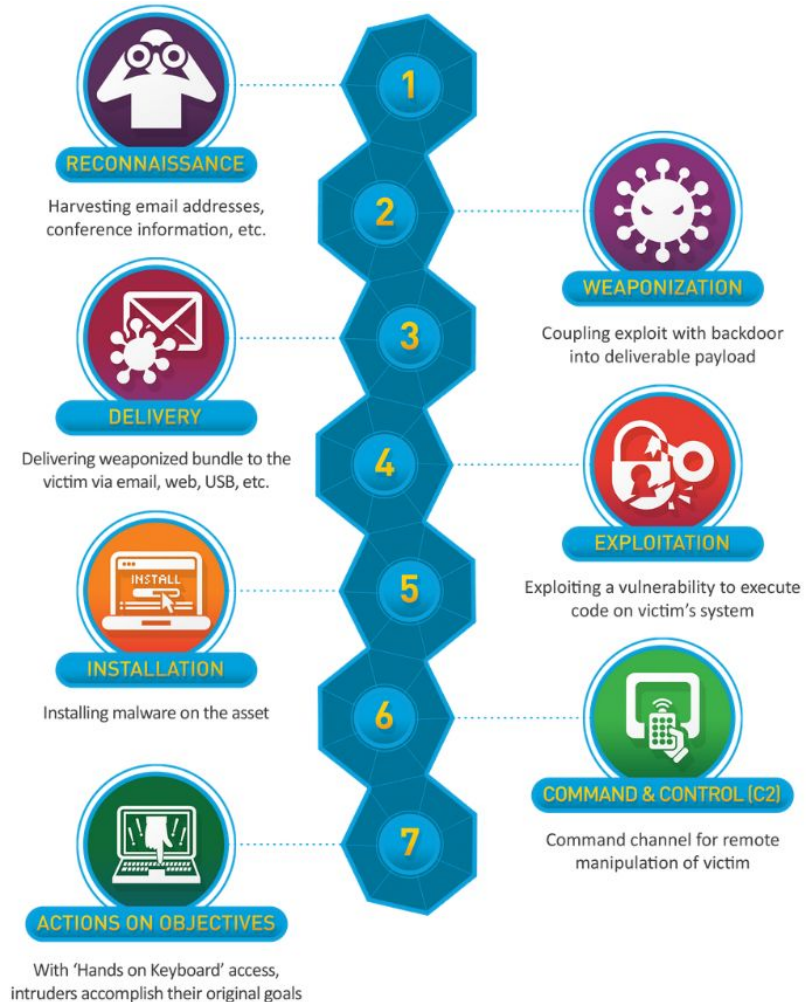
SubSystemData: 0000000000000000
ProcessHeap: 000026382000000

0:015>
```

What is “Hacking”

Cyber killchain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives



ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	External Remote Services	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Defacement (2)	Disk Wipe (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	ESXi Administration Command	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Email Bombing	Endpoint Denial of Service (4)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Exploitation for Client Execution	Create Account (3)	Event Triggered Execution (18)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Data from Cloud Storage	Data from Configuration Repository (2)	Encrypted Channel (2)	Financial Theft	Firmware Corruption
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Exclusive Control	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Data from Information Repositories (6)	Hide Infrastructure	Fallback Channels	Inhibit System Recovery	Network Denial of Service (2)
Search Open Websites/Domains (3)	Trusted Relationship	Native API	Poisoned Pipeline Execution	Event Triggered Execution (18)	Escape to Host	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Data from Network Shared Drive	Taint Shared Content	Ingress Tool Transfer	Scheduled Transfer	Resource Hijacking (4)
Search Threat Vendor Data	Valid Accounts (4)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Exploitation for Privilege Escalation	Execution Guardrails (2)	Email Spoofing	Multi-Factor Authentication Request Generation	Device Driver Discovery	Data from Network Shared Drive	Use Alternate Authentication Material (4)	Multi-Stage Channels	Transfer Data to Cloud Account	Service Stop
Search Victim-Owned Websites	Wi-Fi Networks	Serverless Execution	Serverless Execution	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Execution Guardrails (2)	Network Sniffing	Domain Trust Discovery	Data from Removable Media	Data from Local System	Non-Application Layer Protocol	System Shutdown/Reboot	
		Shared Modules	Shared Modules	Implant Internal Image	File and Directory Permissions Modification (2)	Exploitation for Defense Evasion	File and Directory Permissions Modification (2)	File and Directory Discovery	Data Staged (2)	Data from Network Shared Drive	Non-Standard Port		
		Software Deployment Tools	Software Deployment Tools	Process Injection (12)	Hide Artifacts (14)	File and Directory Permissions Modification (2)	OS Credential Dumping (3)	Group Policy Discovery	Email Collection (2)	Proxy (4)	Protocol Tunneling		
		System Services (3)	System Services (3)	Implant Internal Image	Scheduled Task/Job (5)	Hide Artifacts (14)	Steal Application Access Token						

DEFEND™

A knowledge graph of cybersecurity countermeasures

1.3.0

ATT&CK Lookup

Search D3FEND's 874 Artifacts

D3FEND Lookup

Model	Harden							Detect							Isolate			
+	Agent Authentication	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	Source Code Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Physical Access Monitoring	Platform Monitoring	Process Analysis	User Behavior Analysis	Access Mediation	Access Policy Administration	Content Filtering	Execu Isolat
	Biometric Authentication	Application Configuration Hardening	Certificate Pinning	Message Authentication	Bootloader Authentication	Credential Scrubbing	Dynamic Analysis	Homograph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Electronic Lock Monitoring	Application Performance Monitoring	Database Query String Analysis	Authentication Event Thresholding	Credential Transmission Scoping	Domain Trust Policy	Content Modification	Applic base Proc Isol
	Certificate-based Authentication	Dead Code Elimination	Credential Rotation	Message Encryption	Disk Encryption	Domain Logic Validation	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Application Protocol Command Analysis	Motion Sensor Monitoring	Application Exception Monitoring	File Access Pattern Analysis	Authorization Event Thresholding	IO Port Restriction	Local File Permissions	Content Excision	Execu Allow
	Multi-factor Authentication	Exception Handler Pointer Validation	Certificate Rotation	Transfer Agent Authentication	Driver Load Integrity Checking	Operational Logic Validation	File Content Analysis	Identifier Reputation Analysis	Sender Reputation Analysis	Application Protocol Command Analysis	Proximity Sensor Monitoring	File Integrity Monitoring	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Network Access Mediation	User Account Permissions	Content Format Conversion	Execu Deny
	Password Authentication	Pointer Authentication	Password Rotation		File Encryption	Integer Range Validation	File Content Rules	Domain Name Reputation Analysis		Remote Firmware Update Monitoring	Video Surveillance	Firmware Behavior Analysis	Process Code Segment Verification	Domain Account Monitoring	LAN Access Mediation	User Group Permissions	Content Rebuild	Hardw base Proc Isol
	Token-based Authentication		One-time Password		Hardware-based Write Protection	Pointer Validation	File Hashing	File Hash Reputation Analysis		Byte Sequence Emulation		Firmware Embedded Monitoring Code	Process Self-Modification Detection	Job Function Access Pattern Analysis	Routing Access Mediation		Content Substitution	Hardw base Proc Isol
		Process Segment Execution Prevention	Strong Password Policy		Physical Enclosure Hardening	Memory Block Start Validation		File Hash Reputation Analysis		Certificate Analysis		Firmware Verification	Process Spawn Analysis	Local Account Monitoring	Network Resource Access Mediation		Content Quarantine	Kernel base Proc Isol
		Segment Address Offset Randomization	Change Default Password		RF Shielding	Null Pointer Checking		IP Reputation Analysis		Active Certificate Analysis		Peripheral Firmware Verification	Process Lineage Analysis	Resource Access Pattern Analysis	Remote File Access Mediation		Content Validation	Kernel base Proc Isol
		Stack Frame Canary Validation	Token Binding		Software Update	Reference Nullification		URL Reputation Analysis		Passive Certificate Analysis		System Firmware Verification	Process Lineage Analysis	Session Duration Analysis	Web Session Access Mediation		File Format Verification	Kernel base Proc Isol
					System Configuration Permissions	Trusted Library		URL Analysis		Client-server Payload Profiling		Operating Mode Monitoring	Script Execution Analysis	User Data Transfer Analysis	Endpoint-based Web Server Access Mediation		File Content Decompression Checking	Kernel base Proc Isol
					TPM Boot Integrity	Variable Initialization				Connection Attempt Analysis		Operating System Monitoring	Shadow Stack Comparisons	User Geolocation Logon Pattern Analysis	Proxy-based Web Server Access Mediation		File Internal Structure Verification	Kernel base Proc Isol
						Variable Type Validation				DNS Traffic Analysis		Endpoint Health Beacon	System Call Analysis	User Geolocation Logon Pattern Analysis	Proxy-based Web Server Access Mediation		File Metadata Consistency Validation	Kernel base Proc Isol
										File Carving		Input Device Analysis	File Creation Analysis	Web Session Activity Analysis	Operating Mode		File Metadata Value Verification	Kernel base Proc Isol
										Inbound Session Volume							File Magic Byte Verification	Kernel base Proc Isol

What are the biggest problem in
Cybersecurity?

Top 5 findings that I give customers.

- Default or weak credentials
- Unpatched or legacy systems with known vulnerabilities
- Insecure defaults in software - LLMNR, open LDAP etc.
- Lack of network segmentation
- Publicly exposed API keys and or credentials

Basic configuration errors.

Running systems are old.

Pentesting can be kinda like a computer-janitor

- Clean up after other spill the secrets
- Sounds cool on the outside, it's really not that glamorous
- You're often hidden away in a closet for the business people
- It's often not relevant to do the cool hacking stuff.

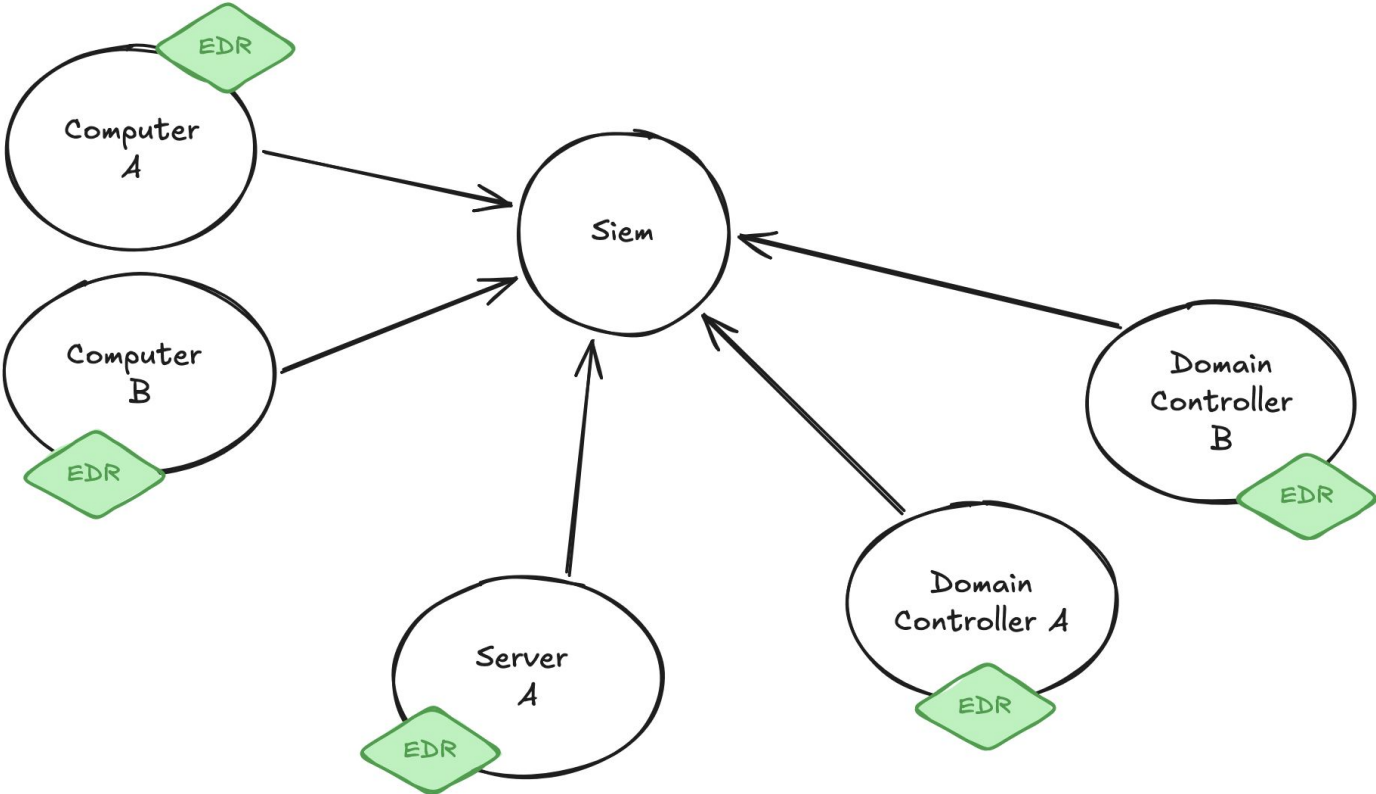


Defending against attacks

An Endpoint Detection and Response (EDR) system monitors devices like laptops and servers for suspicious activity in real time.

It collects and analyzes data from endpoints to detect threats such as malware, ransomware, and unauthorized access by looking into the network logs, processes running, random memory scans etc.

Siem solution simplified overview

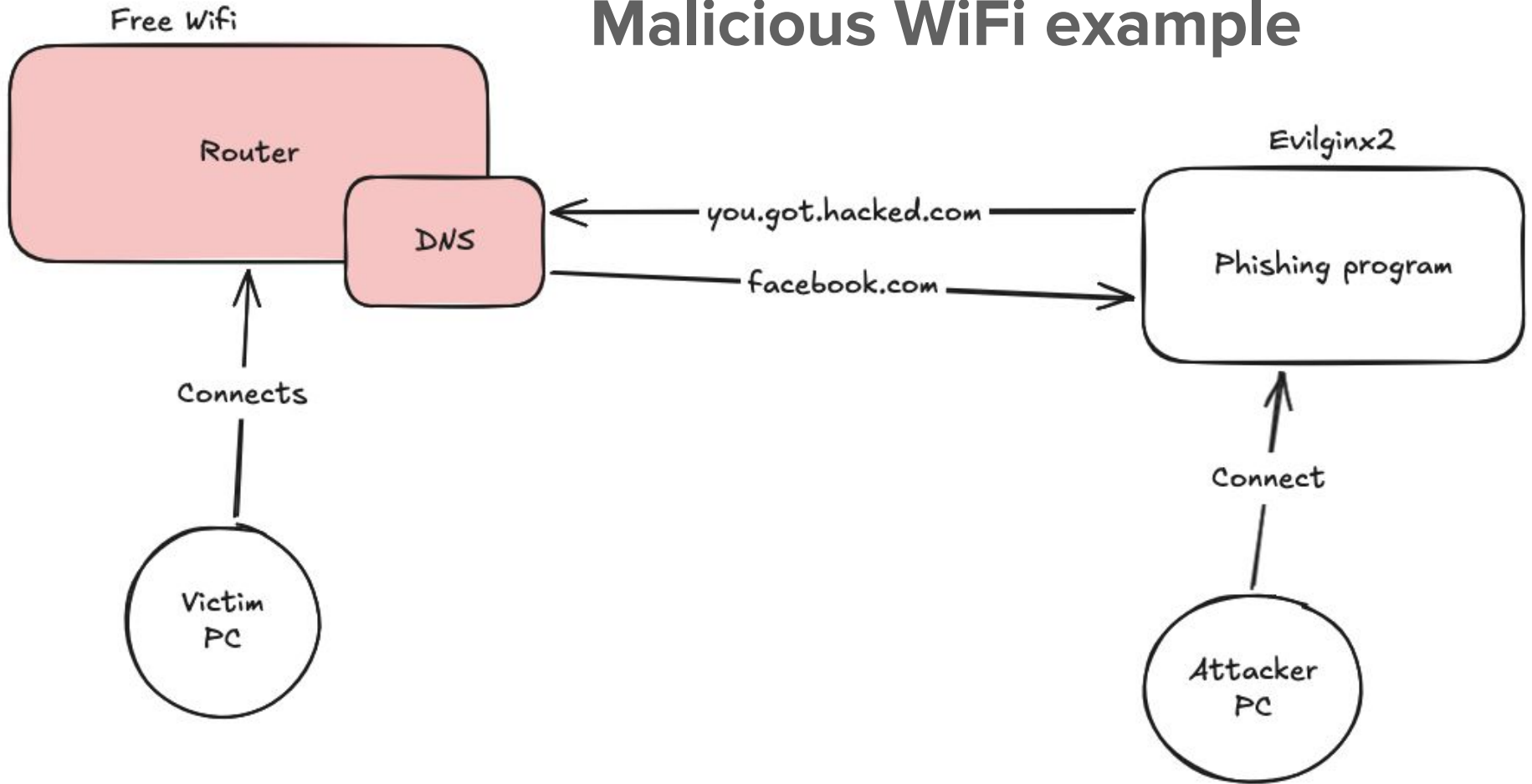


Before AI

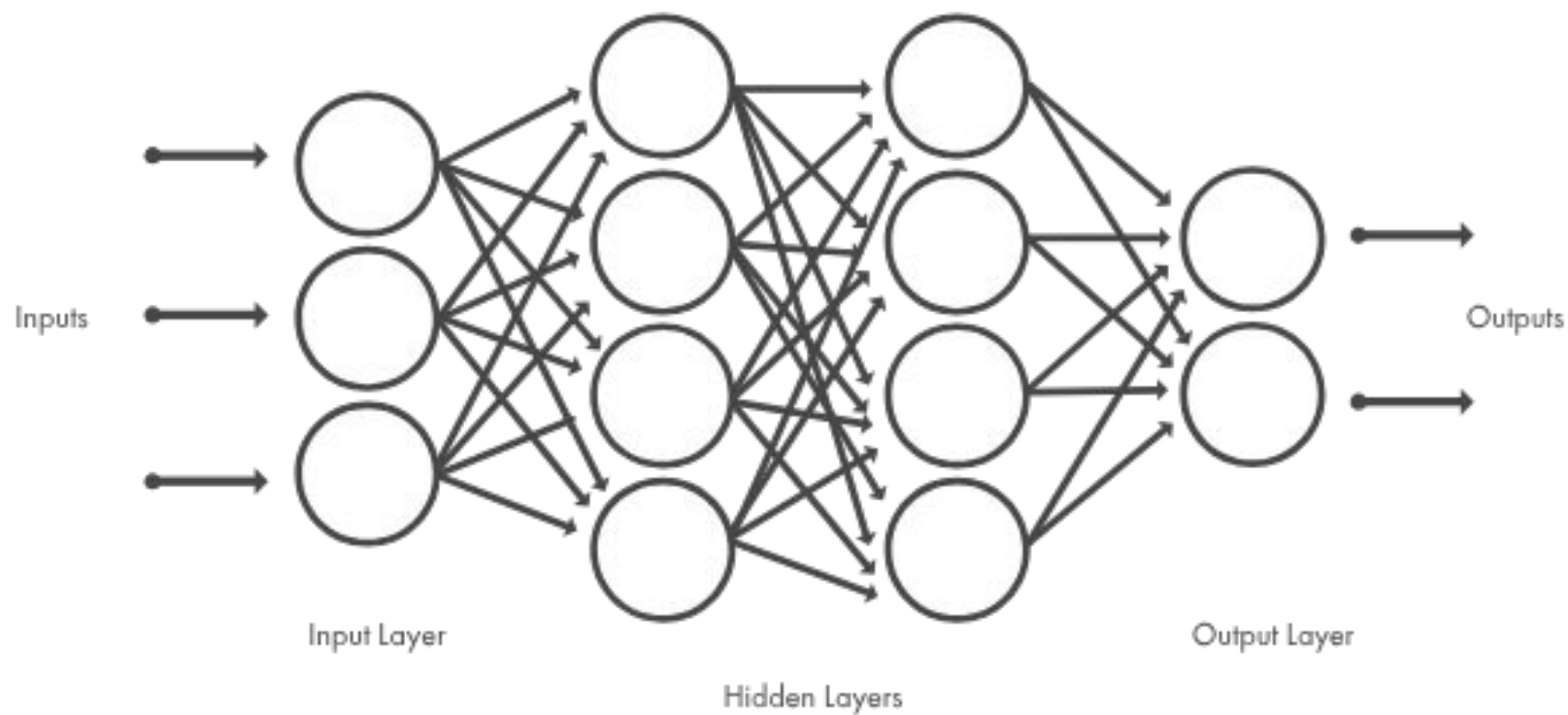
```
23:35:34.377155 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [..], ack 1911, win 1044, options [nop,nop,TS val 3923258880 ecr 3204411711], length 0
23:35:34.377156 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [..], seq 1:1401, ack 1911, win 1044, options [nop,nop,TS val 3923258881 ecr 3204411711], length 1400
23:35:34.377156 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [P.], seq 1401:2801, ack 1911, win 1044, options [nop,nop,TS val 3923258881 ecr 3204411711], length 1400
23:35:34.377157 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [P.], seq 2801:3068, ack 1911, win 1044, options [nop,nop,TS val 3923258881 ecr 3204411711], length 267
23:35:34.377256 IP airtilhdseselle.localdomain.64449 > 93.243.107.34.bc.googleusercontent.com.https: Flags [..], ack 3068, win 2010, options [nop,nop,TS val 3204411736 ecr 3923258881], length 0
23:35:34.379034 IP airtilhdseselle.localdomain.64449 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1911:1975, ack 3068, win 2048, options [nop,nop,TS val 3204411738 ecr 3923258881], length 64
23:35:34.379428 IP airtilhdseselle.localdomain.64449 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1975:2067, ack 3068, win 2048, options [nop,nop,TS val 3204411738 ecr 3923258881], length 92
23:35:34.396842 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [P.], seq 3068:3686, ack 2067, win 1044, options [nop,nop,TS val 3923258908 ecr 3204411738], length 618
23:35:34.396843 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [..], seq 3686:3717, ack 2067, win 1044, options [nop,nop,TS val 3923258908 ecr 3204411738], length 31
23:35:34.396930 IP airtilhdseselle.localdomain.64449 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], ack 3717, win 2038, options [nop,nop,TS val 3204411756 ecr 3923258908], length 0
23:35:34.397649 IP airtilhdseselle.localdomain.64449 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 2067:2098, ack 3717, win 2048, options [nop,nop,TS val 3204411757 ecr 3923258908], length 31
23:35:34.398540 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [SEW], seq 2315919718, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 812550875 ecr 0,sackOK,eol], length 0
23:35:34.416724 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [S.], seq 2752700405, ack 2315919719, win 65535, options [mss 1412,sackOK,TS val 1611678783 ecr 812550875,nop,wscale 8], length 0
23:35:34.416857 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [..], ack 1, win 2057, options [nop,nop,TS val 812550894 ecr 1611678783], length 0
23:35:34.417736 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1:1251, ack 1, win 2057, options [nop,nop,TS val 812550895 ecr 1611678783], length 1250
23:35:34.421768 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64449: Flags [..], ack 2098, win 1044, options [nop,nop,TS val 3923258932 ecr 3204411757], length 0
23:35:34.426768 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [P.], seq 1:1251, win 1046, options [nop,nop,TS val 1611678801 ecr 812550895], length 1250
23:35:34.443914 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [P.], seq 1:219, ack 1251, win 1046, options [nop,nop,TS val 1611678810 ecr 812550895], length 218
23:35:34.444016 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], ack 219, win 2054, options [nop,nop,TS val 812550921 ecr 1611678810], length 0
23:35:34.445065 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1251:1315, ack 219, win 2054, options [nop,nop,TS val 812550922 ecr 1611678810], length 64
23:35:34.445463 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1315:1933, ack 219, win 2054, options [nop,nop,TS val 812550922 ecr 1611678810], length 618
23:35:34.476253 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [..], ack 1933, win 1044, options [nop,nop,TS val 1611678830 ecr 812550922], length 0
23:35:34.640016 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [P.], seq 219:1051, ack 1933, win 1044, options [nop,nop,TS val 1611678986 ecr 812550922], length 832
23:35:34.641017 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [..], ack 1051, win 2041, options [nop,nop,TS val 812551118 ecr 1611678986], length 0
23:35:34.644941 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [P.], seq 1933:2072, ack 1051, win 2048, options [nop,nop,TS val 812551122 ecr 1611678986], length 139
23:35:34.677824 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [..], ack 2072, win 1044, options [nop,nop,TS val 1611679033 ecr 812551122], length 0
23:35:34.817501 IP 93.243.107.34.bc.googleusercontent.com.https > airtilhdseselle.localdomain.64450: Flags [P.], seq 1051:1243, ack 2072, win 1044, options [nop,nop,TS val 1611679183 ecr 812551122], length 192
23:35:34.817615 IP airtilhdseselle.localdomain.64450 > 93.243.107.34.bc.googleusercontent.com.https: Flags [..], ack 1243, win 2045, options [nop,nop,TS val 812551295 ecr 1611679183], length 0
23:35:34.823138 IP airtilhdseselle.localdomain.63076 > unifi.localdomain.domain: 458399: A7 firefox.settings.services.mozilla.com. (55)
23:35:34.851263 IP unifi.localdomain.domain > airtilhdseselle.localdomain.63076: 45839: S/0/1 CNAME mozilla.mop.fastly.net., A 151.101.193.91, A 151.101.65.91, A 151.101.129.91, A 151.101.1.91 (166)
23:35:34.854084 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [SEW], seq 2268545620, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 519840434 ecr 0,sackOK,eol], length 0
23:35:34.862296 IP airtilhdseselle.localdomain.55725 > unifi.localdomain.domain: 12741: PTR 91.65.101.151.in-addr.arpa. (44)
23:35:34.877671 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [S.], seq 1766575755, ack 2268545621, win 65535, options [mss 1460,sackOK,TS val 891272936 ecr 519840434,nop,wscale 9], length 0
23:35:34.877796 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [..], ack 1, win 2059, options [nop,nop,TS val 519840458 ecr 891272936], length 0
23:35:34.877952 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [P.], seq 1:223, ack 1, win 2059, options [nop,nop,TS val 519840458 ecr 891272936], length 222
23:35:34.889841 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], ack 223, win 285, options [nop,nop,TS val 891272960 ecr 519840458], length 0
23:35:34.889843 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], seq 1:1445, ack 223, win 285, options [nop,nop,TS val 891272961 ecr 519840458], length 1444
23:35:34.889844 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [P.], seq 1445:2889, ack 223, win 285, options [nop,nop,TS val 891272961 ecr 519840458], length 1444
23:35:34.889845 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [P.], seq 2889:3063, ack 223, win 285, options [nop,nop,TS val 891272961 ecr 519840458], length 174
23:35:34.889996 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [..], ack 3063, win 2012, options [nop,nop,TS val 519840470 ecr 891272961], length 0
23:35:34.892408 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [P.], seq 223:316, ack 3063, win 2048, options [nop,nop,TS val 519840472 ecr 891272961], length 93
23:35:34.903139 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], ack 316, win 285, options [nop,nop,TS val 891272974 ecr 519840472], length 0
23:35:34.903141 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [P.], seq 3063:3321, ack 316, win 285, options [nop,nop,TS val 891272974 ecr 519840472], length 258
23:35:34.903266 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [..], ack 3321, win 2044, options [nop,nop,TS val 519840483 ecr 891272974], length 0
23:35:34.904083 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [P.], seq 316:415, ack 3321, win 2048, options [nop,nop,TS val 519840484 ecr 891272974], length 99
23:35:34.904133 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [P.], seq 415:689, ack 3321, win 2048, options [nop,nop,TS val 519840484 ecr 891272974], length 274
23:35:34.910202 IP unifi.localdomain.domain > airtilhdseselle.localdomain.55725: 12741: NXDomain 0/1/1 (115)
23:35:34.914041 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], ack 415, win 285, options [nop,nop,TS val 891272985 ecr 519840484], length 0
23:35:34.914042 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], ack 689, win 287, options [nop,nop,TS val 891272985 ecr 519840484], length 0
23:35:34.914043 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [P.], seq 3321:3393, ack 689, win 287, options [nop,nop,TS val 891272985 ecr 519840484], length 72
23:35:34.914044 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [P.], seq 3393:4311, ack 689, win 287, options [nop,nop,TS val 891272986 ecr 519840484], length 918
23:35:34.914532 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [..], ack 4311, win 2033, options [nop,nop,TS val 519840495 ecr 891272986], length 0
23:35:34.914705 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [P.], seq 689:727, ack 4311, win 2034, options [nop,nop,TS val 519840495 ecr 891272986], length 38
23:35:34.916191 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [P.], seq 727:864, ack 4311, win 2048, options [nop,nop,TS val 519840496 ecr 891272986], length 137
23:35:34.925302 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], ack 864, win 287, options [nop,nop,TS val 519840497 ecr 519840496], length 0
23:35:34.927204 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [..], seq 864, win 290, options [nop,nop,TS val 891272998 ecr 519840496], length 0
23:35:34.927205 IP 151.101.65.91.https > airtilhdseselle.localdomain.64451: Flags [P.], seq 4311:4559, ack 864, win 290, options [nop,nop,TS val 891272998 ecr 519840496], length 248
23:35:34.927283 IP airtilhdseselle.localdomain.64451 > 151.101.65.91.https: Flags [..], ack 4559, win 2045, options [nop,nop,TS val 519840507 ecr 891272998], length 0
23:35:36.583638 IP rc-in-f101.1e100.net.https > airtilhdseselle.localdomain.58478: quic, protected
23:35:36.584082 IP airtilhdseselle.localdomain.58478 > rc-in-f101.1e100.net.https: quic, protected
23:35:37.300751 IP unifi.localdomain.53830 > 233.89.188.1 scp-config: UDP, length 4
23:35:37.300755 IP unifi.localdomain.53830 > broadcasthost.scp-config: UDP, length 4
23:35:37.300756 LLD, length 235: UX
```

What are all the unique IPs in this dump? Who is speaking with who?

Malicious WiFi example

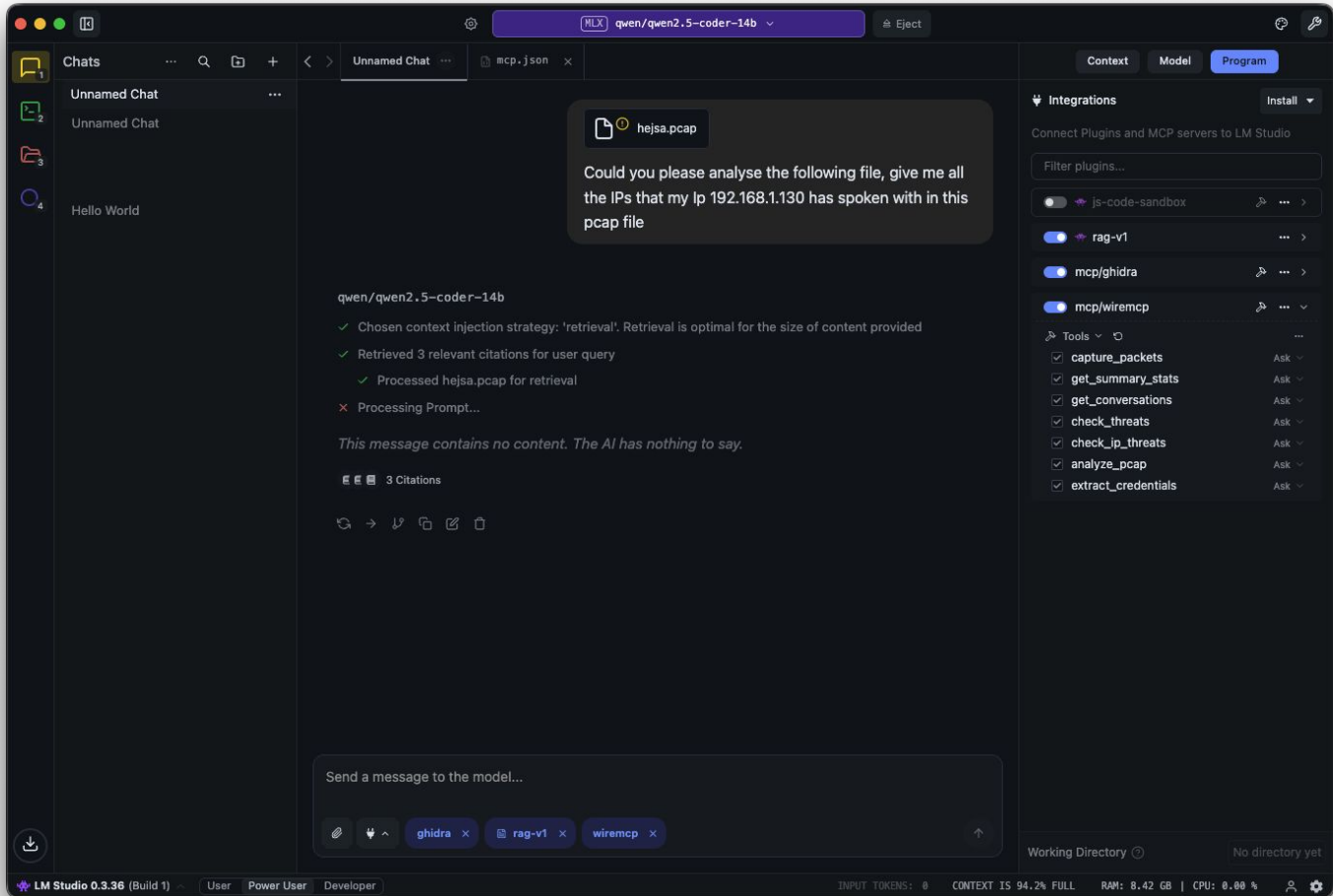


What is done after AI



An **MCP server** (from the Model Context Protocol) is a system that lets an AI connect to tools and data outside itself. It acts like a bridge between the AI and things like databases, apps, or APIs. Instead of just answering questions, the AI can fetch real information or perform actions. The server tells the AI what tools are available and runs them when needed. In short, it helps AI move from just “thinking” to actually “doing.”

```
vim settings.json ~/gemini
{
  "security": {
    "auth": {
      "selectedType": "oauth-personal"
    }
  },
  "mcpServers": {
    "ghidra": {
      "command": "/Users/selle/mcp/GhidraMCP-release-1-4/.venv/bin/python3",
      "args": [
        "/Users/selle/mcp/GhidraMCP-release-1-4/bridge_mcp_ghidra.py",
        "--ghidra-server",
        "http://127.0.0.1:8080/"
      ]
    },
    "wiremcp": {
      "command": "node",
      "args": [
        "/Users/selle/mcp/WireMCP/index.js"
      ]
    }
  }
}
```



→ Here are the resolved hostnames for the IP addresses:

```
- 104.18.11.183: Not found
- 104.18.32.47: Not found
- 121.127.45.81: 429456321.cph.cdn77.com.
- 121.127.45.82: 429456321.cph.cdn77.com.
- 139.45.105.72: 139-45-105-72.norlyscustomer.net.
- 139.45.105.74: 139-45-105-74.norlyscustomer.net.
- 139.45.105.83: 139-45-105-83.norlyscustomer.net.
- 139.45.105.91: 139-45-105-91.norlyscustomer.net.
- 142.250.147.101: rd-in-f101.1e100.net.
- 142.250.147.132: rd-in-f132.1e100.net.
- 142.250.147.84: rd-in-f84.1e100.net.
- 142.250.147.93: rd-in-f93.1e100.net.
- 142.250.147.94: rd-in-f94.1e100.net.
- 142.250.186.78: fra24s05-in-f14.1e100.net., lcfraa-br-in-f14.1e100.net.
- 142.251.127.141: lcfrai-in-f141.1e100.net.
- 142.251.127.84: lcfrai-in-f84.1e100.net.
- 142.251.127.91: lcfrai-in-f91.1e100.net.
- 142.251.141.131: tzfrraa-aj-in-f3.1e100.net.
- 142.251.153.119: Not found
- 142.251.155.119: Not found
- 142.251.9.100: rc-in-f100.1e100.net.
- 142.251.9.101: rc-in-f101.1e100.net.
- 142.251.9.94: rc-in-f94.1e100.net.
- 142.251.9.95: rc-in-f95.1e100.net.
- 151.101.1.140: Not found
```

Took around 5 minutes, even
with gemini

```
Gemini - gemini
* 142.250.147.94: rd-in-f94.1e100.net
* 142.251.127.141: lcfrai-in-f141.1e100.net
* 142.250.147.84: rd-in-f84.1e100.net
* 142.251.9.101: rc-in-f101.1e100.net
* 172.217.16.206: tzfrraa-at-in-f14.1e100.net
* 199.232.41.91: Not found
* 151.101.193.91: Not found
* 3.174.16.159: server-3-174-16-159.cph50.r.cloudfront.net
* 199.232.173.91: Not found
* 139.45.105.91: 139-45-105-91.norlyscustomer.net
* 3.174.18.125: server-3-174-18-125.cph50.r.cloudfront.net
* 139.45.105.74: 139-45-105-74.norlyscustomer.net
* 139.45.105.72: 139-45-105-72.norlyscustomer.net
* 139.45.105.83: 139-45-105-83.norlyscustomer.net
* 121.127.45.82: 429456321.cph.cdn77.com
* 95.101.195.215: a95-101-195-215.deploy.static.akamaitechnologies.com
* 3.174.18.30: server-3-174-18-30.cph50.r.cloudfront.net
* 121.127.45.81: 429456321.cph.cdn77.com
* 151.101.1.140: Not found
* 151.101.193.140: Not found
* 151.101.129.140: Not found
* 104.18.11.183: Not found
* 3.90.238.208: ec2-3-90-238-208.compute-1.amazonaws.com
* 142.251.127.84: lcfrai-in-f84.1e100.net
* 142.251.153.119: Not found

> none of the records have any resemblance to tv2.dk?

.: Have you tried turning it off and on again? (The loading screen, not me.) (esc to cancel, 1m 29s)

Using: 2 MCP servers

> █ Type your message or @path/to/file

~/gemini no sandbox (see /docs) Auto (Gemini 2.5) /model
```

Why not just fully automate it?



Keygraph

SHANNON

AI Pentester for Web Apps and APIs

-Authorized Security Testing Only-

Shannon — AI Pentester by Keygraph



Shannon is an autonomous, white-box AI pentester for web applications and APIs. It analyzes your source code, identifies attack vectors, and executes real exploits to prove vulnerabilities before they reach production.



Announcements



Join Discord



Keygraph.io



Follow Us

Fully Automated Pentesting

See XBOW in action.
Speak to a security expert and strengthen your offensive security.

"Even right now after 1 year, I don't know any other company that is at least close to XBOW in terms of agentic pentesting."

Leo Golovyrin
Application Security Lead of Seznam.cz



2

r3aper__

Reputation	1927
Signal	7.00
Impact	35.16



1

xbow

Reputation	3999
Signal	6.73
Impact	17.32



3

n3rdnymph

Reputation	1901
Signal	7.00
Impact	15.00

80x

Faster

Than manual pentesting

1,092±

Vulnerabilities

Zero-day vulnerabilities discovered

XBOW Lightspeed
On-Demand Autonomous Pentest

Zero Day / Zero Pay: If you purchase a Lightspeed pentest, XBOW guarantees an exploit-validated security finding or you don't pay.

XBOW Enterprise
Autonomous Offense at Scale

Plus

\$4,000 /per test

**Comprehensive pentest
for a single application.**

Best for

Lightweight applications with few interconnected features, a modest set of CRUD resources, simple workflows and low integration complexity.

Depth of Test

Provides the depth of a 2 week manual penetration test.

Premium

\$8,000 /per test

**Deeper coverage for
more complex applications.**

Best for

An application or platform with multiple functional modules, integrations, and multi-step workflows. These applications have deeper access control patterns and data models.

Depth of Test

Provides the depth of a 4 week manual penetration test.

Enterprise

Request a Quote

**Continuous coverage for
organizations at scale.**

Best for

A mature application portfolio with broad functionality, such as a multimodule SaaS product supporting complex workflows, admin tools, and extensive resource relationships.

Depth of Test

Continuous security hardening for all feature releases.

What you Get

Comprehensive compliance ready report that meets SOC 2, ISO27001, HIPAA, GDPR, 40+ compliance frameworks.

[GET STARTED](#)

What you Get

Comprehensive compliance ready reports, plus continuous security hardening.

[CONTACT SALES](#)

Fully-Automatic AI is really good at being the IT janitor.

Hacking the AI itself

Model extraction

RAG poisoning

Training data

“Computer science is no more about computers, than astronomy is about telescopes”

- Edsger W. Dijkstra

Hacking has never been about the computer

It is everything about human psychology

Generative AI...

<https://thispersondoesnotexist.com/>



I Cloned My Voice With AI in 5 Minutes. Here's How You Can Too.



Justin Levitt

Follow

7 min read · Oct 22, 2025



4



The Problem Every Content Creator Knows Too Well

I can write faster than I can record. Way faster.

“Bad internet - I need to drop camera”

The end
