

Ástandsvitund í ótryggum heimi

SKÝ 29. október 2025

Kristján Valur Jónsson

Um mig

- Tölvunörd frá 1982
- Öryggisnörd í um þrjá áratugi
- Rúman áratug starfandi í net og upplýsingaöryggi
- Seðlabanki Íslands
TIBER Cyber Team - Test Manager
- Ph.D - GIAC GCTI



kristjan.valur.jonsson@sedlabanki.is

<https://www.linkedin.com/in/kristjanvj/>

Efnisyfirlit

- Heimurinn í dag (í örstuttu máli)
- Ástandsvitund, CTI og OSINT í breiðum skilningi
- Tegundir OSINT og upplýsingaveitur
- Hvernig nota árársaraðilar OSINT?
- Hvernig getum við notað OSINT?
- Lokaorð

Þessi fyrirlestur notar raunveruleg OSINT gögn.
Viðkvæmar upplýsingar um bæði fyrirtæki og einstaklinga
eru þó afmáðar eins og unnt er.

Aðilar voru valdir af handahófi og notkun gagna ætti ekki
að skilja sem neikvætt mat á þeirra öryggisstöðu.

Notkun upplýsinga og aðferða er alfarið
á ábyrgð lesanda og/eða áheyranda

Staða heimsins

- Tengdur heimur og snertiflötur stafrænna kerfa
 - Ófriður í Evrópu og víðar
 - Rússland og önnur Evrópulönd
 - Breytingar á valdajafnvægi
 - Óviss staða og hraðar breytingar
-
- Upplýsingar eru vopn – „information“, „disinformation“
 - „Cyber“ sem vopn og „cyberspace“ sem vettvangur átaka°- „Hybrid Warfare“ og „Hybrid Operations“



in·tel·li·gence | \ in-'te-lə-jən(t)s \

1a(1): the ability to learn or understand or to deal with new or trying situations : REASON *also* : the skilled use of reason
(2): the ability to apply knowledge to manipulate one's environment or to think abstractly as measured by objective criteria (such as tests)

c: mental acuteness : SHREWDNESS

b*Christian Science* : the basic eternal quality of divine Mind

2a: INFORMATION, NEWS

b: information concerning an enemy or possible enemy or an area *also* : an agency engaged in obtaining such information

3: the act of understanding : COMPREHENSION

4: the ability to perform computer functions

5a: intelligent minds or mind cosmic *intelligence*

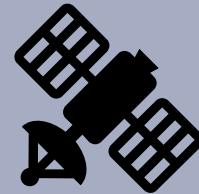
b: an intelligent entity *especially* : ANGEL

<https://www.merriam-webster.com/dictionary/intelligence>

SIGINT



GEOINT



HUMINT



MASINT



„Open-Source Intelligence“ - OSINT



Opnar upplýsingar s.s. úr prentmiðlum,
af netinu og úr skýrslum.
Safnað, unnar og miðlað til að styðja við skilgreint
markmið.

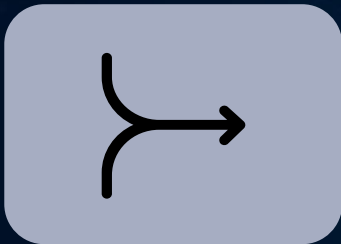
Net- og upplýsingaöryggi

Upplýsingar um kerfi, fólk, fyrirtæki og ferla sem
hægt er að afla með löglegum hætti af netinu

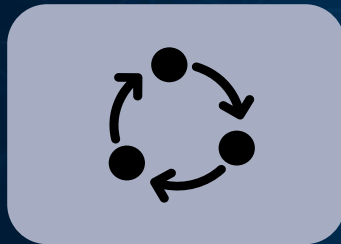
Óvirkt (passive)
Án snertingar

Ástandsvitund „Situational Awareness“

OSINT

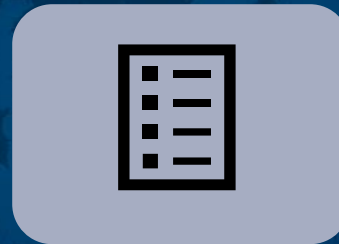


Söfnun upplýsinga

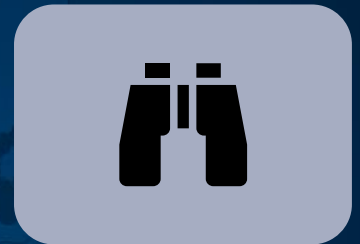


Vinnsla og samþætting

CTI



“Intelligence”



Ástandsvitund



Árás

Upplýsingar sem hafa verið unnar þannig hægt er að beita þeim

CTI – „Cyber Threat Intelligence“



Stefnumarkandi

Langtíma áhættumat
Greiningarskýrslur

Aðgerðamiðað

Tíðara áhættumat
Upplýsingar um herferðir

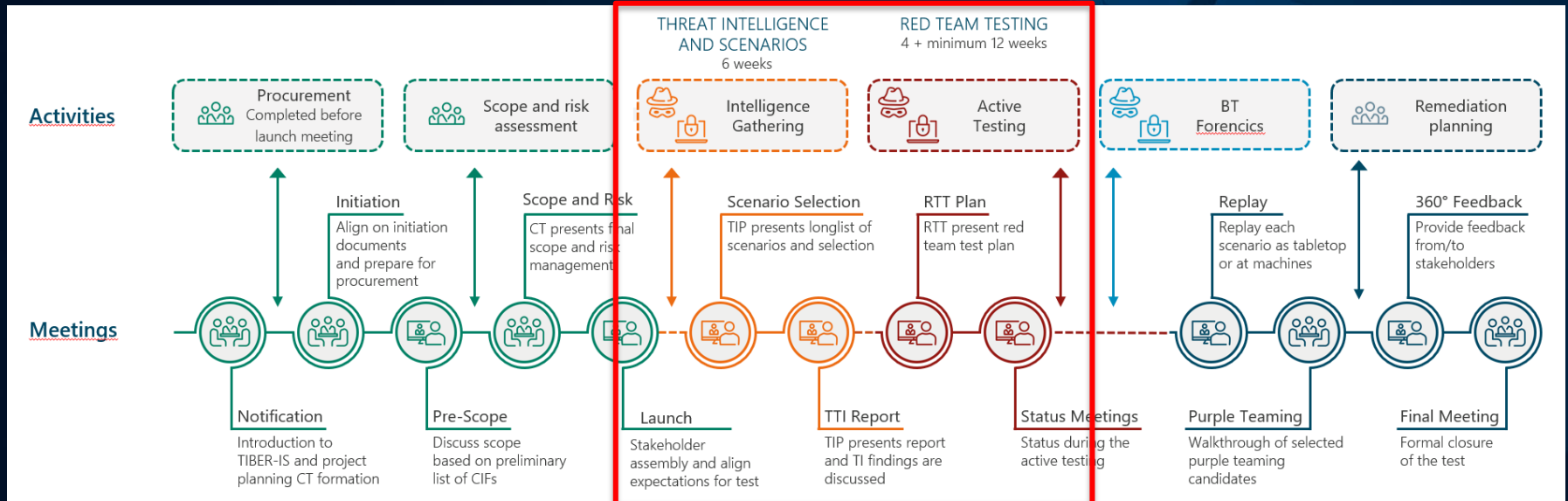
Varnamiðað

Veikleikar í notkun
IoCs og blocklists
„Signatures“



TIBER og TLPT

Threat Intelligence-Based Ethical Red-teaming DORA Threat-Led Penetration Testing



<https://sedlabanki.is/greidslumidlun/rekstrar-og-netoryggismal/>

<https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html>

Hvar finnum við OSINT?

Yfirborðsvefurinn

Surface Web (4-10%)

Opnar upplýsingar

„Google“

Djúpvefurinn

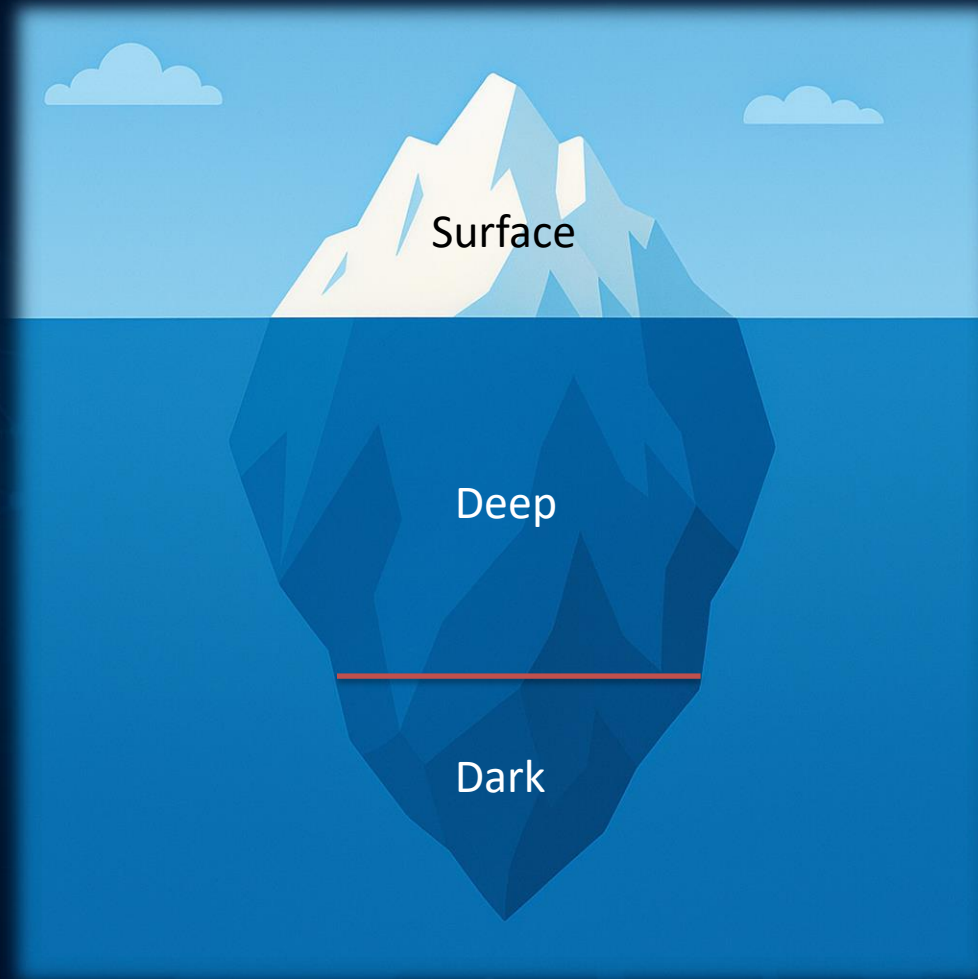
Deep Web (85-95%)

„private“

Hulduvefurinn

Dark Web (<5%)

„anonymous“



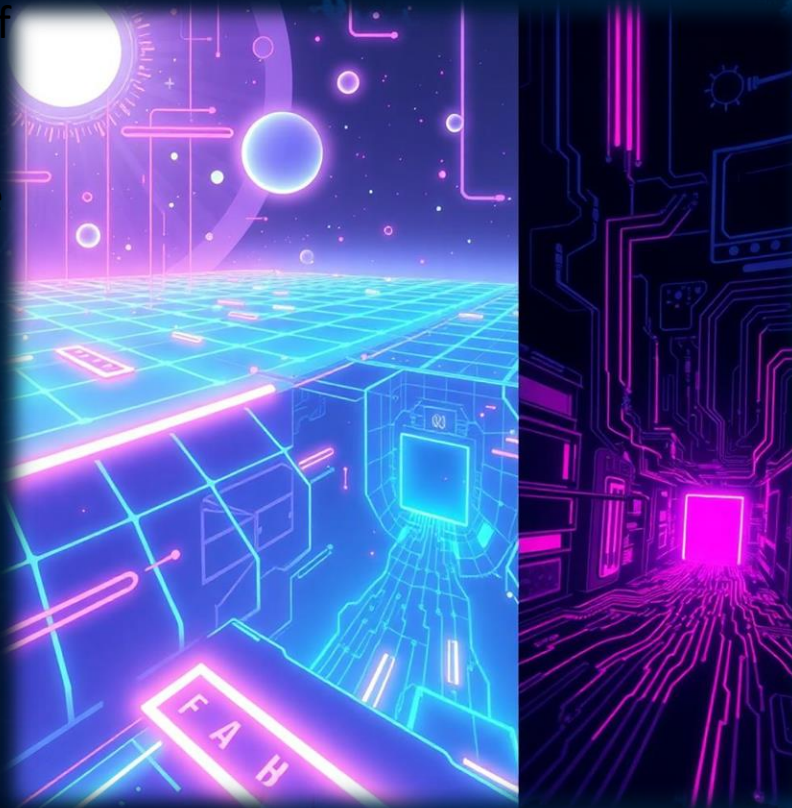
Dark web Hulduvefurinn

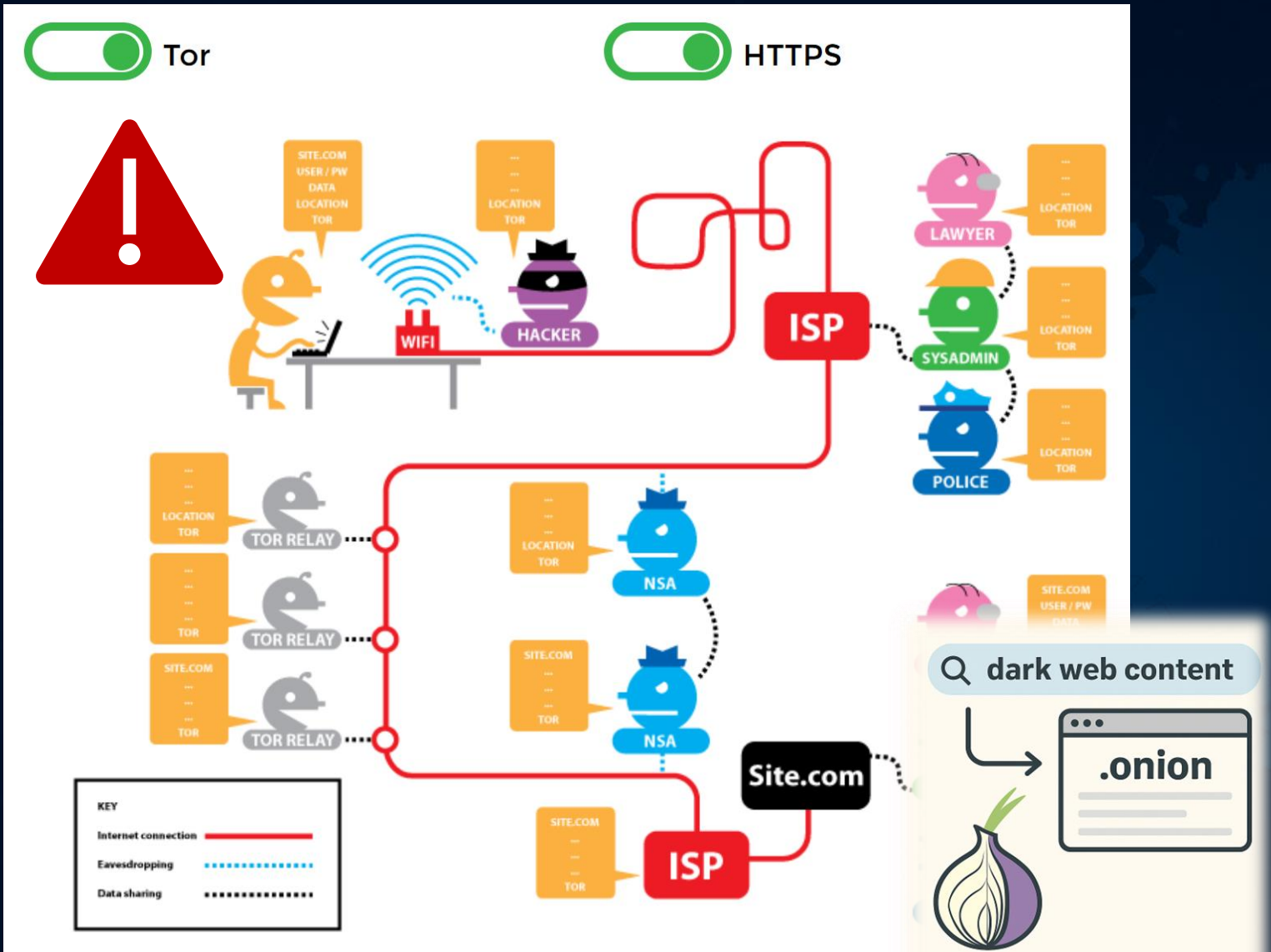
S
u
r
f
a
c
e



<5%

„anonymous“





<https://tor-https.eff.org>

High-level topic	Low-level topics	Uniques	Mirrors	Total
Sexual and violent content	Sexual content Violent content	1,104 (28.5%)	32,426	33,530 (48.2%)
Repositories and search engines	Repositories and search engines	877 (22.7%)	18,221	19,098 (27.5%)
Carding	CVV marketplaces Card dumps and fullz Banking Carding	463 (12%)	6,449	6,912 (9.9%)
Cryptocurrencies	Cryptocurrencies Crypto swapping and exchanges	392 (10.1%)	4,437	4,829 (6.9%)
Marketplaces	Hardware marketplaces Mobile and device marketplaces Drug marketplaces Firearm marketplaces Generic markets	245 (6.3%)	1,614	1,859 (2.7%)
Media, forums and personal websites	Personal websites and blogs News and media Debian community Debian conferences	214 (5.5%)	1,491	1,705 (2.5%)
Navigation pages	Javascript pages Login and register pages DDoS protection pages Redirecting pages Error pages One-line pages 'Index of' pages	196 (5%)	330	526 (0.8%)
Hacking	Data leaks Hacking	180 (4.7%)	332	512 (0.7%)
Counterfeits	Passports and certificates Counterfeits	72 (1.9%)	195	267 (0.4%)
Privacy-preserving services	Image and file hosting Privacy-preserving services	65 (1.7%)	79	144 (0.2%)
Hiring services	Betting services Hitman services Escrow services	61 (1.6%)	56	117 (0.2%)
Total		3,869 (100%)	65,630	69,499 (100%)

A Big Data Architecture for Early Identification and Categorization of Dark Web Sites, Pastor-Galindo et.al, 2024

Synthesis technologies and analysis

Methods of synthesis. From experimental home options to industrial

Amphetamines (phenylethylamines)

Threads: 138 Messages: 1.2K

Methcathinones

Threads: 36 Messages: 167

Tryptamines

Threads: 31 Messages: 94

Cannabinoids

Threads: 55 Messages: 414

Opioids

Threads: 36 Messages: 133

Other






Threads: 87 Messages: 318

Laboratory FAQ


Threads: 45 Messages: 183


Analytical chemistry

Threads: 37 Messages: 94


 MARKET [PREMIUMINFO] - FIRSTHAND FULLZ SSN LOOKUP DL LOOKUP DOCS/PHOTOS - WELCOME - Premiuminfo · Sep 18, 2021 2	🔗 Replies: 30 Views: 6K	24 minutes ago ayamga
 MARKET ★★ < 1977.SH - Market Place SSN BANK SHOP TRAVEL Bank Self-Registration > ★★ 1977 · Jan 11, 2022 2 3 4	🔗 Replies: 64 Views: 7K	31 minutes ago 1977
 MARKET WIZARD'S SHOP EXCLUSIVE CC+CVV PRIVATE SNIFFERS BEST QUALITY ON FORUMS AUTO/NON VBV BINS Harry Potter · Feb 14, 2022 13 14 15	🔗 Replies: 289 Views: 30K	38 minutes ago madman247
 MARKET Sells of USA_Bank Info Tor: http://i5lInq2vuv7in7kmgmw26kxlxxso3f46xhzhlgfhw62r3nboantid.onion sefcu · Oct 3, 2021 9 10 11	🔗 Replies: 217 Views: 28K	Today at 4:34 PM z4n3tti1
 MARKET ⚡ ==> FINDSOME. RU <== THE HOUSE OF CREDIT CARD 【TRUSTED SHOP】 - RESELLERS WELCOME ⚡ FINDSOME-ADMIN · Feb 22, 2022 6 7 8	🔗 Replies: 140 Views: 12K	Today at 4:32 PM FINDSOME-ADMIN

🟢 Today at 1:29 PM · lydiare seller

 Kratom Acid-Base Extraction
Wednesday at 11:24 AM · ASheSCh

 Concentrating acetic acid by freezi...
Yesterday at 3:31 PM · DocX

 Aluminium amalgam (Al/Hg) sum...
Yesterday at 10:21 PM · Pennywise

 Amphetamine assessment protocol
Yesterday at 3:17 PM · G.Patton



<https://branddefense.io/blog/leaked-credentials-from-ransomware-groups>

Surface web

Yfirborðsvefurinn




4-10%
„google“



Identifier	CISA Key Info	Published Date	CNA	Description
CVE-2025-9999	✖	2025-09-05	arcinfo	Some payload elements of the messages sent between two stations in a networking architecture are not properly checked on the receiving station allowing an attacker to execute unauthorized commands in the application.
CVE-2025-9998	✖	2025-09-05	arcinfo	The sequence of packets received by a Networking server are not correctly checked. An attacker could exploit
CVE-2025-9997	✖	2025-09-09	Schneider Ele	
CVE-2025-9996	✖	2025-09-09	Schneider Ele	
CVE-2025-9994	✖	2025-09-09		
CVE-2025-9993	✖	2025-09-30		
CVE-2025-9992	✖	2025-09-18		

MICROSOFT | WINDOWS

 [CVE-2025-59287](#)

Microsoft Windows Server Update Service (WSUS) Deserialization of

BLEEPINGCOMPUTER

NEWS TUTORIALS VIRUS REMOVAL GUIDES DOWNLOADS DEALS VPNS FORUMS MORE

Home > News > Security > The Heat Wasn't Just Outside: Cyber Attacks Spiked in Summer 2025

The Heat Wasn't Just Outside: Cyber Attacks Spiked in Summer 2025

Sponsored by Picus Security | August 5, 2025 | 10:02 AM | 0



Summer 2025 wasn't just hot; it was relentless.

Ransomware hammered hospitals, retail giants suffered data breaches, insurance firms were hit by phishing, and nation-state actors launched disruptive campaigns.

From stealthy PowerShell loaders to zero-day SharePoint exploits, attackers kept defenders on their heels.

 ENISA

EUROPEAN UNION AGENCY FOR CYBERSECURITY



ENISA THREAT LANDSCAPE 2025

OCTOBER 2025

- <https://nvd.nist.gov/vuln/search#/nvd/home?sortOrder=5&sortDirection=1&resultType=records>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://www.bleepingcomputer.com/news/security/the-heat-wasnt-just-outside-cyber-attacks-spiked-in-summer-2025/>
- <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf>

Upplýsingar um starfsfólk

Specialties: Microsoft:

- Microsoft Certified Trainer (MCT)
 - Microsoft Certified Solutions Expert: Server Infrastructure
 - Microsoft Certified Solutions Expert: Private Cloud
 - MCITP, MCP, MCSA, MCSE
- HP:

Hæfniskröfur

- Reynsla og góð þekking á Flutter, React og Typescript
- Reynsla af app þróun fyrir Apple og Android
- Þekking á AWS umhverfinu

Microsoft SQL Server

Endorsed by 3 colleagues at Platon A/S

16 endorsements

Oracle

11 endorsements

SSRS

10 endorsements

SharePoint

9 endorsements

OLAP

8 endorsements

Menntunar- og hæfniskröfur

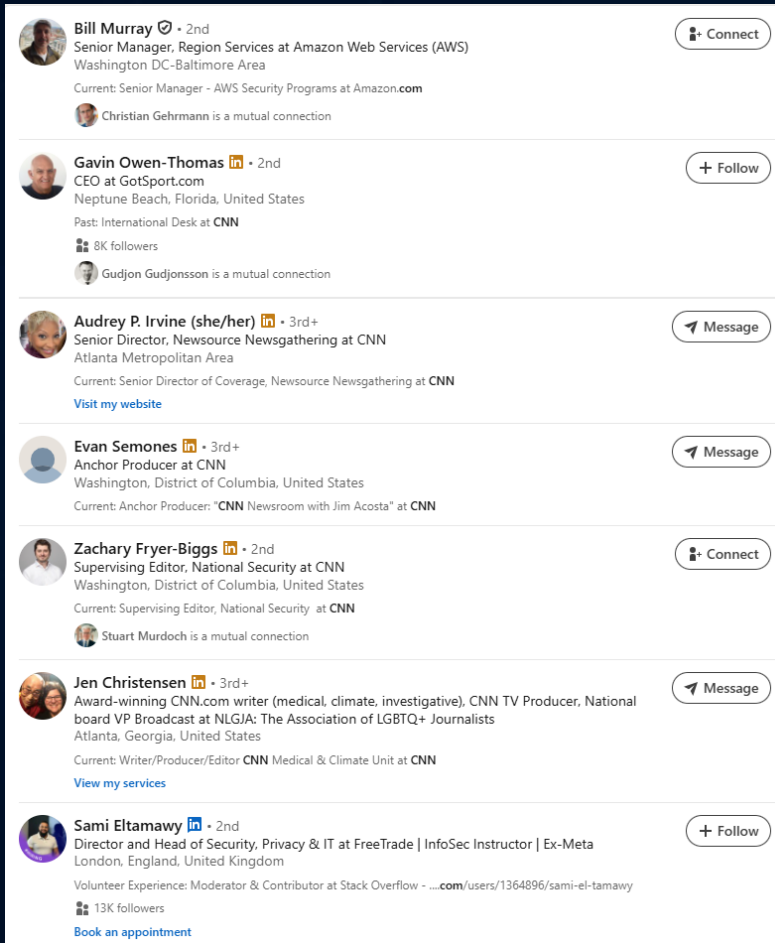
- Gerð er krafa um reynslu sem
- Reynsla af þjónustu við útstöðv
- Reynsla af Cisco netkerfum ko
- Reynsla af Microsoft kerfum na
- Reynsla af rekstri Linux kerfa k
- Reynsla af Jira beiðnakerfinu kostur

Menntunar- og hæfniskröfur

- Háskólamenntun sem nýtist í starfi eða viðeigandi starfsreynsla
- Þekking og reynsla af rekstri á Linux er nauðsynleg
- Þekking og reynsla af Docker og/eða Kubernetes er nauðsynleg
- Þekking á Ansible, Chef og öðrum tólum fyrir sjálfvirknivæðingu er nauðsynleg
- Reynsla af DevOps vinnubrögðum er kostur ásamt CI/CD pipelines
- Reynsla af forritun er kostur

- Gerð er krafa um ríka þjónustulund, jákvæðni, skipulagshæfileika, sjálfstæði og vönduð vinnubrögð ásamt ábyrgðarkennd
- Gott vald á íslensku, jafnt töluðu sem rituðu máli er nauðsynlegt
- Gott vald á ensku, jafnt töluðu sem rituðu máli er nauðsynlegt

Samfélagsmiðlar



A screenshot of a LinkedIn search results page for the keyword 'cnn.com'. The page displays a list of seven profiles, each with a profile picture, name, current position, location, and a button to interact (Connect, Follow, or Message). The profiles are:

- Bill Murray** (2nd): Senior Manager, Region Services at Amazon Web Services (AWS), Washington DC-Baltimore Area. Button: Connect.
- Gavin Owen-Thomas** (2nd): CEO at GotSport.com, Neptune Beach, Florida, United States. Past: International Desk at CNN. 8K followers. Button: Follow.
- Audrey P. Irvine (she/her)** (3rd+): Senior Director, Newsource Newsgathering at CNN, Atlanta Metropolitan Area. Current: Senior Director of Coverage, Newsource Newsgathering at CNN. Button: Message.
- Evan Semones** (3rd+): Anchor Producer at CNN, Washington, District of Columbia, United States. Current: Anchor Producer: "CNN Newsroom with Jim Acosta" at CNN. Button: Message.
- Zachary Fryer-Biggs** (2nd): Supervising Editor, National Security at CNN, Washington, District of Columbia, United States. Current: Supervising Editor, National Security at CNN. Button: Connect.
- Jen Christensen** (3rd+): Award-winning CNN.com writer (medical, climate, investigative), CNN TV Producer, National board VP Broadcast at NLGJA: The Association of LGBTQ+ Journalists, Atlanta, Georgia, United States. Current: Writer/Producer/Editor CNN Medical & Climate Unit at CNN. Button: Message.
- Sami Eltamawy** (2nd): Director and Head of Security, Privacy & IT at FreeTrade | InfoSec Instructor | Ex-Meta, London, England, United Kingdom. Volunteer Experience: Moderator & Contributor at Stack Overflow. 13K followers. Button: Follow.



<https://twitter.com/needabadge>

https://www.linkedin.com/search/results/people/?keywords=cnn.com&origin=CLUSTER_EXPANSION

Google „Dorks“

<https://www.hackthebox.com/blog/What-Is-Google-Dorking>

```
# SECURITY WARNING: keep the secret key used in production secret!  
SECRET_KEY = 'efja(6f^2d+flw9=3!g4sy_&!qn&vdk5fb!2$2g0_i*-tqwt*%'
```

› configs ▾ Þýða þessa síðu

__init__.py	2020-09-02 07:10	0
__pycache__/	2022-01-14 14:15	-
arches.log	2022-05-03 12:19	1.7M
celery.py	2020-09-02 07:10	278
datatypes/	2020-09-02 07:10	-
functions/	2020-09-02 07:10	-
logs/	2022-01-18 12:02	-
management/	2020-09-02 07:10	-
media/	2020-09-02 08:43	-
package.json	2020-09-02 08:41	1.9K
search	2020-09-02 07:10	348
search_components/	2020-09-02 07:10	-
search_indexes/	2020-09-02 07:10	-
settings.py	2022-01-14 13:56	6.0K
settings_local.py	2020-09-02 07:10	70
static/	2020-09-02 08:43	-

```
DATABASES = {  
    "default": {  
        "ATOMIC_REQUESTS": False,  
        "AUTOCOMMIT": True,  
        "CONN_MAX_AGE": 0,  
        "ENGINE": "django.contrib.gis.db.backends.postgis",  
        "HOST": "localhost",  
        "NAME": "lincoln",  
        "OPTIONS": {},  
        "USER": "postgres",  
        "PASSWORD": "postgis",  
        "PORT": "5432", # Keep this inline with docker compose file.  
        "POSTGIS_TEMPLATE": "template1", # Current docker image uses template1  
        "TEST": {  
            "CHARSET": None,  
            "COLLATION": None,  
            "MIRROR": None,  
            "NAME": None  
        },  
        "TIME_ZONE": None  
    }  
}
```

intitle:index of settings.py

intext:"wordpress" filetype:xls login & password

https://[redacted].files.wordpress.com › 2014/07 ▾ XLS

Project Lists - WordPress.com

2, SNO, PROJECT NAME, DOMAIN NAME, TECHNOLOGY, USERNAME, PASSWORD. 3, 1,
[redacted], Wordpress, admin ...

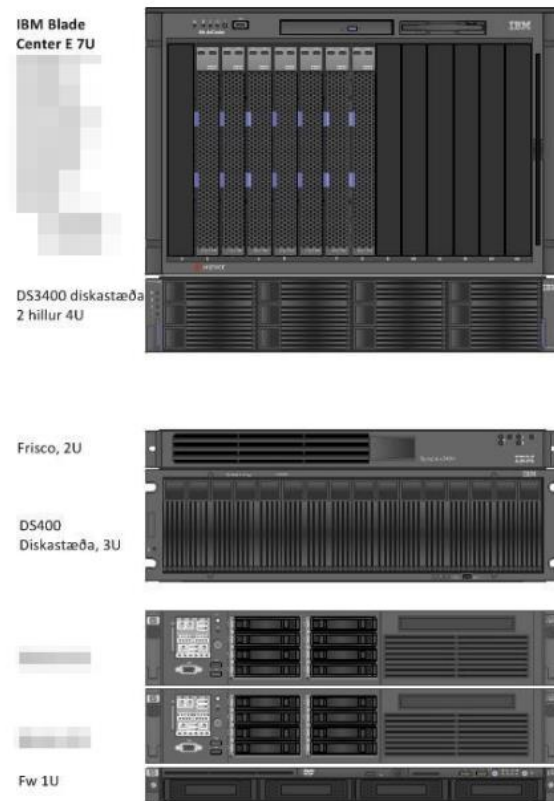
SNO	PROJECT NAME	DOMAIN NAME	TECHNOLOGY	USERNAME	PASSWORD
1	[redacted]	[redacted]	Wordpress	admin	[redacted]
2	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
3	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
4	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
5	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
6	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
7	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
8	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
9	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
10	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]
11	[redacted]	[redacted]	Wordpress	[redacted]	[redacted]

Útboðsgögn

4.2.2 Rekstur miðlægs tölvubúnaðar

Netstýrikerfi og netþjónar

Eftirfarandi netþjóna og diskastæður skal hýsa og reka.



Miðlægir netþjónar

Lénsstjórar (domain controllers)

- [redacted]c01 (primary), [redacted]Fs01, [redacted] (secondary).

Nafnþjónar (DNS; DHCP)

- [redacted]Dc01, [redacted]

Rekstrarþjónar (utility servers)

- Windows Update Server (WUS): [redacted]Dc01.
- Trend Office Scan: [redacted]Util01.
- Server Protect Server: [redacted]Util01.
- Desktop Authority Server: [redacted]Util01.
- Windows Deployment Services: [redacted].

Afritunarþjónar (backup servers)

- [redacted]Util01.

Skráarþjónar (file servers)

- [redacted]Fs01.

Prentþjónar (print servers)

- [redacted].

Tölvupósthús (mail servers)

- Exchange Server: [redacted]Exh01.
- Exchange Server fyrir OneSystems: [redacted].

Vefþjónar (web servers)

- IIS fyrir Gagnasjá: [redacted].

Skjáhermun (terminal server)

- [redacted]Term01.

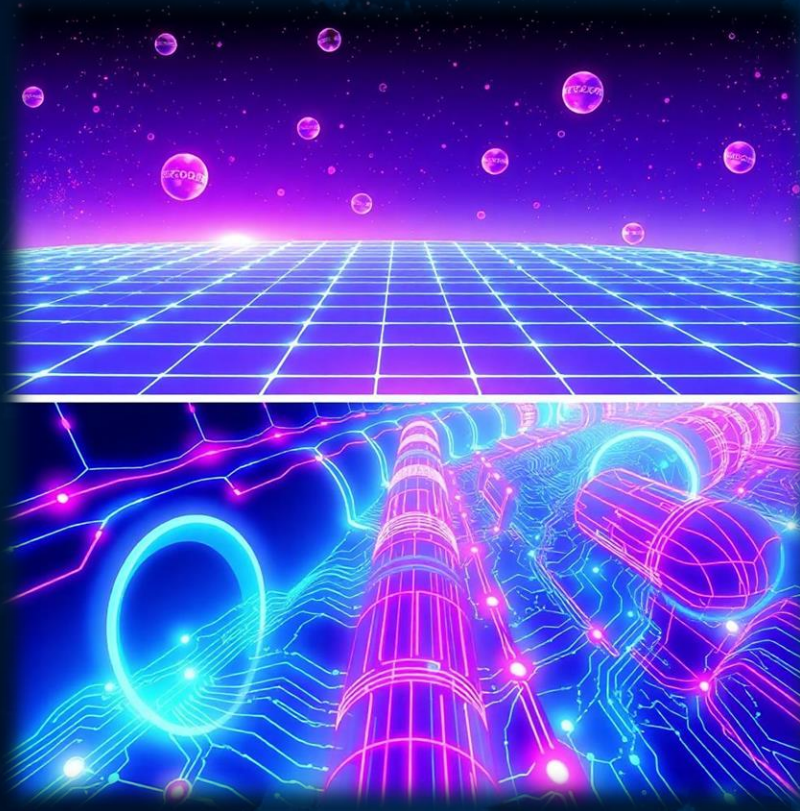
Sýndarþjónar (virtual servers)

- [redacted]Esx; keyrir m.a. [redacted] og [redacted].

Deep web Djúpvefurinn





85-95%
„private“




Greiningarskýrslur






Upplýsingar um starfsfólk

Wendy Brundige  Senior Vice President
wendy.brundige@cnn.com 



 100%


1 source ▾

Jamie Foster  Vice President of Tale
jamie.foster@cnn.com 



 100%


1 source ▾

Amanda Rottier  Senior Vice President
amanda.rottier@cnn.com 

 100%

1 source ▾

Ryan Kadro  Senior Vice President of Content Strategy
ryan.kadro@cnn.com 

 100%

1 source ▾

Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain. You are searching 34 billion records.

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [*.ru](#), [*.gov.uk](#), [solarwinds.com](#)

- Domains
- Email Addresses
- URLs

henrykoblavi@cocacola.com
scholars@cocacola.com
charlesfoster@cocacola.com
eudialogue@cocacola.com
rose@cocacola.com
victoria.gist@cocacola.com
cocacola2009@cocacola.com
midyearpromo@cocacola.com
kamwilliams@cocacola.com
joestrada@cocacola.com
julgarcia@cocacola.com
micrichardson@cocacola.com
fechols@cocacola.com
bwindham@cocacola.com

<https://phonebook.cz/>

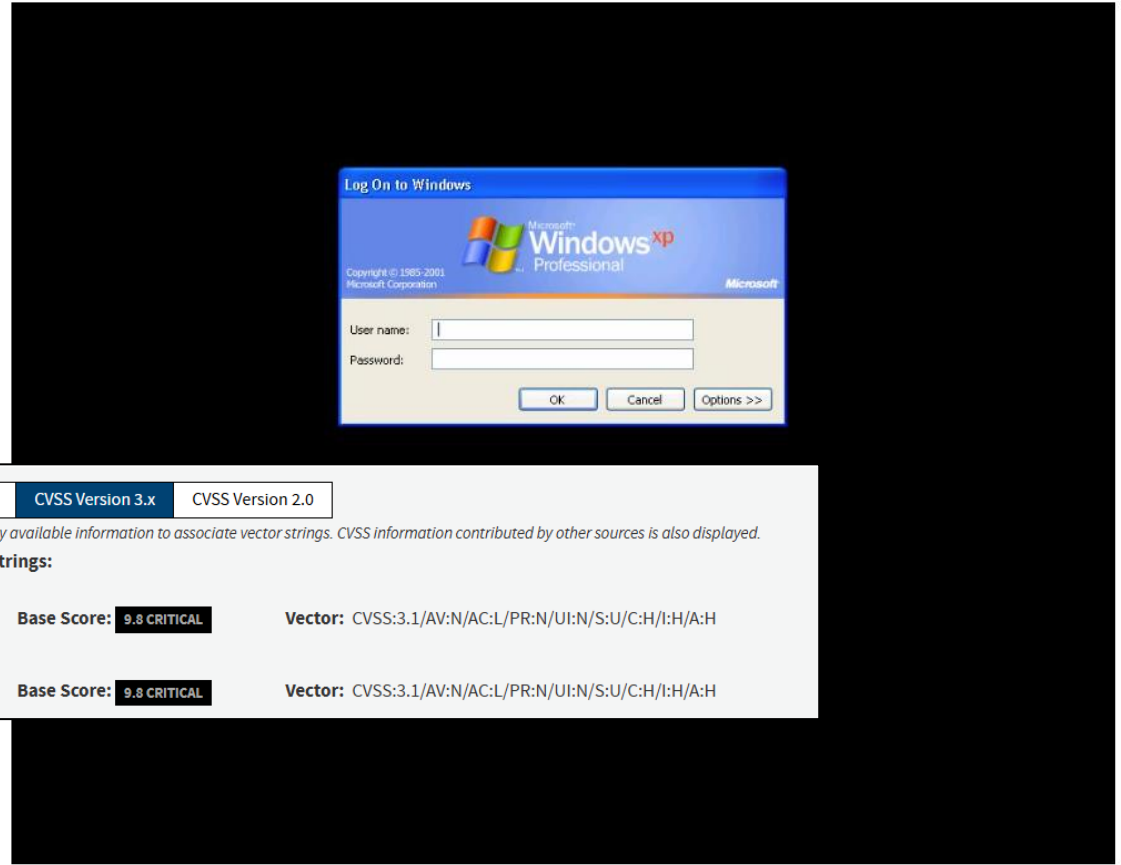
<https://hunter.io/search/cnn.com>

Vulnerabilities

CVE-2019-0708

Remote Desktop Protocol
\\x03\\x00\\x00\\x0b\\x06\\xd0\\x00\\x00\\x124\\x00

Log On to Windows
User name:
Password:
Cancel options



Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

ADP: CISA-ADP

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H




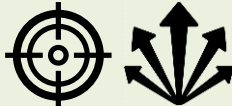
Darkweb á Deepweb

🔍 Top Dark-Web & Breach-Monitoring Services (Legitimate Sources)			
Service	Focus	Access Model	Notes
Have I Been Pwned (HIBP)	Public database of breached email addresses and domains.	Free (with API for orgs)	Maintained by Troy Hunt; trusted, non-commercial OSINT source for breach exposure checks.
SpyCloud	Compromised credentials, botnet data, and account takeover prevention.	Commercial	Provides enterprise feeds and password-reuse intelligence.
Constella Intelligence (former 4iQ)	Dark-web breach data, personal data exposure monitoring.	Commercial	Aggregates massive historical breach datasets for identity protection.
DarkOwl Vision	Crawls Tor, I2P, and other hidden services for exposed data and chatter.	Commercial	Leading dark-web search platform used by CTI analysts; provides API access.
Recorded Future	Threat intelligence platform with dark-web, surface, and technical sources.	Commercial	Integrates with SIEM/TIP tools and provides leak alerts & actor tracking.
SOCRadar	Dark-web monitoring, credential leaks, phishing domain detection.	Freemium	Offers "ThreatHose" portal with limited free breach & dark-web results.
Flare.io	Dark-web and clear-web monitoring for corporate leaks, fraud, and brand mentions.	Commercial	Focus on continuous monitoring and takedown workflows.
Hudson Rock (Cavalier)	Database of credentials & malware logs from infected devices.	Commercial / vetted access	Specializes in "Infostealer" logs; used for threat actor tracking.
KELA	Cyber-crime intelligence with dark-web marketplace coverage.	Commercial	Focused on access brokers, ransomware groups, and underground economy.




* Svar ChatGPT birt án ábyrgðar





 Velja skotmarkið 

OSINT

Fyrsti aðgangur

Innskráning
“credentials stuffing”
“password spraying”

Misnota veikleika
Handvirkar aðgerðir
Árásatól

Lekagögn
„Initial Access Brokers“

Spjallborð hakkara
Markaðstorg á darkweb



Reconnaissance 10 techniques		Resource Development 8 techniques		Initial Access 11 techniques	
Active Scanning (0/3)		Acquire Access		Content Injection	
Gather Victim Host Information (4/4)	Client Configurations	Acquire Infrastructure (0/6)		Drive-by Compromise	
	Firmware	Compromise Accounts (0/3)		Exploit Public-Facing Application	
	Hardware	Compromise Infrastructure (0/6)		External Remote Services	
Gather Victim Identity Information (3/3)	Software			Hardware Additions	
	Credentials		Code Signing Certificates	Phishing (0/4)	
	Email Addresses		Digital Certificates	Replication Through Removable Media	
Gather Victim Network Information (5/6)	Employee Names	Develop Capabilities (1/4)	Exploits	Supply Chain Compromise (0/3)	
	DNS		Malware	Trusted Relationship	
	Domain Properties		Cloud Accounts		Cloud Accounts
	IP Addresses	Establish Accounts (3/3)	Email Accounts	Valid Accounts (4/4)	Default Accounts
Gather Victim Org Information (3/4)	Network Security Appliances		Social Media Accounts	Domain Accounts	
	Network Topology		Artificial Intelligence	Local Accounts	
	Network Trust Dependencies		Code Signing Certificates		
Phishing for Information (0/4)	Business Relationships	Obtain Capabilities (4/7)	Digital Certificates	Wi-Fi Networks	
	Determine Physical Locations		Exploits		
	Identify Business Tempo		Malware		
Search Closed Sources (0/2)	Identify Roles		Tool		
			Vulnerabilities		
Search Open Technical Databases (4/5)	CDNs	Stage Capabilities (0/6)			
	Digital Certificates				
	DNS/Passive DNS				
	Scan Databases				
Search Open Websites/Domains (3/3)	WHOIS				
	Code Repositories				
	Search Engines				
Search Victim-Owned Websites	Social Media				

<https://mitre-attack.github.io/attack-navigator/>

<https://attack.mitre.org/>

Lazarus group

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/3)	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (1/4)	Account Discovery (1/4)	Exploitation of Remote Services	Adversary-in-the-Middle (1/4)	Application Layer Protocol (1/5)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (3/8)	Drive-by Compromise	Command and Scripting Interpreter (3/12)	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Brute Force (1/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3/3)	Communication Through Removable Media	Data Transfer Size Limits (0/3)	Data Destruction (0/3)
Gather Victim Identity Information (1/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (2/14)	Account Manipulation (0/3)	Build Image on Host	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (1/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (2/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/3)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (1/2)	Defacement (1/2)	Data Manipulation (0/3)
Gather Victim Org Information (1/4)	Develop Capabilities (2/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution (2/14)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (3/8)	Browser Session Hijacking	Data Obfuscation (1/3)	Exfiltration Over C2 Channel (1/3)	Disk Wipe (2/2)
Phishing for Information (0/4)	Establish Accounts (2/3)	Phishing (3/4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Email Bombing
Search Closed Sources (0/2)	Obtain Capabilities (3/7)	Replication Through Removable Media	Input Injection	Create Account (0/3)	Event Triggered Execution (0/17)	Domain or Tenant Policy Modification (0/2)	Input Capture (1/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (1/2)	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (2/6)	Supply Chain Compromise (0/3)	Inter-Process Communication (0/3)	Create or Modify System Process (1/5)	Create or Modify System Process (1/5)	Email Spoofing	Modify Authentication Process (0/9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (1/4)	Financial Theft
Search Open Websites/Domains (1/3)		Trusted Relationship	Native API	Event Triggered Execution (0/17)	Domain or Tenant Policy Modification (0/2)	Execution Guardrails (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/5)	Hide Infrastructure	Exfiltration Over Web Service (1/4)	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts	Scheduled Task/Job (1/5)	Exclusive Control	Escape to Host	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Ingress Tool Transfer	Inhibit System Recovery	Network Denial of Service (0/2)
		Wi-Fi Networks	Serverless Execution	External Remote Services	Event Triggered Execution (0/17)	Hide Artifacts (1/14)	Network Sniffing	Group Policy Discovery		Data from Network Shared Drive	Multi-Stage Channels	Resource Hijacking (0/4)	Service Stop
			Shared Modules	Hijack Execution Flow (2/12)	Exploitation for Privilege Escalation	Hijack Execution Flow (2/12)	OS Credential Dumping (0/6)	Log Enumeration		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	System Shutdown/Reboot
			Software Deployment Tools	Implant Internal Image	Hijack Authentication Process (0/9)	Impair Defenses (2/11)	Steal Application Access Token	Network Service Discovery		Data from Staged (1/2)	Non-Standard Port	Transfer Data to Cloud Account	
			System Services (0/3)	Modify Authentication Process (0/9)	Process Injection (1/12)	Indicator Removal (3/10)	Steal or Forge Kerberos Tickets (0/5)	Network Share Discovery		Email Collection (0/3)	Protocol Tunneling		
			User Execution (2/4)	Modify Registry	Scheduled Task/Job (1/5)	Indirect Command Execution	Steal Web Session Cookie	Network Sniffing		Input Capture (1/4)	Proxy (2/4)		
			Windows Management Instrumentation	Office Application Startup (0/6)	Valid Accounts (0/3)	Masquerading (4/11)	Unsecured Credentials (0/8)	Password Policy Discovery		Screen Capture	Remote Access Tools (0/3)		
				Power Settings	Modify Registry	Modify Authentication Process (0/9)	Modify Cloud Compute Infrastructure (0/5)	Peripheral Device Discovery		Video Capture	Traffic Signaling (0/2)		
				Pre-OS Boot (1/5)	Scheduled Task/Job (1/5)	Masquerading (4/11)	Modify Cloud Resource Hierarchy	Permission Groups Discovery (0/3)			Web Service (1/3)		
				Scheduled Task/Job (1/5)	Valid Accounts (0/3)	Modify Authentication Process (0/9)	Modify Registry	Process Discovery					
				Server Software	Modify System Image (0/2)	Modify Cloud Compute Infrastructure (0/5)	Modify System Image (0/2)	Query Registry					
						Modify Cloud Resource Hierarchy		Remote System Discovery					
						Modify Registry		Software Discovery (0/1)					
						Modify System Image (0/2)		System Information Discovery					

<https://mitre-attack.github.io/attack-navigator/>



Beitum OSINT til að



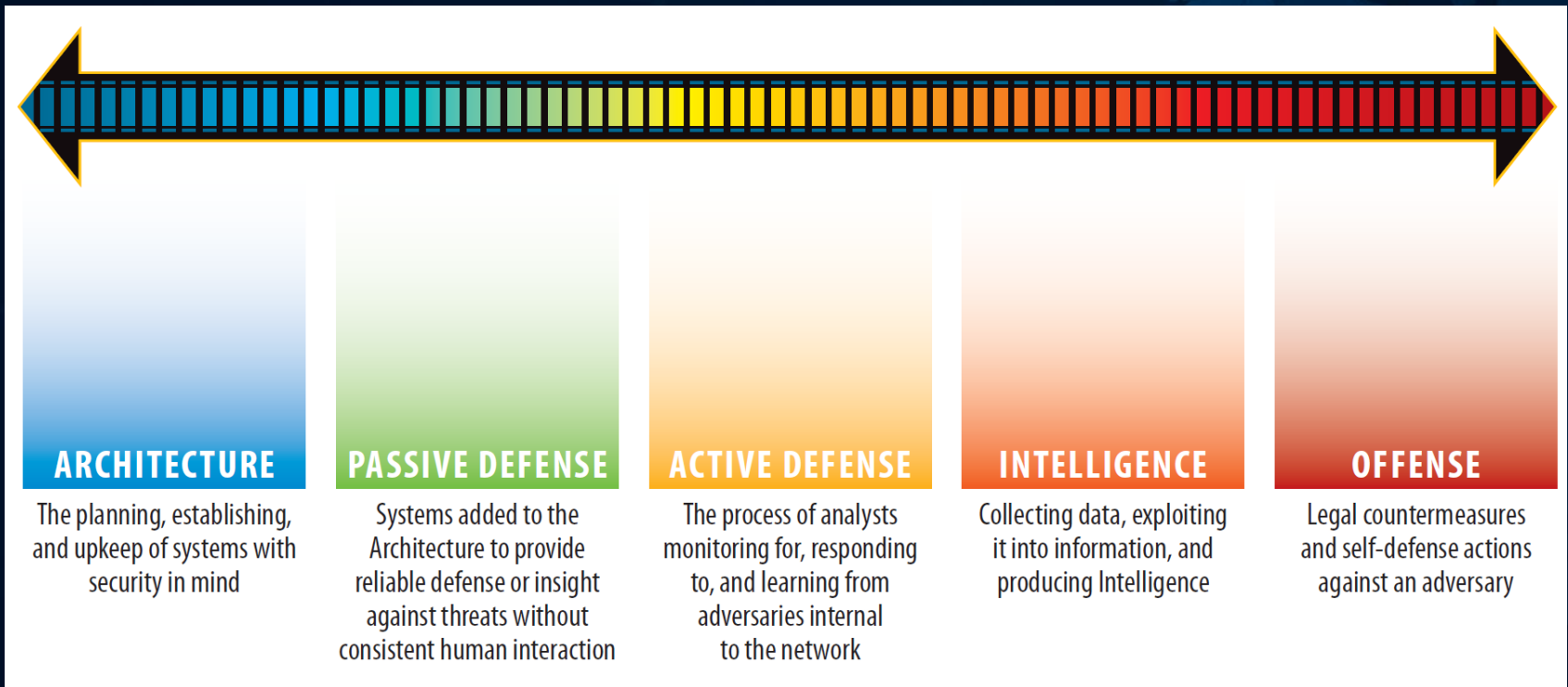
Meta hvernig andstæðingurinn sér okkur

Bregðast við og lágmarka ógnir

Rýna mikilvæga birgja

Endurbæta varnir og ferla

Forgangsröðun

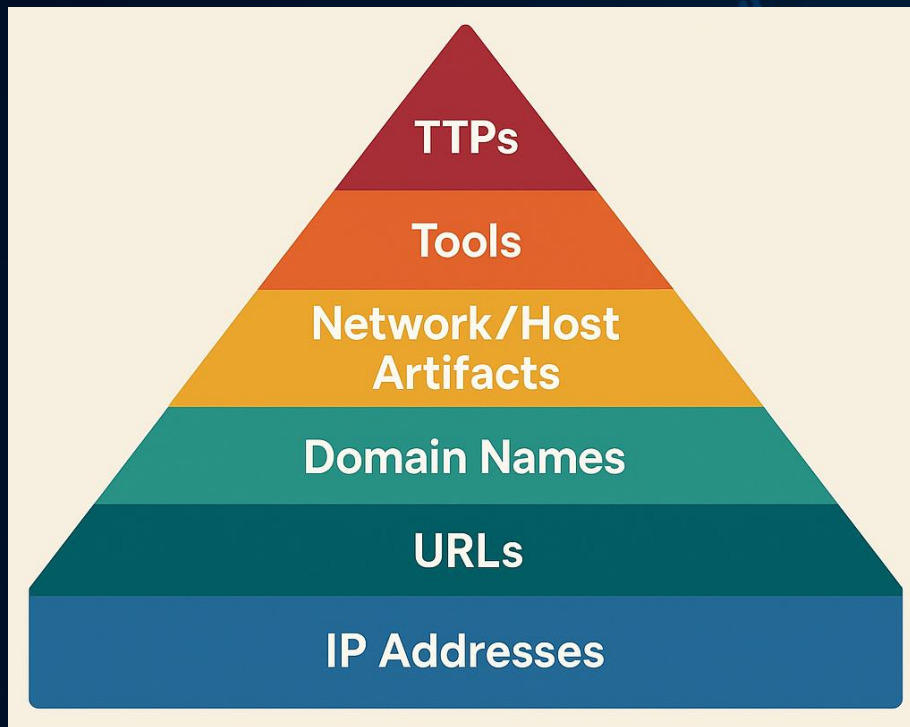


Opnar skýrslur og „feed“
Árásarflöturinn okkar

Meiri fjárfesting í greiningargetu
Virki leit á „darkweb“

The Sliding Scale of Cyber Security, Robert M. Lee, 2015

Pyramid-of-Pain



Þróað áhættu- og ástandsmat.
Langtíma spá um hegðun árársaraðila

Einfaldir blokklistar og grundvallar ástandsmat.
Skammtíma IoC.

<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>



kristjan.valur.jonsson@sedlabanki.is

<https://www.linkedin.com/in/kristjanvj/>