

Sistem de alertă timpurie și informare în timp real - RO-SAT

- prezentarea tehnică a proiectului -

Dumitru DAVID

Şef Serviciu Administrare și Dezvoltare Infrastructură

AGENDA

- Obiective proiect
- Arhitectura funcțională a sistemului
- Surse principale de date
- Module platformă RO-SAT sistem: Darknet, HoneyNet, **Senzor SOC**, Scanner vulnerabilități, Crawling website-uri, OSINT, Cyber Threat Intelligence, Colectare, normalizare și îmbogățire, Big Data Security Analytics, Diseminare date - (API)
- Întrebări

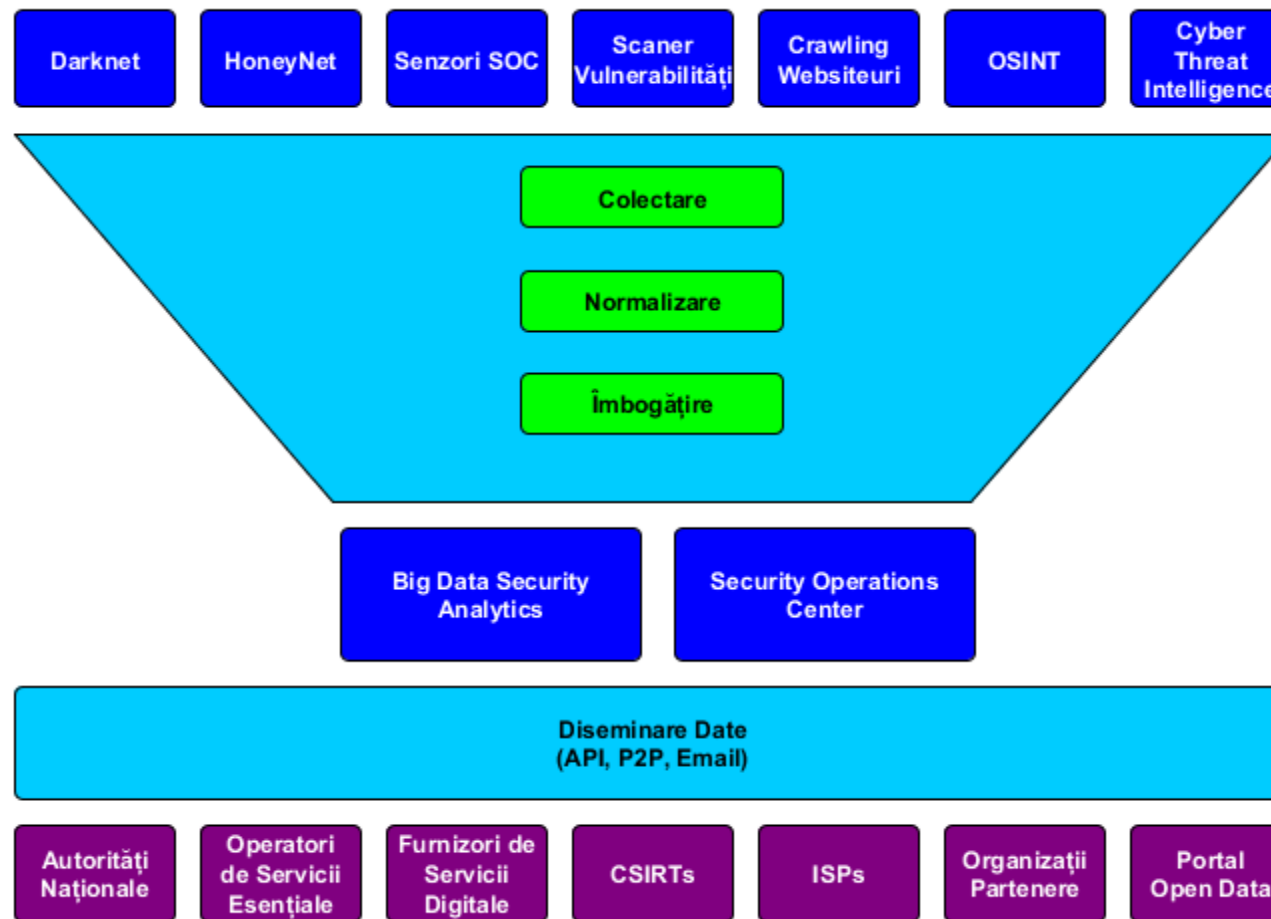
Obiectiv general

Creșterea capacității operaționale a CERT-RO în vederea asigurării capabilităților naționale de prevenire, identificare, analiză și reacție la incidentele de securitate cibernetică

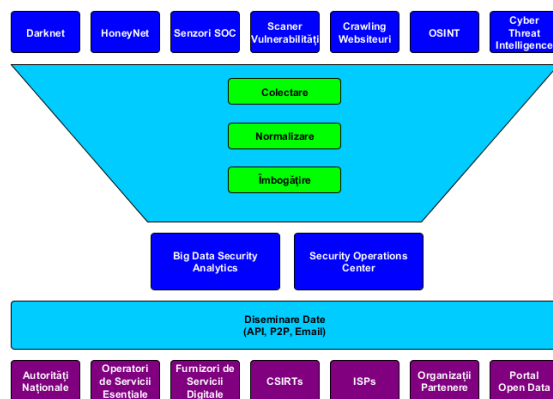
Obiective specifice

1. Dezvoltarea unui sistem național de avertizare în timp real a persoanelor fizice și/sau juridice vizate de atacuri cibernetice și/sau afectate de incidente cibernetice, precum și pentru informarea și cooperarea cu autoritățile competente;
2. Amplasarea unor sisteme de tip senzor SOC (Security Operation Center) de monitorizare în timp real a rețelelor din locațiile beneficiarilor: Poșta Română, Loteria Română și Autoritatea Electorală Permanentă, rețele distribuite la nivel național;
3. Realizarea unui număr de cel puțin 120 audituri de securitate pentru rețelele din locațiile beneficiarilor în care vor fi amplasate echipamente;
4. Instruirea unui număr de 20 specialiști. Domeniile de interes sunt: procesarea alertelor generate de terminalele SOC, managementul terminalelor SOC, managementul sistemului de alertă timpurie și informare în timp real, intervenția rapidă în caz de atac cibernetic, investigarea atacurilor cibernetice, ethical hacking etc;
5. Operaționalizarea a patru echipe de intervenție on-site în vederea derulării investigațiilor în cazul incidentelor de Securitate cibernetică.

Arhitectura funcțională a sistemului



Arhitectura funcțională a sistemului



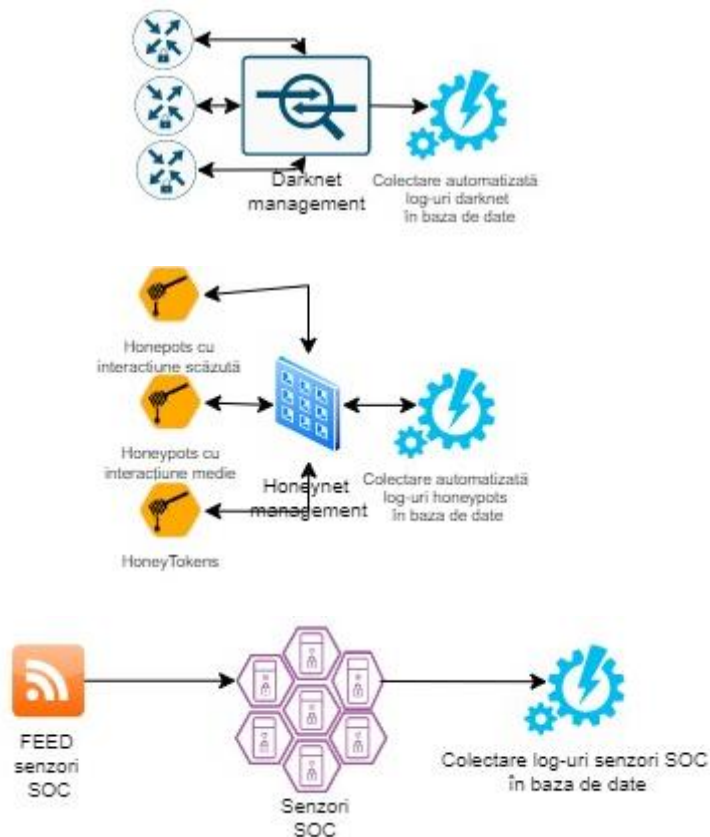
RO-SAT reprezintă un sistem integrat, modern, robust, scalabil, capabil să asigure preluarea, procesarea și transmiterea unui număr foarte mare de alerte de securitate cibernetică, din surse diferite, alerte ce vizează organizații publice sau private din spațiul cibernetic național.

RO-SAT va fi accesibil utilizatorilor prin intermediul unei interfețe WEB intuitive, ce va oferi posibilitatea administrării sistemului și realizării majorității funcționalităților sistemului.

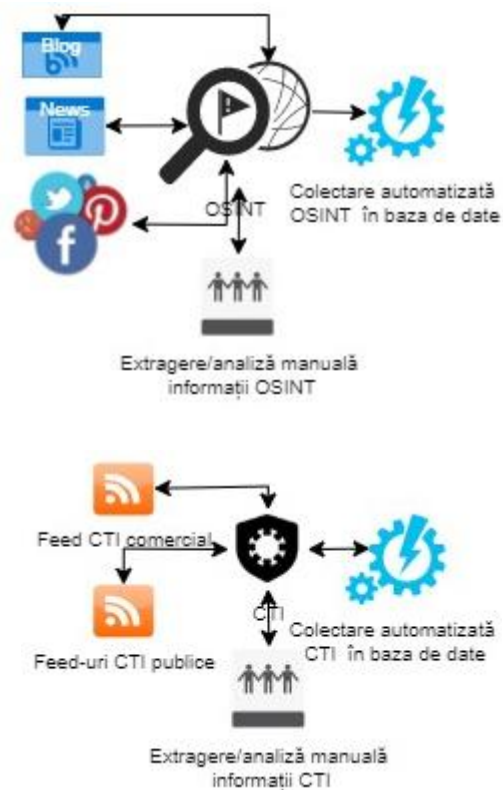
RO-SAT va funcționa ca un sistem integrat, modular, flexibil și scalabil, format din diverse module și sub-module, ce vor îndeplini numeroase funcții. Modularitatea și flexibilitatea vor oferi posibilitatea dezvoltării ulterioare de funcționalități suplimentare, care să poată apela cu ușurință modulele deja dezvoltate.

Proiectul vizează asigurarea interoperabilității RO-SAT cu alte sisteme informatice, beneficiare directe ale datelor din RO-SAT, respectiv organizații afectate sau posibil afectate în cadrul atacurilor cibernetice raportate la CERT-RO, cărora să le poată fi transmise toate datele necesare, în timp util și într-un format standardizat, în vederea luării tuturor măsurilor ce se impun pentru reducerea efectelor incidentelor.

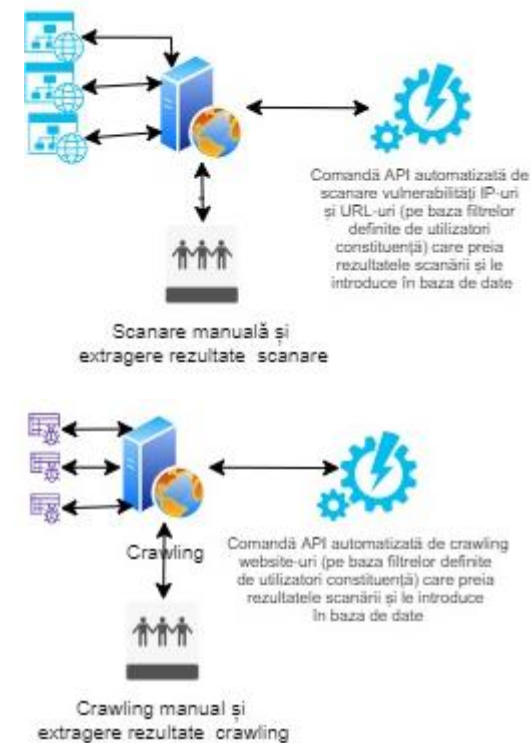
Surse principale de date



TRAFIC REȚEA/INTERNET (log-uri Darknet, HonetNet, senzori SOC)



Informații din surse publice și comerciale (cyber threat intelligence + OSINT)



SCANARE VULNERABILITĂȚI + CRAWLING

Modulul “Darknet”

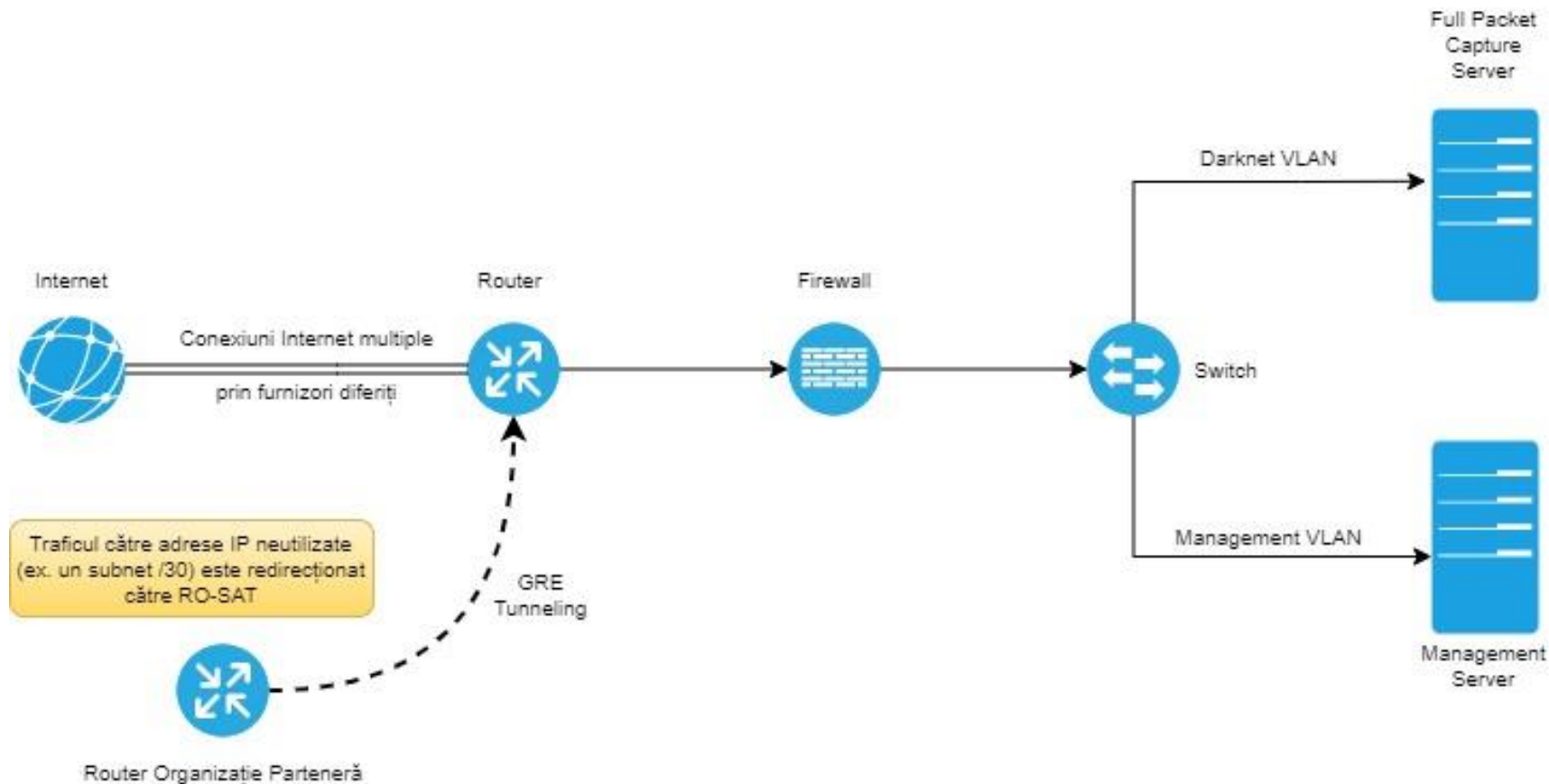
În contextul proiectului RO-SAT, DARKNET va fi reprezentat de o platformă prin care se va putea observa și studia trafic de rețea ce reprezintă conexiuni către adrese IP neasignate vreunui sistem informatic. Acest tip de trafic este prin definiție malițios, reprezentând adesea scanări în masă ale spațiului de adrese IP pentru identificarea de sisteme vulnerabile.

Modulul Darknet este un mecanism software de monitorizare a unui spațiu continuu de adrese IP nealocate unui echipament, astfel încât aceste adrese nu pot genera trafic iar traficul care ajunge la aceste adrese este considerat ca fiind trafic ofensiv (scanări malware, scanări premergătoare atacurilor, mass scan după anumite vulnerabilități, etc.).

Cu cât spațiul de adrese este mai mare, cu atât datele provenite din darknet vor fi mai relevante din punctul de vedere al monitorizării strategiilor, tacticilor și tehnicilor atacatorilor, putând evidenția de exemplu, noi campanii de exploatare a unor vulnerabilități sau care sunt serviciile și tipurile de atacuri folosite de atacatori, și ajutând la clasificarea acestora prin corelarea informațiilor obținute.

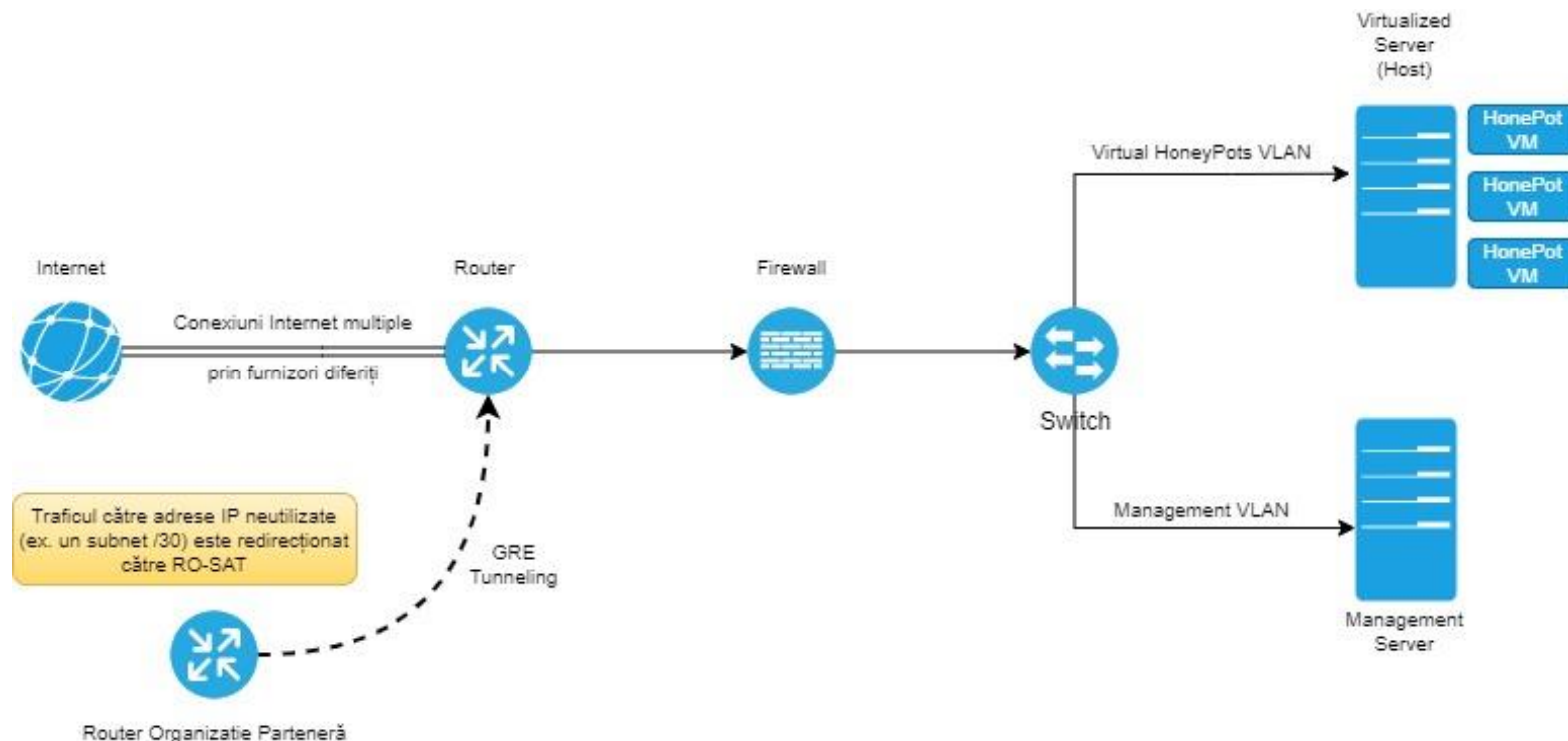
Modulul “Darknet”

Vor fi monitorizate spațiile de adrese IP neutilizate ale CERT-RO și ale partenerilor sau beneficiarilor proiectului. Acest lucru se va realiza prin configurarea routerelor astfel încât să direcționeze către RO-SAT tot traficul de date destinat unor adrese IP nealocate.



Modulul “HoneyNet”

Modulul HoneyNet va consta într-o rețea de senzori de tip HoneyPot – sisteme informatice vulnerabile expuse intenționat atacurilor în vederea analizării tehnicilor și uneltelor de exploatare utilizate de atacatori. Modulul Honeynet va emula echipamente de rețea, servere, servicii de email și file sharing, stații de lucru (diferite sisteme de operare), echipamente industriale, dispozitive IoT, sisteme de control industrial (ICS/SCADA) dar și alte tipuri de echipamente considerate de interes pentru atacatori



Modulul “Senzor SOC”

În cadrul proiectului se va dezvolta un senzor ce va fi pus la dispoziția tuturor entităților care vor dori să-l folosească.

Acest senzor va fi capabil să inspecteze traficul de rețea și să identifice amenințări de securitate cibernetică, comportamente malițioase, violarea unor politici (funcționalități echivalente unui IDS - Intrusion Detection System) și să genereze o alertă la identificarea acestora.

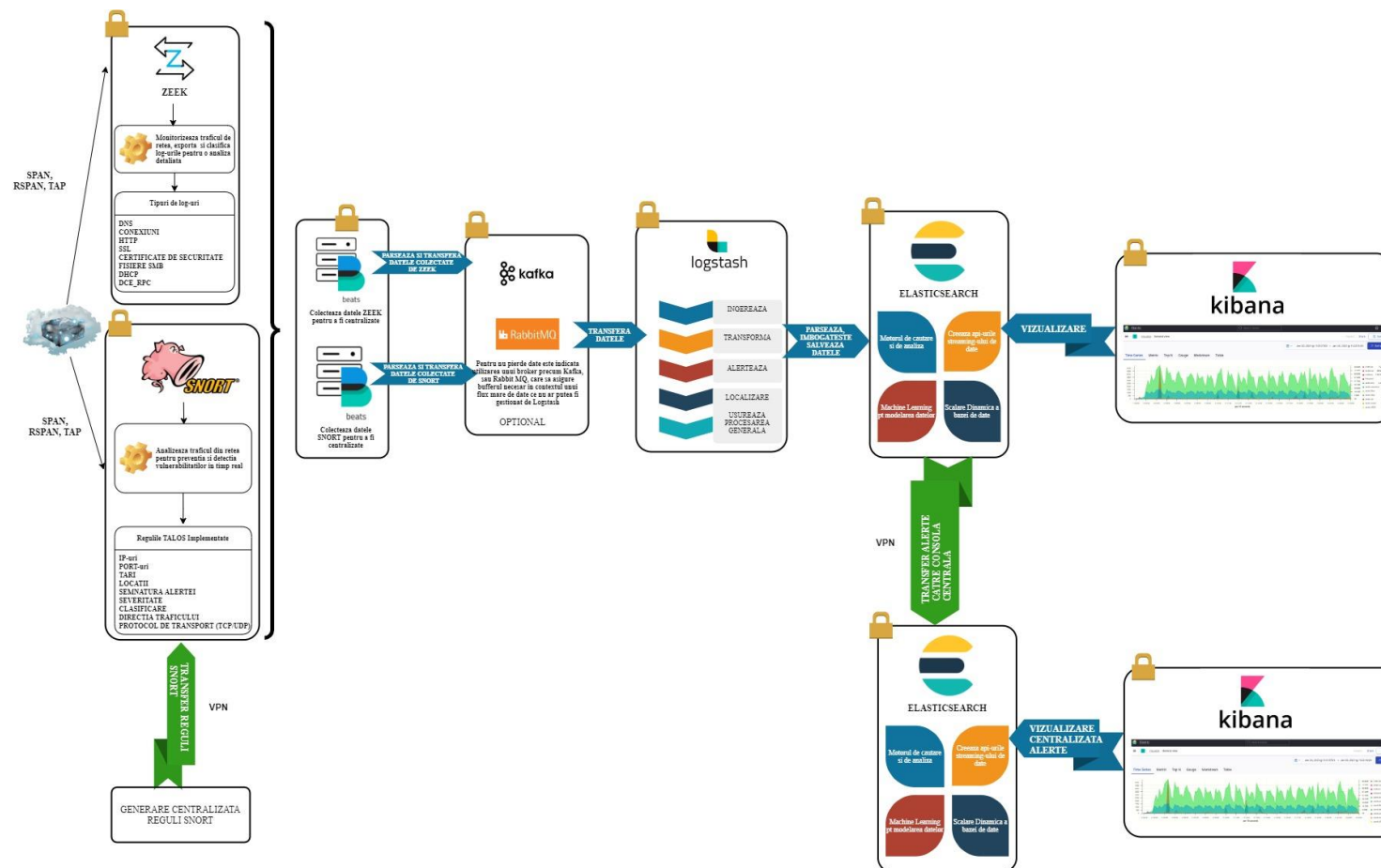
De asemenea, senzorul va fi capabil să realizeze capturi de trafic, care vor fi analizate ulterior în vederea identificării activităților cu caracter malițios.

Această componentă va avea următoarele caracteristici generale:

- Permite colectarea traficului în regim “full packet capture”
- Colectarea traficului se face în regim round-robin (traficul colectat este salvat în limita spațiului disponibil, datele cele mai vechi fiind suprascrise)
- Oferă o interfață web care permite explorarea traficului PCAP colectat
- Oferă instrumente de indexare, regăsire și export a traficului colectat
- Permite extragerea de fișiere (file carving)

O altă funcționalitate ce va fi asigurată de senzor este integrarea log-urilor de la alte echipamente din cadrul infrastructurii și posibilitatea de corelare a acestora.

Modulul “Senzor SOC”



Modulul “Senzor SOC” - ZEEK

ZEEK este un framework de analiză a traficului de rețea. Cu ajutorul acestui framework în cadrul senzorului SOC va fi analizat în timp real traficul de rețea primit prin intermediul unei conexiuni de tip mirror/SPAN.

Zeek creează o varietate de log-uri. Acestea sunt stocate în fișiere ce au nume ce permit identificarea rapidă a tipului de informație conținut. Primul beneficiu obținut este setul extins de log-uri ce cuprind nu numai informații privind fiecare conexiune observată ci și informații la nivel de layer de aplicație. Acestea includ de exemplu toate sesiunile HTTP cu URI-urile solicitate, cereri DNS și răspunsurile primite la acestea, certificate SSL, informații privind sesiunile SMTP etc

Modulul “Senzor SOC” - ZEEK

Zeek a fost ales pentru că permite înțelegerea mai bună a modului în care o infrastructură de rețea este utilizată și oferă un instrument ce permite detectarea facilă a unor activități malițioase.

- conn.log
- dns.log
- http.log
- files.log
- ftp.log
- ssl.log
- x509.log
- smtp.log
- ssh.log
- pe.log
- dhcp.log
- ntp.log
- SMB Logs (plus DCE-RPC, Kerberos, NTLM)
- irc.log
- rdp.log
- traceroute.log
- tunnel.log
- dpd.log
- known_*.log and software.log
- weird.log and notice.log
- capture_loss.log and reporter.log

Modulul “Senzor SOC” – ZEEK – use case DNS

DNS rămâne una dintre cele mai eficiente metode de detectare a activităților malițioase dintr-o rețea. Fișierul dns.log va surprinde aproape tot ceea ce dorim să aflăm despre o interogare DNS și despre răspunsul la aceasta, ceea ce înseamnă că vom putea identifica un site malițios chiar dacă acesta utilizează HTTPS prin combinarea informațiilor conținute de dns.log cu informațiile conținute în ssl.log și x509.log. De aceea un administratorii de rețea și inginerii de securitate vor începe adesea o investigație prin analiza înregistrărilor conținute în dns.log.

Modulul “Senzor SOC” – ZEEK – use case DNS

Câmpurile de la care poate fi pornită o analiză sunt:

- A. UID oferă un index/cheie ce permite efectuarea unei analize corelate prin utilizarea informațiilor ce se regăsesc în celelalte fișiere cu log-uri generate de ZEEK (de ex. conn.log)
- B. Cererea DNS emisă de un client DNS
- C. Răspunsul (răspunsurile) date de către server-ul DNS
- D. Durata de timp pentru care serverul DNS își instruiește clienții să păstreze valoarea (cache)

dns.log | DNS query/response details

	FIELD	TYPE	DESCRIPTION
	ts	time	Earliest timestamp of DNS protocol message
A	uid & id		Underlying connection info > See conn.log
	proto	enum	Transport layer protocol of connection
	trans_id	count	16-bit identifier assigned by program that generated DNS query
	rtt	interval	Round trip time for query and response
B	query	string	Domain name subject of DNS query
	qclass	count	QCLASS value specifying query class
	qclass_name	string	Descriptive name for query class
	qtype	count	QTYPE value specifying query type
	qtype_name	string	Descriptive name for query type
	rcode	count	Response code value in DNS response
	rcode_name	string	Descriptive name of response code value
	AA	bool	Authoritative Answer bit: responding name server is authority for domain name
	TC	bool	Truncation bit: message was truncated
	RD	bool	Recursion Desired bit: client wants recursive service for query
	RA	bool	Recursion Available bit: name server supports recursive queries
	Z	count	Reserved field, usually zero in queries and responses
C	answers	vector	Set of resource descriptions in query answer
D	TTLs	vector	Caching intervals of RRs in answers field
	rejected	bool	DNS query was rejected by server
	auth	table	Authoritative responses for query
	addl	table	Additional responses for query

Modulul “Senzor SOC” – ZEEK – use case DNS

Ce informații pot ridica semne de întrebare ?

➤ Cereri DNS de dimensiuni mari

O cerere DNS care se abate de la dimensiunile standard ar putea fi un indicator al unui atac de tip DNS tunneling sau al unei exfiltrări de date. În principiu orice cerere DNS cu o dimensiune mai mare de 75 de caractere ar putea fi un indicator al unei activități malițioase și ar trebui investigată

➤ Răspunsuri de dimensiuni mari la cererile DNS

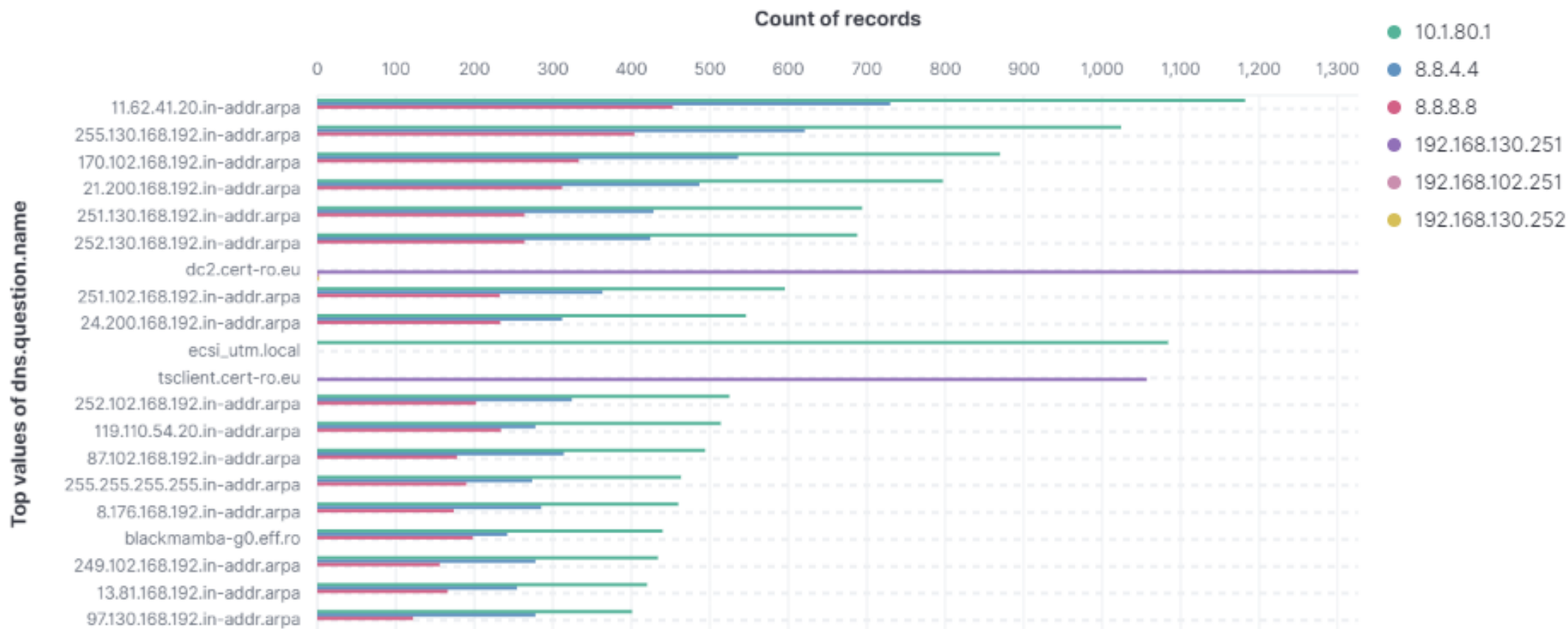
Informațiile de acest tip ar putea fi utilizate pentru a identifica serverele interne DNS care sunt configurate greșit și pot fi utilizate ca open-relay în cadrul unui atac de tip DNS amplification. În principiu orice răspuns cu dimensiuni mai mari de 475 de caractere ar putea fi un indicator

➤ Cereri DNS ce primesc NXDOMAIN ca răspuns

NXDOMAIN este răspunsul standard pentru un domeniu care nu există sau care nu poate fi rezolvat de serverul DNS care a primit cererea. Un număr mare de răspunsuri de tip NXDOMAIN poate indica un server DNS configurat greșit, sau poate indica un malware care încearcă să rezolve un domeniu care nu mai este activ. Un răspuns de tip NXDOMAIN poate fi de asemenea o dovadă a unei posibile exfiltrări de date

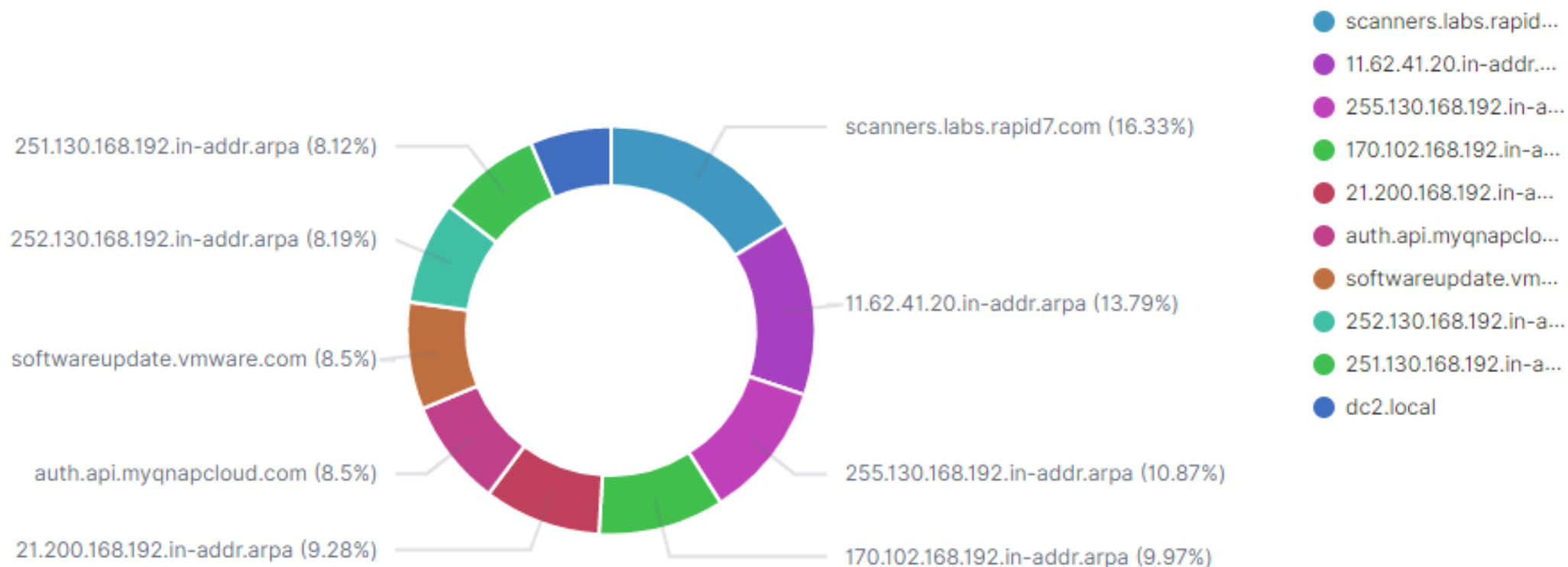
Modulul “Senzor SOC” – ZEEK – use case DNS

Top 10 DNS NXDOMAIN split by dns.question.name



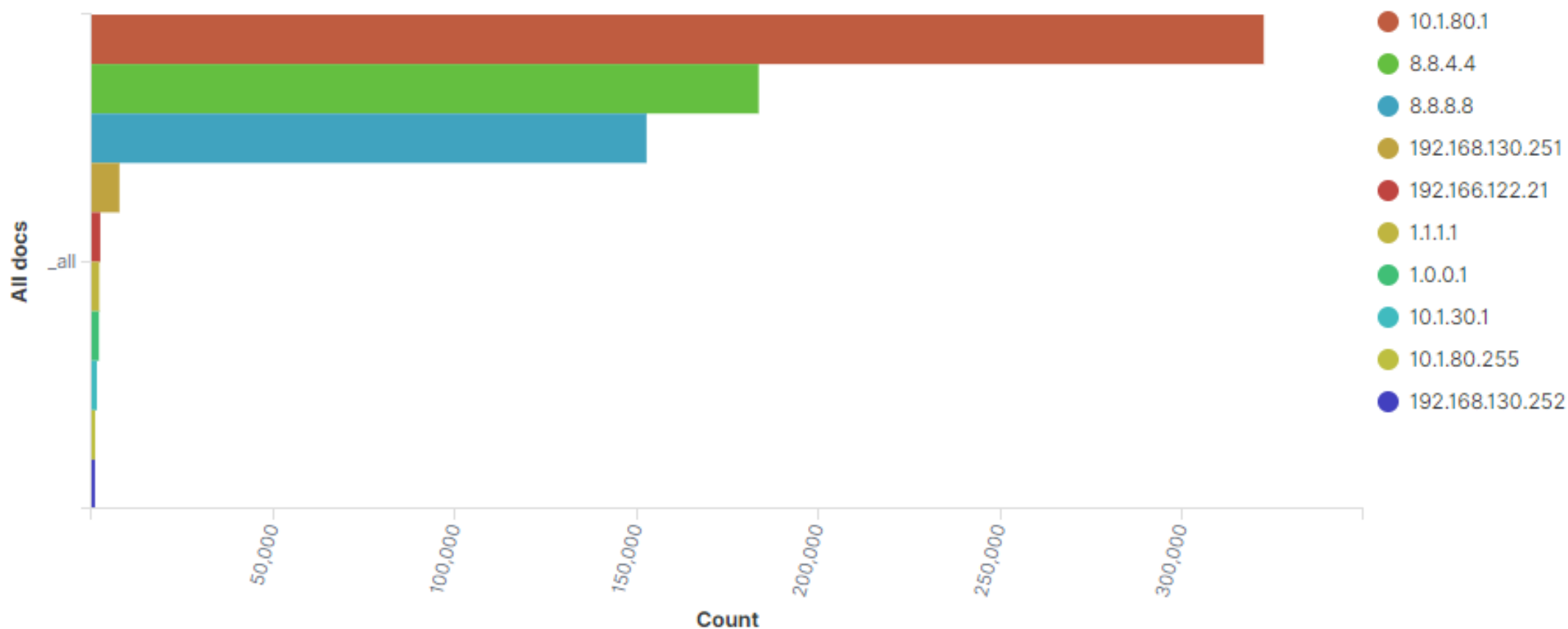
Modulul “Senzor SOC” – ZEEK – use case DNS

Top DNS Domains [Filebeat Zeek]



Modulul “Senzor SOC” – ZEEK – use case DNS

TOP10 Responding servers



Modulul “Senzor SOC” – ZEEK – use case HTTP

Fișierul http.log conține un rezumat al tranzacțiilor HTTP. Acest jurnal poate fi extins cu ușurință pentru a colecta detalii HTTP suplimentare. Administratorii de rețea și inginerii de securitate pot utiliza informațiile http.log pentru a înțelege activitatea HTTP din rețea, pentru a depana probleme de rețea sau pentru a căuta activități anormale.

Câmpurile de la care poate fi pornită o analiză sunt:

A. Timestamp

B. UID oferă un index/cheie ce permite efectuarea unei analize corelate prin utilizarea informațiilor ce se regăsesc în celelalte fișiere cu log-uri generate de ZEEK (de ex. conn.log, dns.log)

C. Method (GET, POST, etc), host header, URI utilizat pentru request

D. User Agent

http.log | HTTP request/reply details

	FIELD	TYPE	DESCRIPTION
A	ts	time	Timestamp for when request happened
B	uid & id		Underlying connection info > See conn.log
	trans_depth	count	Pipelined depth into connection
	method	string	Verb used in HTTP request (GET, POST, etc.)
	host	string	Value of HOST header
C	uri	string	URI used in request
	referrer	string	Value of "referrer" header
	version	string	Value of version portion of request
D	user_agent	string	Value of User-Agent header from client
	request_body_len	count	Uncompressed data size from client
	response_body_len	count	Uncompressed data size from server
	status_code	count	Status code returned by server
	status_msg	string	Status message returned by server
	info_code	count	Last seen 1xx info reply code from server
	info_msg	string	Last seen 1xx info reply message from server
	tags	table	Indicators of various attributes discovered
	username	string	Username if basic-auth is performed
	password	string	Password if basic-auth is performed
	proxied	table	Headers indicative of a proxied request
	orig_fuids	vector	Ordered vector of file unique IDs
	orig_filenames	vector	Ordered vector of filenames from client
	orig_mime_types	vector	Ordered vector of mime types
	resp_fuids	vector	Ordered vector of file unique IDs
	resp_filenames	vector	Ordered vector of filenames from server
	resp_mime_types	vector	Ordered vector of mime types
	client_header_names	vector	Vector of HTTP header names sent by client
	server_header_names	vector	Vector of HTTP header names sent by server
	cookie_vars	vector	Variable names extracted from all cookies
	uri_vars	vector	Variable names extracted from URI

Modulul “Senzor SOC” – ZEEK – use case HTTP

Ce informații pot ridica semne de întrebare ?

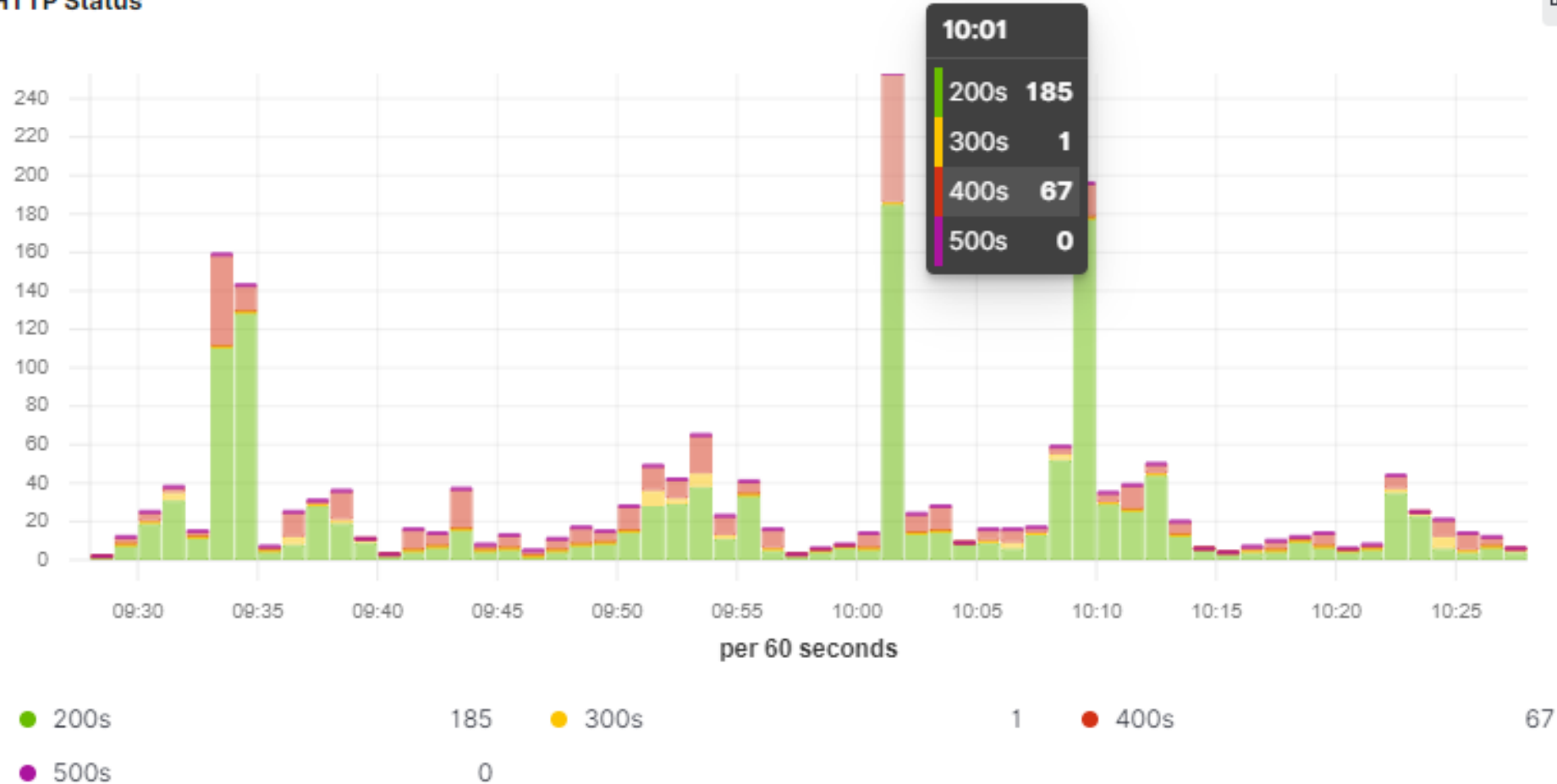
- Trafic HTTP sau DNS care rulează pe porturi non-standard
- Volum mare al codurilor de răspuns HTTP din categoria 400 – erori client și 500 – erori server

O creștere a codurilor din seria 400 ar putea indica activitate de recunoaștere sau scanare, în timp ce un număr neobișnuit de mare de coduri din seria 500 ar putea indica tentative de conectare eșuate sau injecție SQL.

Ca și în cazul altor analize, cunoașterea rapoartelor codurilor de răspuns observate în mod obișnuit poate ajuta la identificarea tendințelor anormale care necesită investigații suplimentare

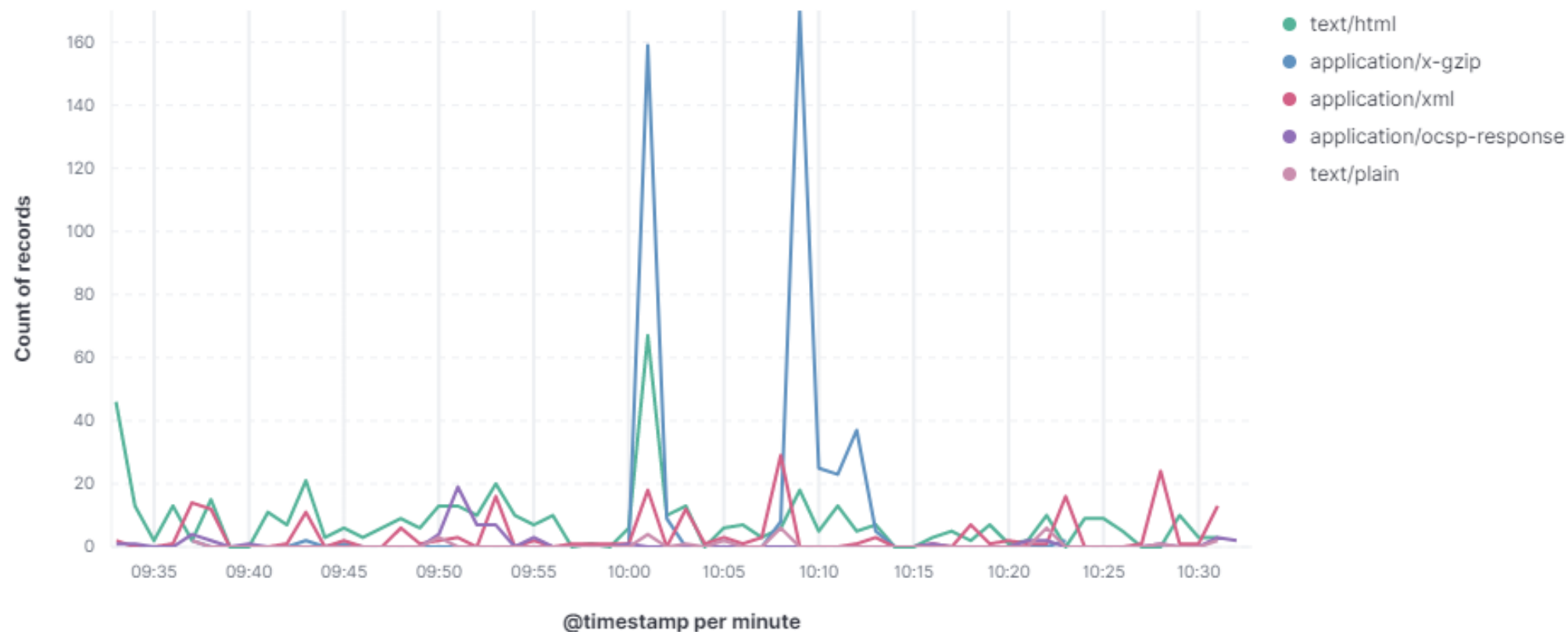
Modulul “Senzor SOC” – ZEEK – use case HTTP

HTTP Status



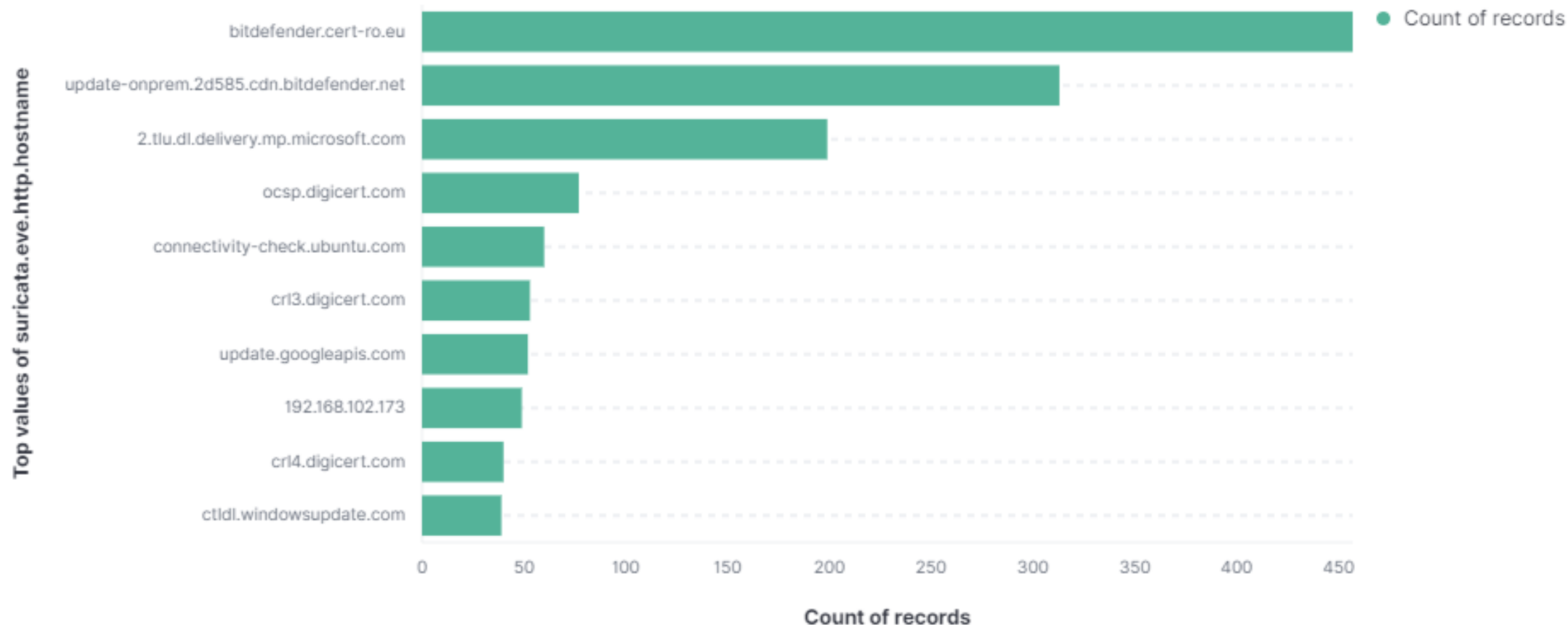
Modulul “Senzor SOC” – ZEEK – use case HTTP

2.HTTP_response_type



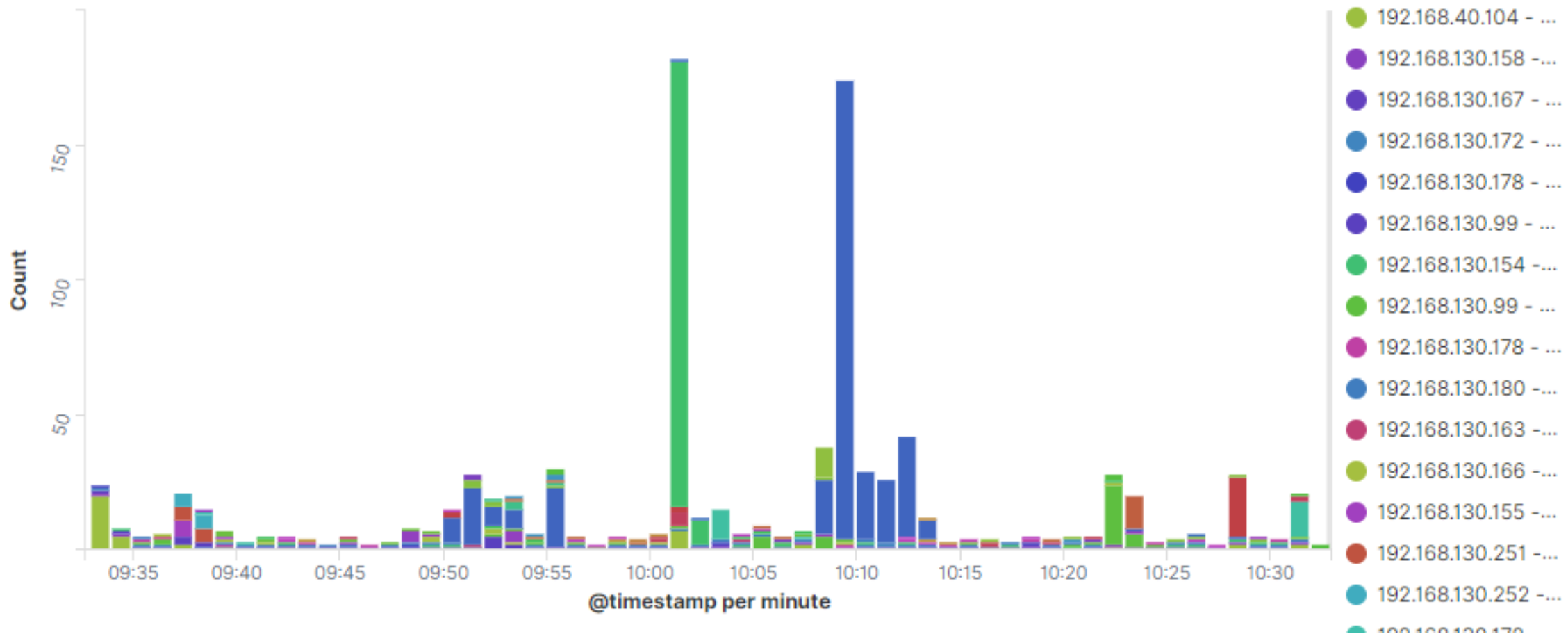
Modulul “Senzor SOC” – ZEEK – use case HTTP

2.HTTP_host_name

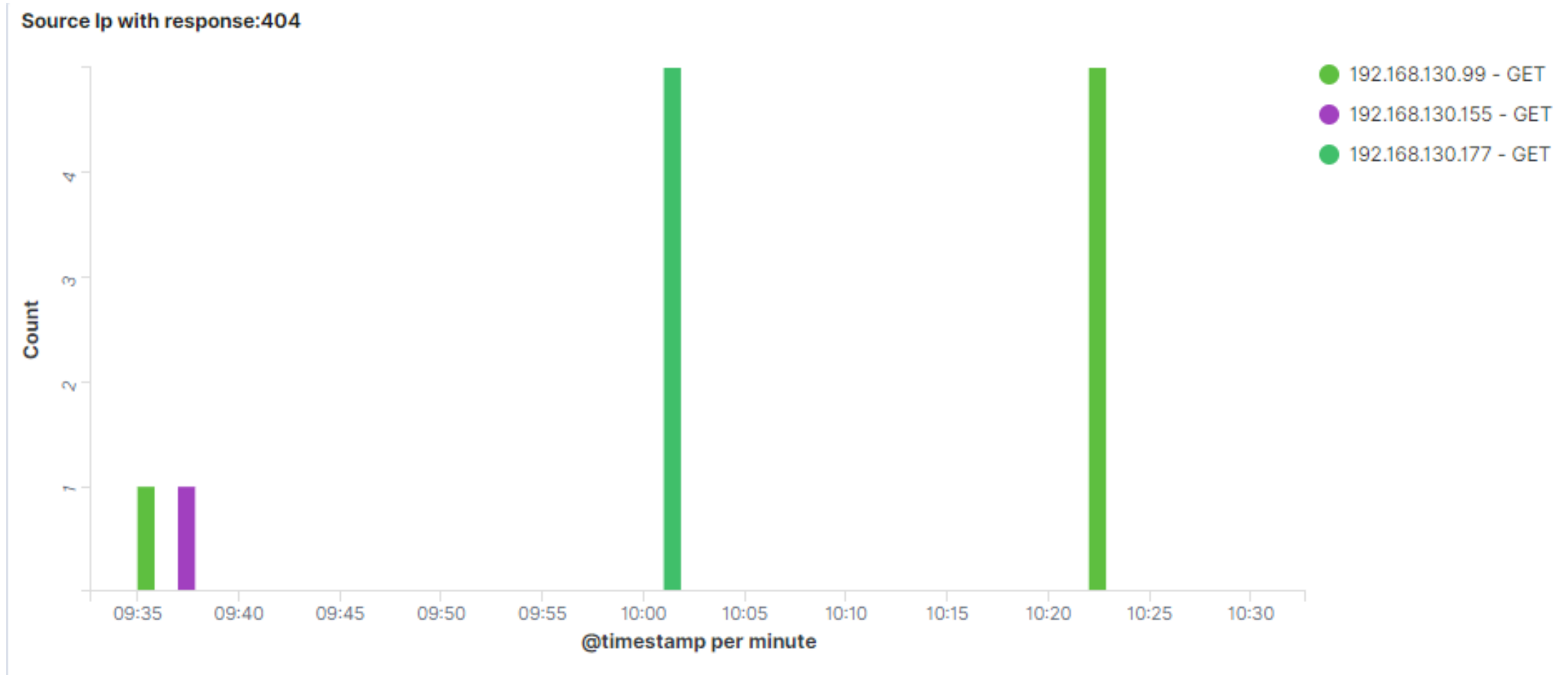


Modulul "Senzor SOC" – ZEEK – use case HTTP

Source Ip with response:200



Modulul "Senzor SOC" – ZEEK – use case HTTP



Modulul “Senzor SOC” – ZEEK – use case SSL și x509

Fișierul ssl.log conține informații colectate la nivel de handshake SSL sau TLS. ZEEK nu poate decodifica direct traficul SSL/TLS dar pot fi investigate informațiile colectate la stabilirea unei sesiuni de date criptate precum și informațiile legate de certificatele utilizate pentru criptare. Informațiile legate de certificatele utilizate pentru criptarea traficului sunt stocate în fișierul x509.log

Ce informații pot ridica semne de întrebare ?

- Certificatele self-signed și expirate sau care vor expira în curând
- Certificatele cu o perioadă de valabilitate foarte mare
- Utilizarea de algoritmi de criptare slabi sau cunoscuți ca fiind vulnerabili

Modulul “Senzor SOC” – ZEEK – use case SSL și x509

Câmpurile de la care poate fi pornită o analiză sunt:

- A. UID oferă un index/cheie ce permite efectuarea unei analize corelate prin utilizarea informațiilor ce se regăsesc în celelalte fișiere cu log-uri generate de ZEEK (de ex. conn.log, dns.log)
- B. Versiunea SSL sau TLS selectată/utilizată de server
- C. Tipul de criptare selectat de server
- D. Next Protocol Negotiation Extension – utilizat pentru negocierea criptării la nivel de aplicație.
- E. ID ce conectează informațiile din ssl.log cu cele din x509.log (acesta oferă informații suplimentare legate de certificatul utilizat pentru criptare)

ssl.log | SSL handshakes

	FIELD	TYPE	DESCRIPTION
	ts	time	Time when SSL connection first detected
A	uid & id		Underlying connection info > See conn.log
B	version	string	SSL/TLS version server chose
C	cipher	string	SSL/TLS cipher suite that server chose
	curve	string	Elliptic curve server chose when using ECDH/ECDHE
	server_name	string	Server Name Indicator SSL/TLS extension value
	resumed	bool	Flag that indicates session was resumed
	last_alert	string	Last alert seen during the connection
D	next_protocol	string	Next protocol server chose using application layer next protocol extension, if present
	established	bool	Flags if SSL session successfully established
	cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by server
E	client_cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by client
	subject	string	Subject of X.509 cert offered by server
	issuer	string	Subject of signer of server cert
	client_subject	string	Subject of X.509 cert offered by client
	client_issuer	string	Subject of signer of client cert
	validation_status	string	Certificate validation result for this connection
	ocsp_status	string	OCSP validation result for this connection
	valid_ct_logs	count	Number of different logs for which valid SCTs encountered in connection
	valid_ct_operators	count	Number of different log operators for which valid SCTs encountered in connection

Modulul “Senzor SOC” – ZEEK – use case SSL și x509

Câmpurile x509.log de la care poate fi pornită o analiză sunt:

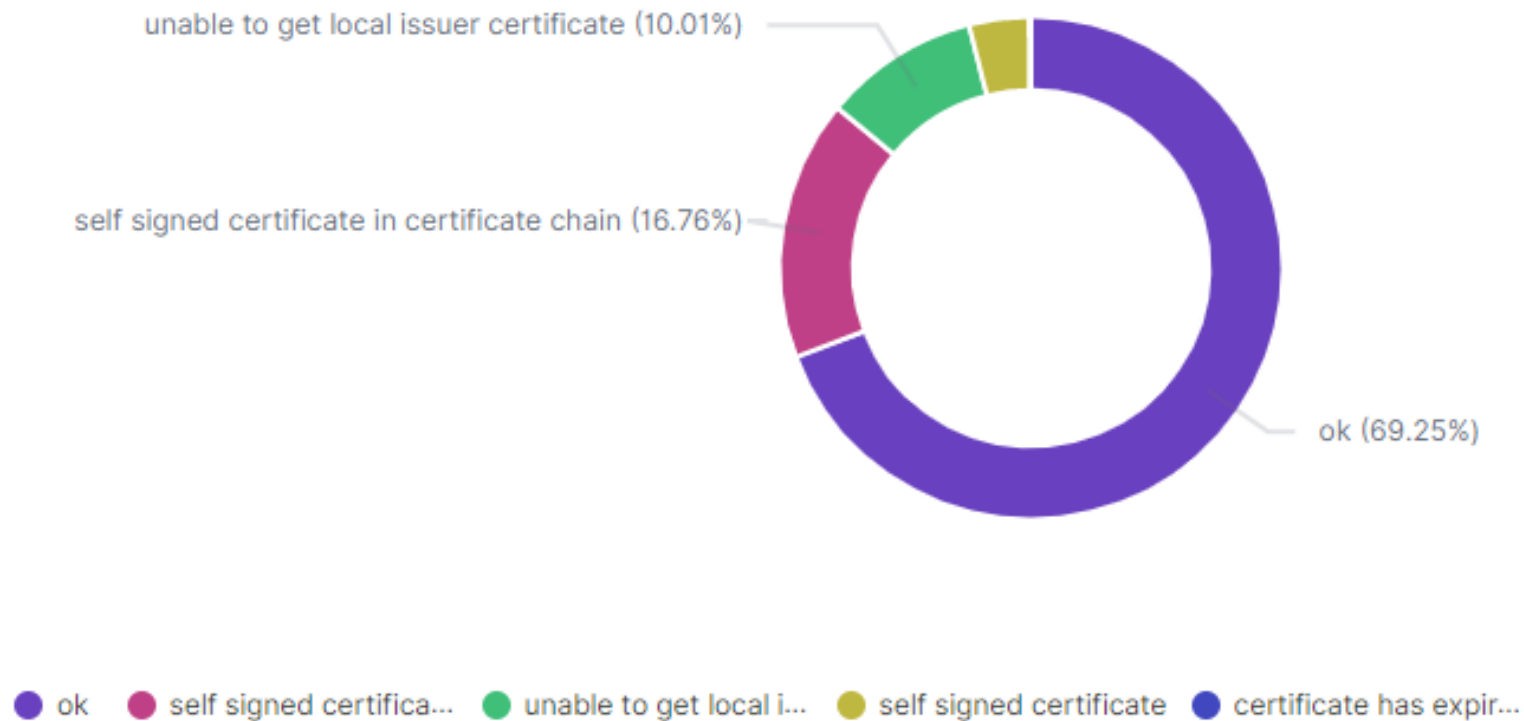
- A. Oferă un index/cheie ce permite efectuarea unei analize corelate prin utilizarea informațiilor ce se regăsesc în celelalte fișiere cu log-uri generate de ZEEK (de ex. ssl.log). Toate certificatele sunt tratate ca fișiere
- B. Emitentul certificatului
- C. Valabilitatea certificatului
- D. Lungimea cheii certificatului

x509.log | SSL certificate details

	FIELD	TYPE	DESCRIPTION
	ts	time	Time when the cert was seen
A	id	string	File unique ID
	certificate.version	count	Cert version number
	certificate.serial	string	Cert serial number
	certificate.subject	string	Cert subject
B	certificate.issuer	string	Cert issuer
	certificate.not_valid_before	time	Time the cert is valid from
C	certificate.not_valid_after	time	Time the cert is valid until
	certificate.key_alg	string	Name of the key algorithm
	certificate.sig_alg	string	Name of the signature algorithm
	certificate.key_type	string	Key type (RSA, DSA or EC)
D	certificate.key_length	count	Key length, in bits
	certificate.exponent	string	Exponent, if RSA
	certificate.curve	string	Curve, if EC
	san.dns	string_vec	List of DNS entries in Subject Alternative Name (SAN)
	san.uri	string_vec	List of URI entries in SAN
	san.email	string_vec	List of email entries in SAN
	san.ip	addr_vec	List of IP entries in SAN
	basic_constraints.ca	bool	CA flag set?
	basic_constraints.path_len	count	Maximum path length

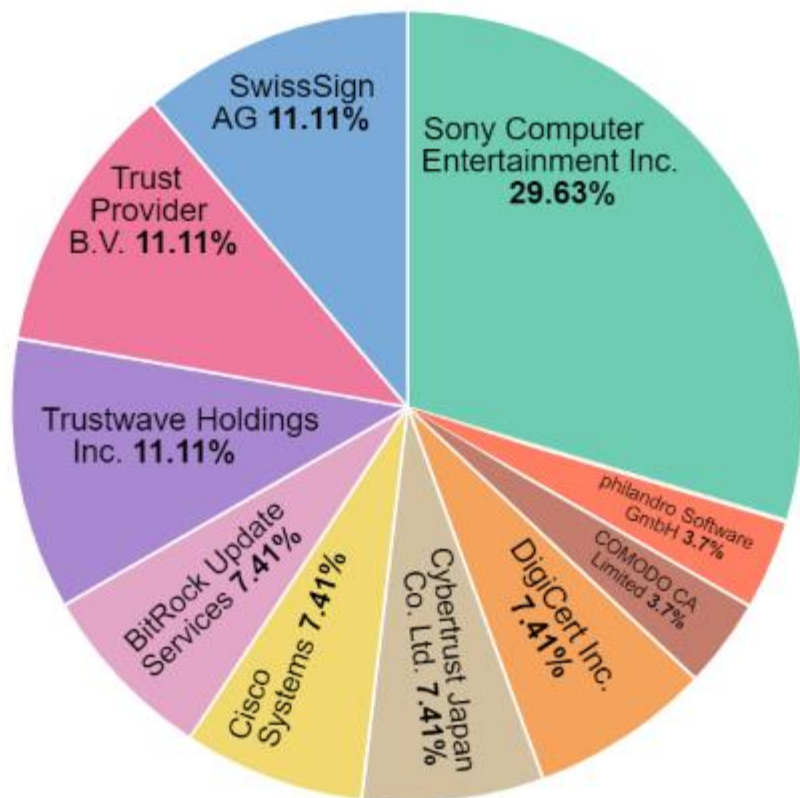
Modulul “Senzor SOC” – ZEEK – use case SSL și x509

6.SSL_Certificate_validation_status

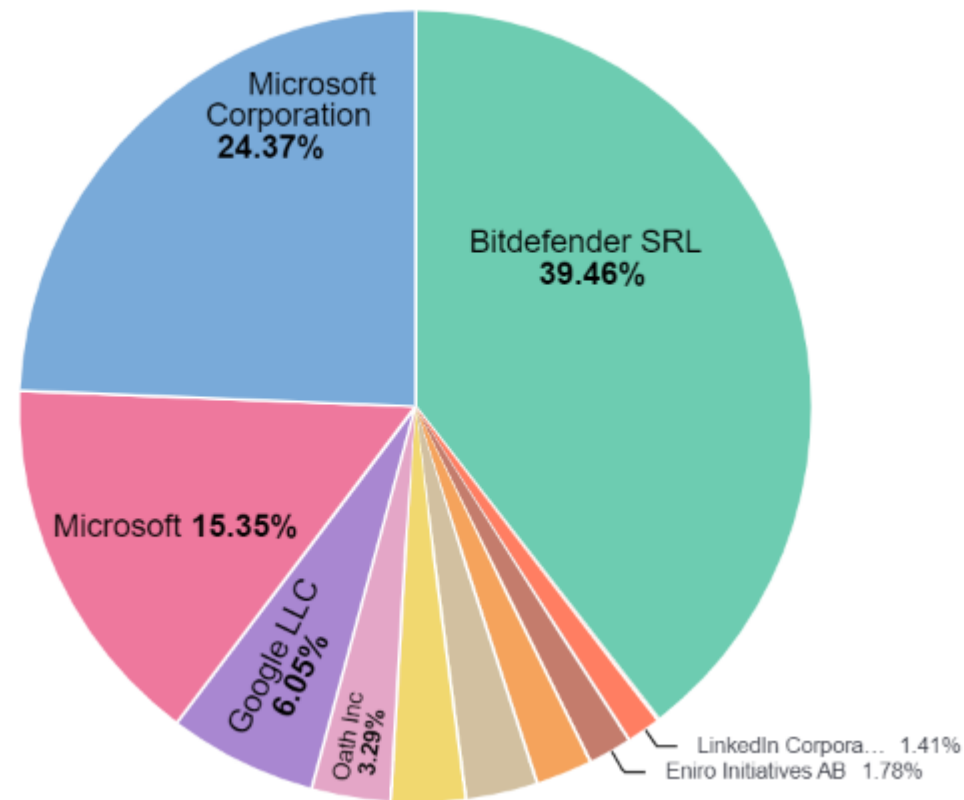


Modulul “Senzor SOC” – ZEEK – use case SSL și x509

6.SSL-x509.Issuer.organization-ascending sort

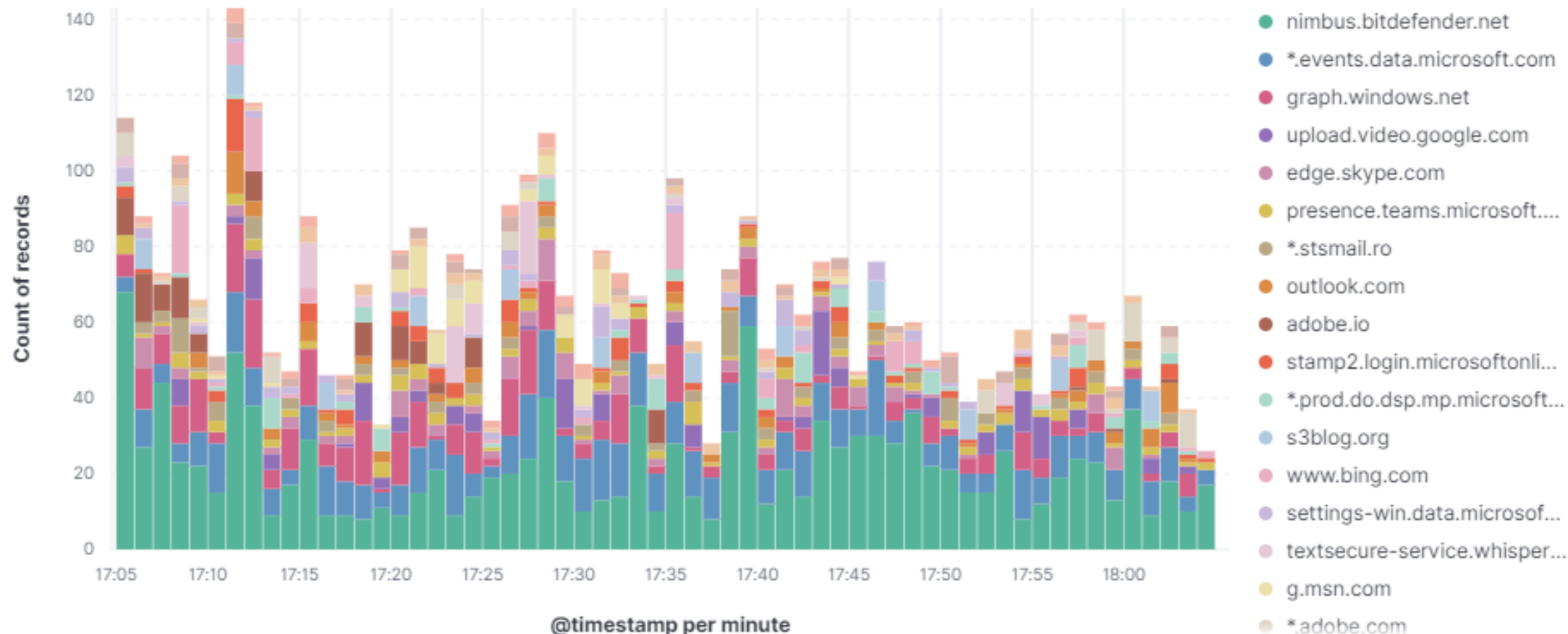


6.SSL-x509.Subject.organization-descending sort



Modulul “Senzor SOC” – ZEEK – use case SSL și x509

X509 Connection Handshake _c[zeeK]



Modulul “Senzor SOC” – ZEEK – use case SMB

Log-urile din fișierul smb.log pot fi utilizate pentru documentarea accesului utilizatorilor la fișiere partajate în rețea. De asemenea în combinație cu log-urile stocate în dce-rpc.log log-urile pot furniza informații cu privire la mișcările laterale.

The most accessed files

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\MICROSOFT\IEAK\BRANDING

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\MICROSOFT

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\Documents & Settings

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\Applications

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\Registry.pol

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\MICROSOFT\IEAK\install.ins

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\Preferences\Groups\Groups.xml

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\MICROSOFT\IEAK\BRANDING\ZONES\seczones.inf

cert-ro.eu\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\User\Preferences\RegionalOptions\RegionalOptions.xml

cert-ro.eu\Policies\{59F87312-4A3D-47F5-8DC8-F74D1C9EE4EE}\User\MICROSOFT\IEAK\install.ins

Modulul “Senzor SOC” – SNORT

SNORT este un sistem de detectare a intruziunilor în rețea (IDS) și un sistem de prevenire a intruziunilor (IPS).

Detectarea activităților malițioase din rețea se face prin definirea unor reguli. Aceste reguli vor genera alerte sau vor bloca pachetele de date atunci când un pachet de date va îndeplini criteriile introduse în regulă.

Spre deosebire de semnături, regulile se bazează pe detectarea vulnerabilității efective, nu a unui exploit sau a unei bucăți de date unice. Dezvoltarea unei reguli necesită o bună cunoaștere a modului în care funcționează de fapt vulnerabilitatea.

Modulul “Senzor SOC” – SNORT

Avantajul Snort este că soluția se bucură de o rată de adopție destul de largă, care se pretează la remedii rapide (reguli de detecție) pentru amenințări emergente.

Google

snort rules for sunburst

Toate Imagini Cumpărături Videoclipuri Știri Mai multe

Aproximativ 1.080.000 rezultate (0,56 secunde)

<https://github.com> › blob › all... Traducerea acestei pagini

[sunburst_countermeasures/all-snort.rules at main · fireeye ...](#)

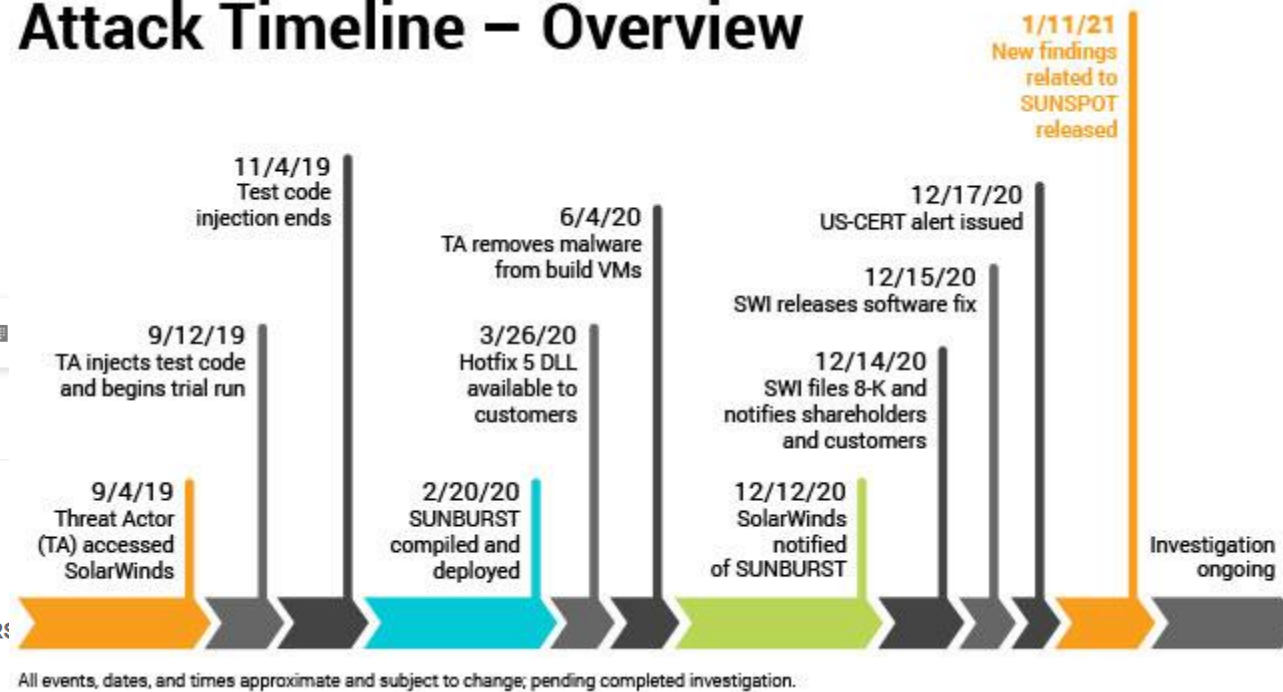
16 dec. 2020 — alert tcp \$HOME_NET any -> any any (msg:"APT.Backdoor.MSIL.SUNBURST"; content:"T "; offset:2; depth:3; content:"/swip/upd/SolarWinds.

<https://www.snort.org> › rule_d... Traducerea acestei pagini

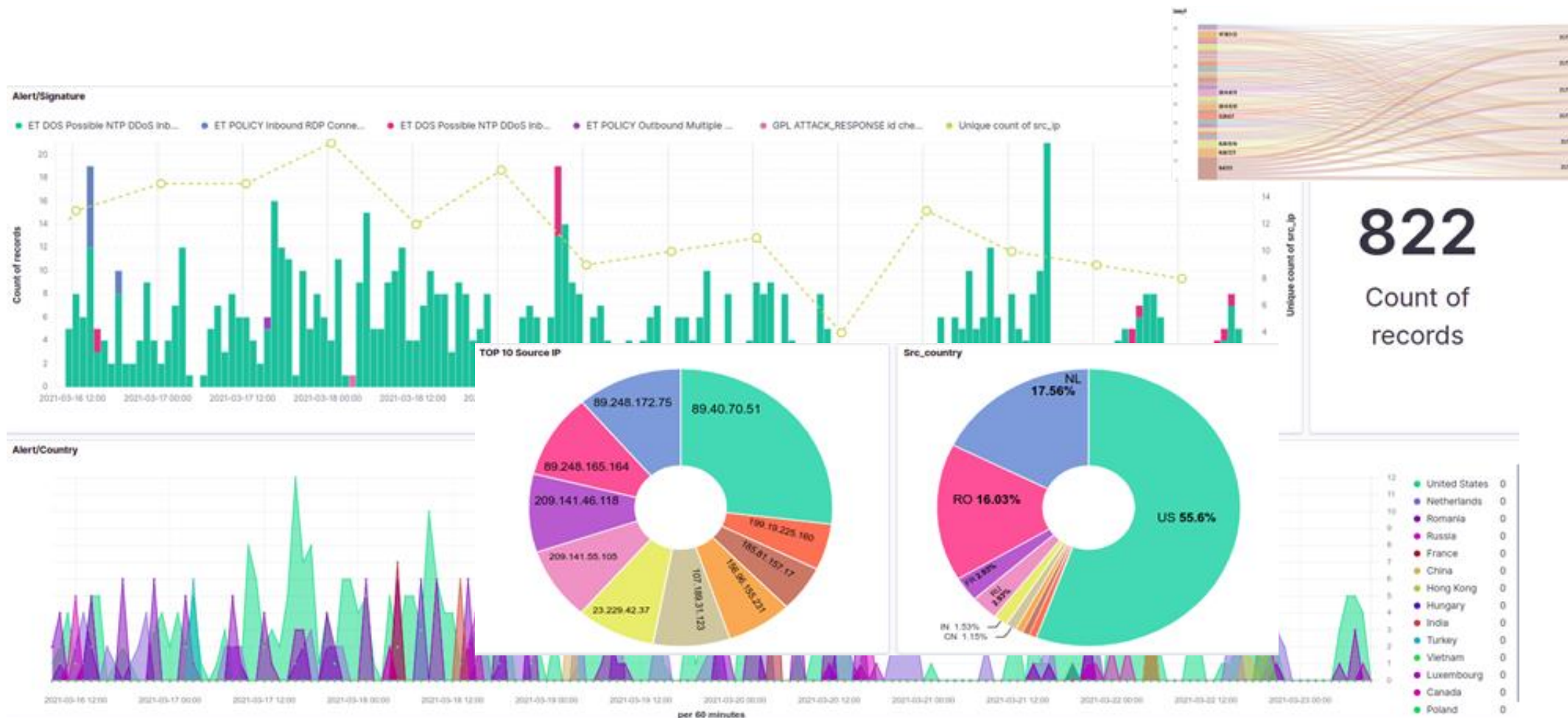
Rule Docs - Snort

MALWARE-CNC -- **Snort** has detected a Comand and Control (CNC) rule violation, ... This rule alerts on command and control traffic for Win.Backdoor.**Sunburst**.

Attack Timeline – Overview



Modulul "Senzor SOC" – SNORT



Modulul “Scanner vulnerabilități”

Modulul Scanner de vulnerabilități va permite scanarea neintrusivă a adreselor IP și URL și va avea în vedere:

- identificarea tehnologiilor folosite
- identificarea versiunilor tehnologiilor folosite
- compararea tehnologiilor și versiunilor acestora cu baze de date de vulnerabilități publice sau private și identificarea celor vulnerabile

Modulul va permite introducerea automată (ex. API) și manuală a adreselor IP și a URL-urilor (individuale sau listă) ce vor fi scanate.

La nivelul platformei RO-SAT vor fi dezvoltate formulare web prin intermediul cărora beneficiarii platformei vor completa informații precum: ip-uri, domenii/url-uri proprii, domeniul de activitate, etc

Pe baza acestor informații vor fi realizate în mod automatizat scanări iar rezultatele acestora vor fi furnizate manual/automatizat beneficiarilor platformei.

Modulul “Crawling website-uri”

Acest modul va permite analiza site-urilor din aria de competență a CERT-RO (siteuri .ro sau site-uri găzduite în România) pentru identificarea malware-ului și amprentarea vulnerabilităților existente la nivelul acestora. Analiza va fi făcută neintruziv (fără acțiuni ce ar putea afecta buna funcționare a site-ului; ex: injecturi) pentru a descoperi informații care să permită detectarea și evaluarea vulnerabilităților existente.

Modulul va permite introducerea automată (ex. API) și manuală a adreselor IP și a URL-urilor (individuale sau listă) ce vor fi scanate.

La nivelul platformei RO-SAT vor fi dezvoltate formulare web prin intermediul cărora beneficiarii platformei vor completa informații precum: ip-uri, domenii/url-uri proprii, domeniul de activitate, etc

Pe baza acestor informații vor fi realizate în mod automatizat scanări de website-uri/url-uri iar rezultatele acestora vor fi furnizate manual/automatizat beneficiarilor platformei.

Modulul “OSINT”

Acest modul va fi utilizat pentru agregarea automată a informațiilor din surse publice (portaluri web, forumuri, blog-uri etc.) referitoare la amenințări, vulnerabilități și riscuri cibernetice- folosind surse publice si private, cum ar fi forumuri, site-uri web, social media

Soluția va oferi acces la date disponibile în internet astfel încât un analist să poată înțelege cine este atacatorul și ce infrastructură folosește pentru a-și efectua atacurile. Pentru aceasta un analist va furniza indicatori de compromitere (IOC) sau artefacte suspecte, cum ar fi (dar nu limitat la) un domeniu, o adresă IP sau o adresă de e-mail, înregistratorii WHOIS, informații despre certificatul SSL etc.

Soluția va permite exportarea manuală și automatizată a informațiilor colectate către alte baze de date, printr-o interfață de tip restAPI

Modulul „Cyber Threat Intelligence”

Modulul de Cyber Threat Intelligence va colecta informații din mai multe surse de acest tip, le va agrega și le va transmite către platforma de analiză. În cadrul acestui modul vor fi incluse subscripții la diferite servicii de tip Cyber Threat Intelligence, unele dintre acestea fiind oferite gratuit structurilor de tip CERT, altele fiind accesibile contracost.

Obiectivul principal al acestui modul este acela de a integra și corela informațiile obținute prin intermediul terminalelor SOC, al modulelor de darknet și honeynet cu cele furnizate prin intermediul subscripțiilor pentru a putea fi identificate tipurile de atacuri existente deja în spațiul cibernetic național, precum și atacatorii care le derulează, în scopul facilitării procesului de investigare și de limitare a efectelor atacurilor cibernetice.

Modulul colectare, normalizare și îmbogățire

Modulul colectare, normalizare și îmbogățire este responsabil de corelarea și analiza datelor colectate la nivelul platformei. Practic alertele sunt normalizate, standardizate și îmbogățite cu detaliile lipsă, fiind transpuse într-o bază de date, structurată conform nevoilor interne, pentru a simplifica regăsirea datelor, analiza acestora precum și identificarea anumitor corelații între atacuri.

Datele colectate vor fi îmbogățite cel puțin cu următoarele tipuri de informații: **GeoIP, subnet IP, deținător, adresă email abuse, ASN, DNS Name/domenii asignate IP-urilor, țară asignată, zonă/localitate, reputație IP/URL** (bazat pe CTI colectate/disponibile prin intermediul platformei RO-SAT)

Structura internă a bazei de date va urmări formatul internațional STIX de schimb de date despre incidentele de securitate cibernetică.

Modulul “Big Data Security Analytics”

Acest modul va utiliza tehnologii de tip Machine Learning și Artificial Intelligence pentru analiza automată a datelor colectate de soluțiile RO-SAT într-o platforma de tip Big Data precum și generarea de informații despre: alerte, tendințe, tehnici de atac, unelte de atac, etc.

Obiectivul principal al acestui modul este acela de a asigura procesarea informațiilor obținute din modulele descrise anterior, astfel încât să poată fi identificate pattern-urile ce pot anticipa activități specifice pregătirii unor atacuri cibernetice sau activități specifice unor atacuri aflate în derulare, dar încă nedescoperite (nedocumentate).

Modul “Security Operations Center”

Acest modul va cuprinde capacitățile de monitorizare în timp real al evenimentelor, alertelor, incidentelor pe diferite tipuri de infrastructuri esențiale (conform celor definite de Directiva NIS).

Obiectivul principal al acestui modul este acela de a furniza în timp real informații despre situațiile care necesită intervenție/reacție rapidă a echipelor specializate din cadrul CERT-RO, astfel încât să fie asigurate stoparea atacurilor cibernetice, limitarea efectelor/pierderilor, coordonarea în vederea restabilirii funcționării normale și efectuarea investigațiilor aferente.

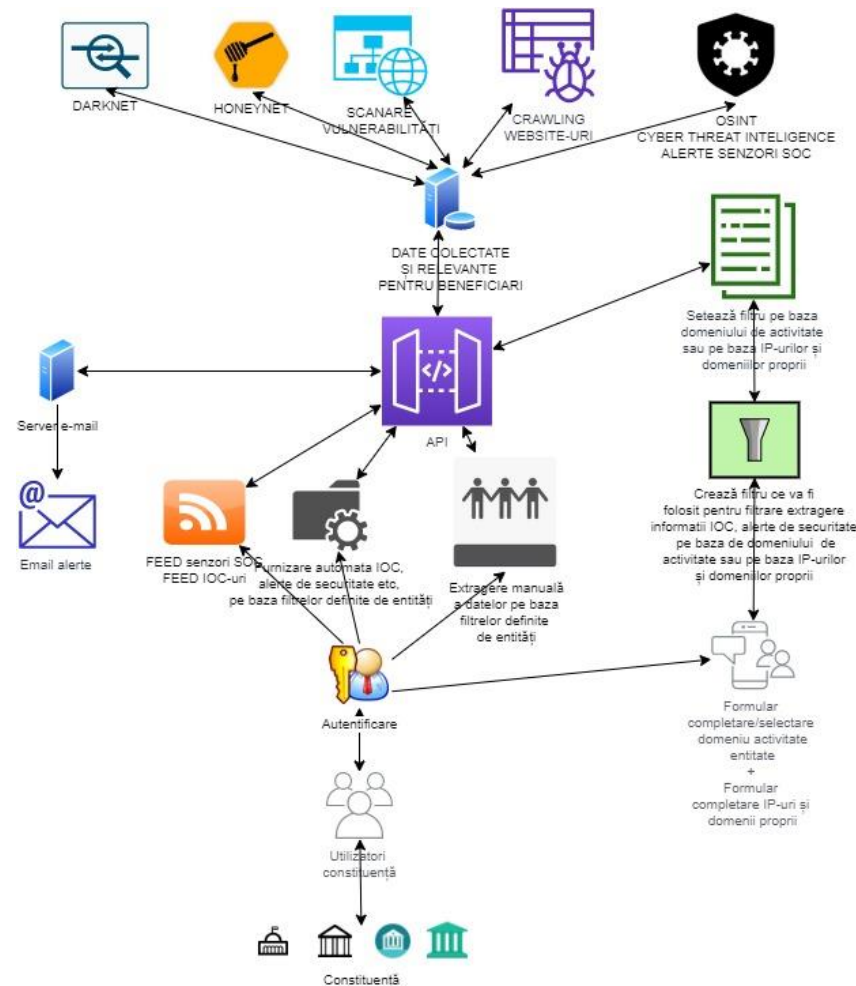
Modulul „Diseminare date” (API)

Prin intermediul modulului, datele corelate vor fi făcute disponibile partenerilor în funcție de responsabilitățile acestora (autorități publice, ISP-iști, furnizori de servicii digitale etc.) sau în baza prevederilor protoalelor de cooperare bilaterale încheiate.

De asemenea, acest modul va intermedia accesul la serviciile ce vor fi oferite prin platforma RO-SAT, respectiv:

- alertare timpurie referitor la posibilitatea/iminența derulării unor atacuri
- alerte de securitate referitoare la atacurile identificate/raportate
- rapoarte referitoare la nivelul de amenințare cibernetică
- statistici de securitate
- indicatori de compromitere (IoC) care vor putea fi preluați de beneficiari/parteneri automat și/sau manual.

Modulul „Diseminare date” (API) - utilizare



Întrebări



Email: gabriel.ene@cert.ro

Email: dumitru.david@cert.ro