ЧОМУ БУТИ "БЕЗПЕЧНИМ" **ТЯЖКО**, **ДОВГО** ТА **ДОРОГО**?

ІНФОРМАЦІЙНА БЕЗПЕКА VS КІБЕРБЕЗПЕКА

ХТО ПРАЦЮЄ

- Blue Team:
  - CISO
  - InfoSec Director
  - SecOps Specialists (Analysts)
- Red Team:
  - PenTesters

ЧОМУ?


NORSE
ATTACK ORIGINS
ATTACK TYPES
ATTACK TARGETS
LIVE ATTACKS

Кібертероризм
(Cyberterrorism)

Шахрайство в
інтернеті
(Internet Fraud)

Кібервійни
(Cyberwarfare)

Кібервимагання
(CyberXtortion)

Кібератака на енергетичні компанії України [ред. • ред. код]

Матеріал з Вікіпедії — вільної енциклопедії.

Кібератака на енергетичні компанії України — перша зареєстрована успішна кібератака на енергетичну систему з виведенням її із ладу. Сталась 23 грудня 2015 року. Російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України. Наступна, і набагато менш масштабна за наслідками, кібератака сталась вночі з 17 на 18 грудня 2016 року. Протягом трохи більше однієї години була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берегу Києва та прилеглих районів області[1].

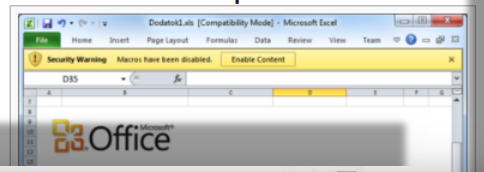
Найб
близ
годи

Водн
насл
мере
Феде

Зага

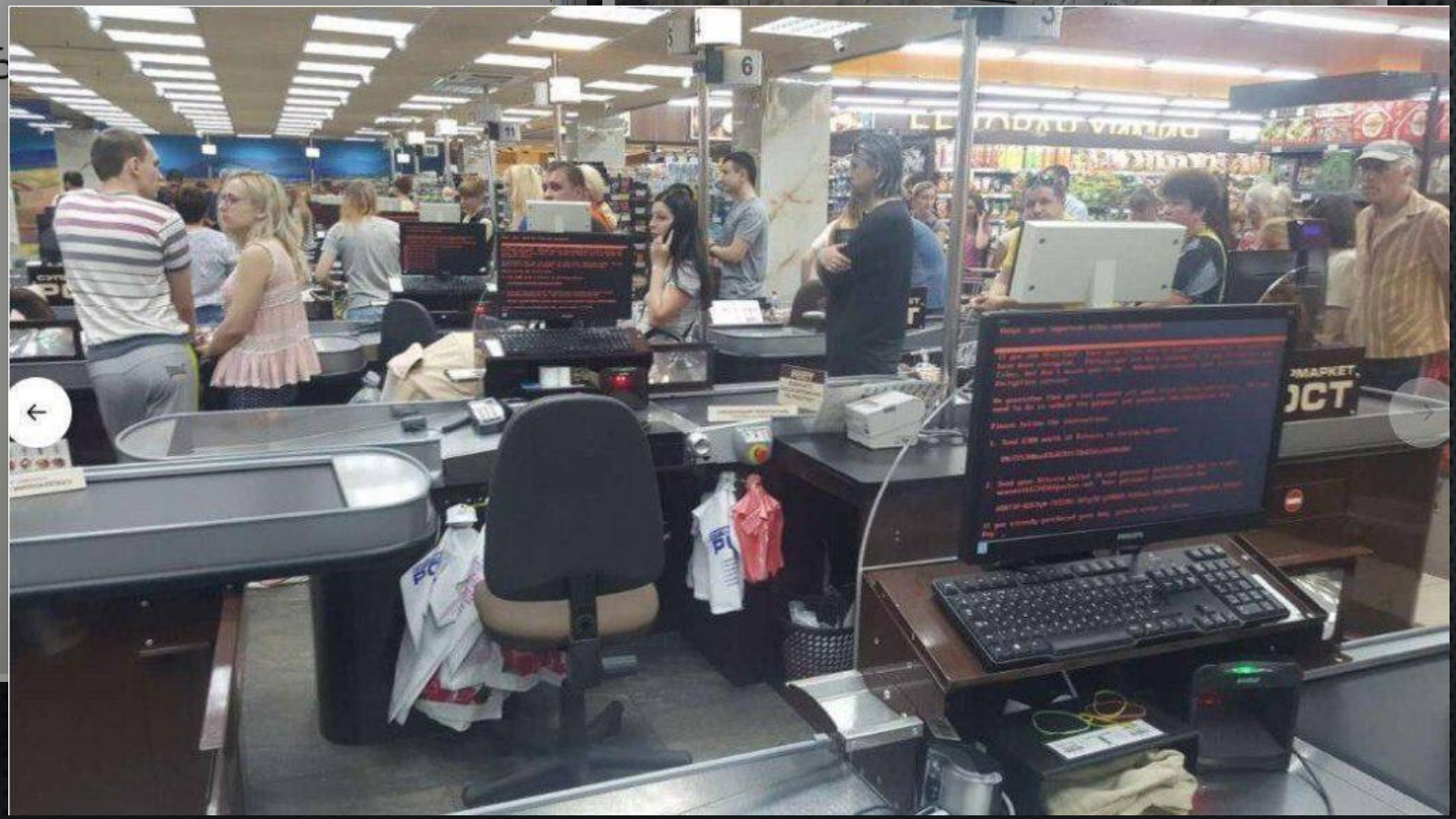
- П
в
- З
- В

Кібератака на енергетичні компанії України



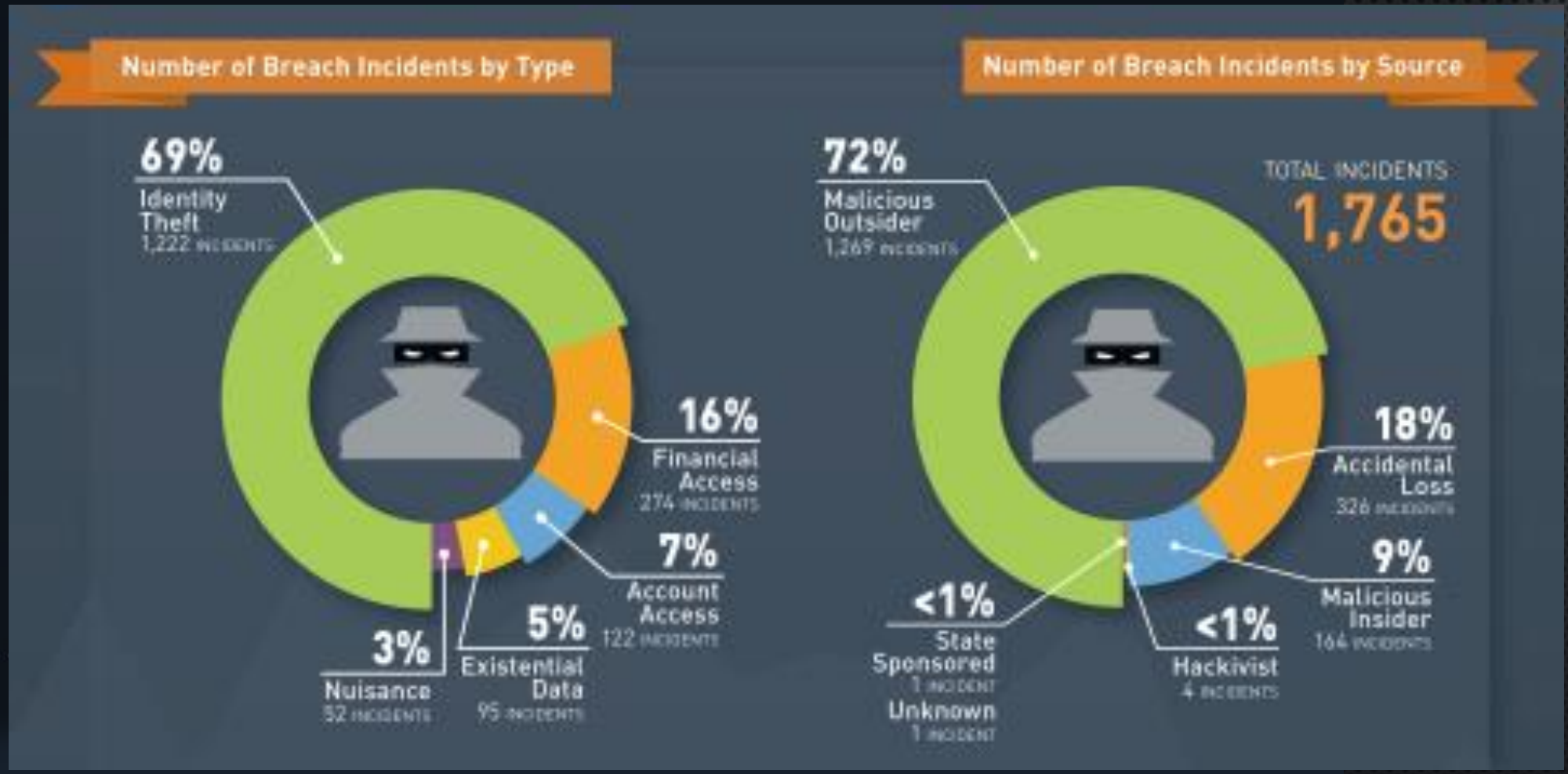
AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

США: доказательства вмешательства РФ в выборы неопровержимы

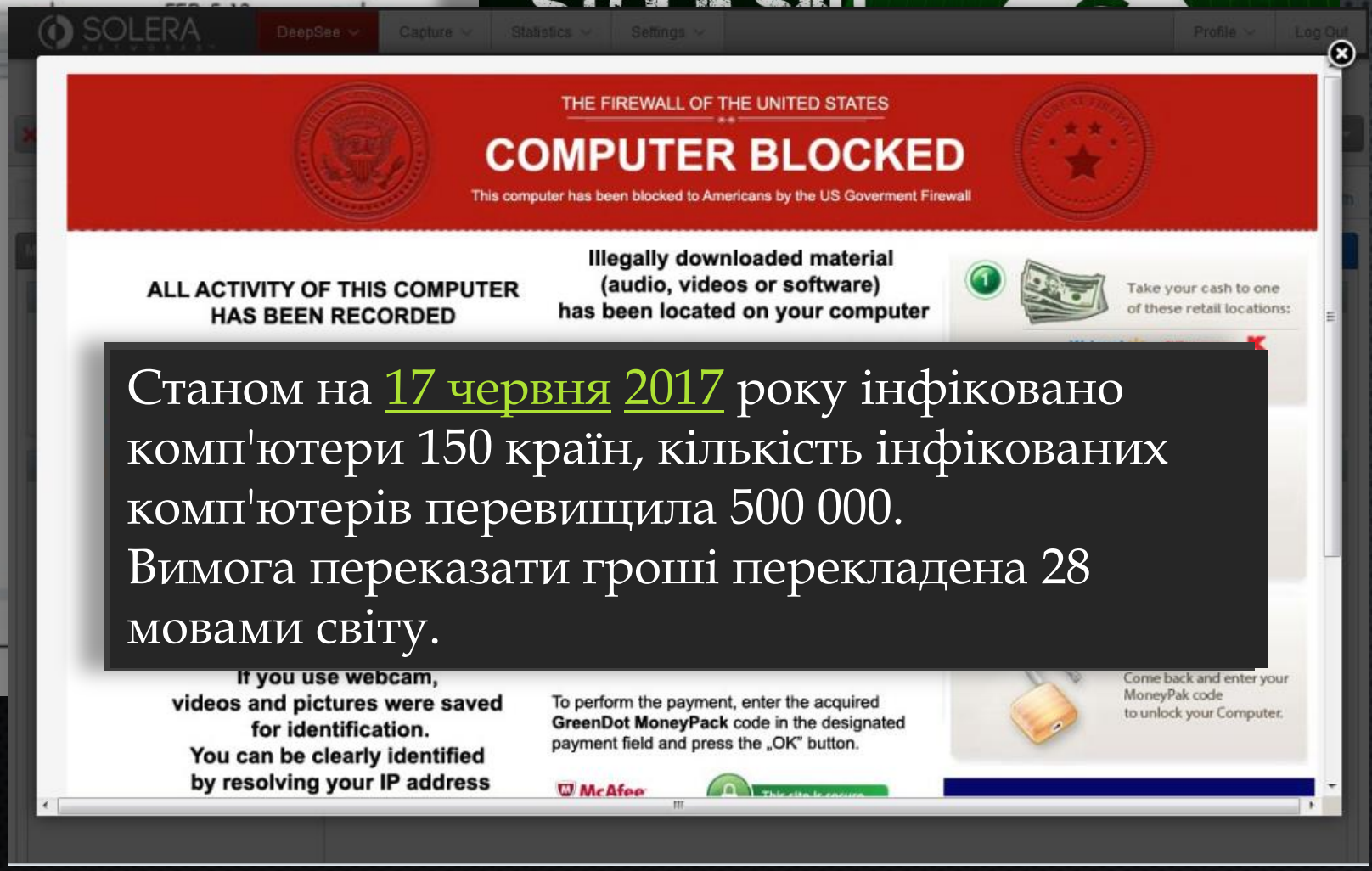


Number of health care providers affected by electronic hacks, 2010 - 2019

PBS NEWS HOUR



cords-stolen-compromised-2017



Станом на 17 червня 2017 року інфіковано комп'ютери 150 країн, кількість інфікованих комп'ютерів перевищила 500 000.
Вимога переказати гроші перекладена 28 мовами світу.

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

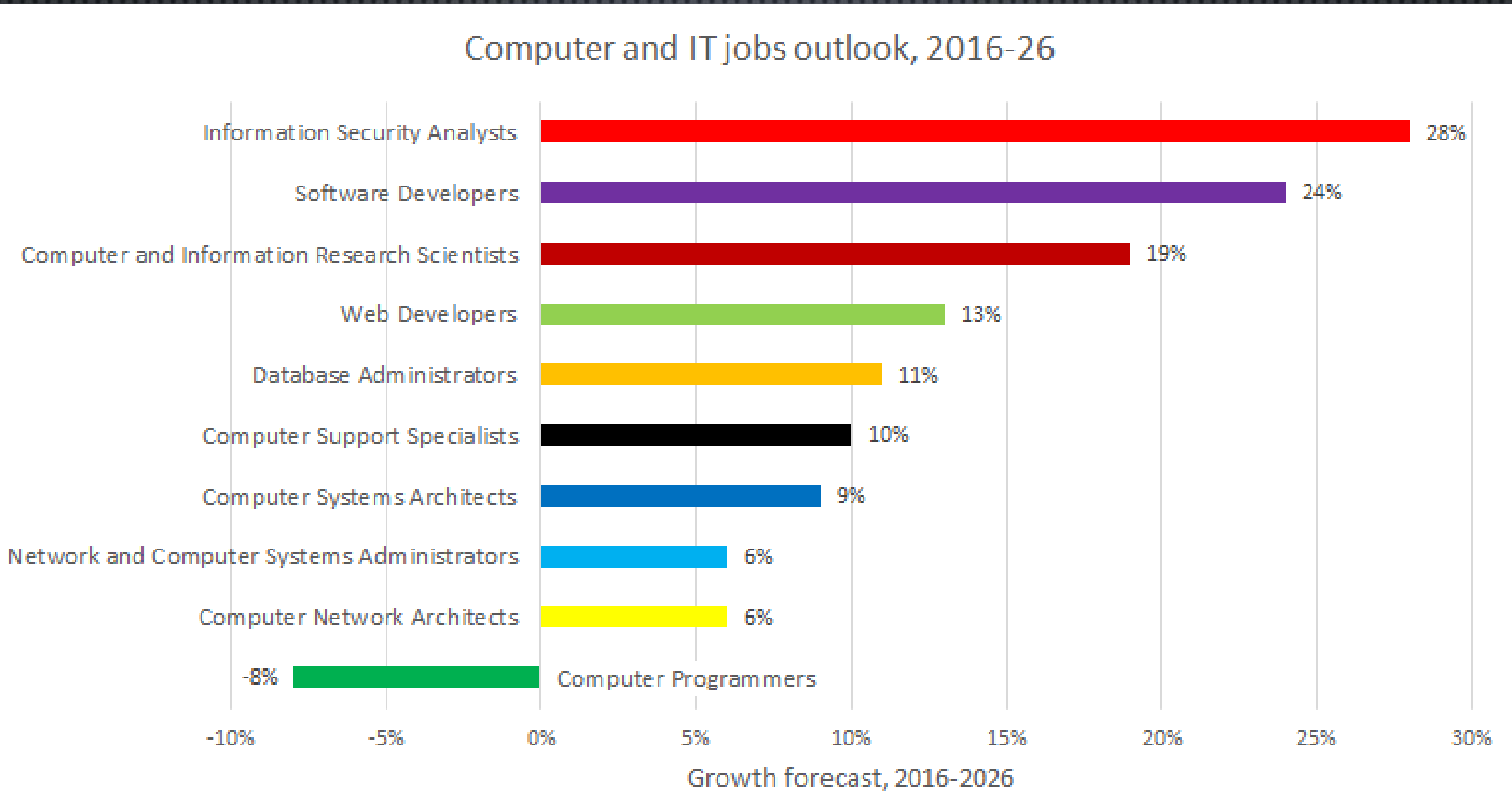
1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

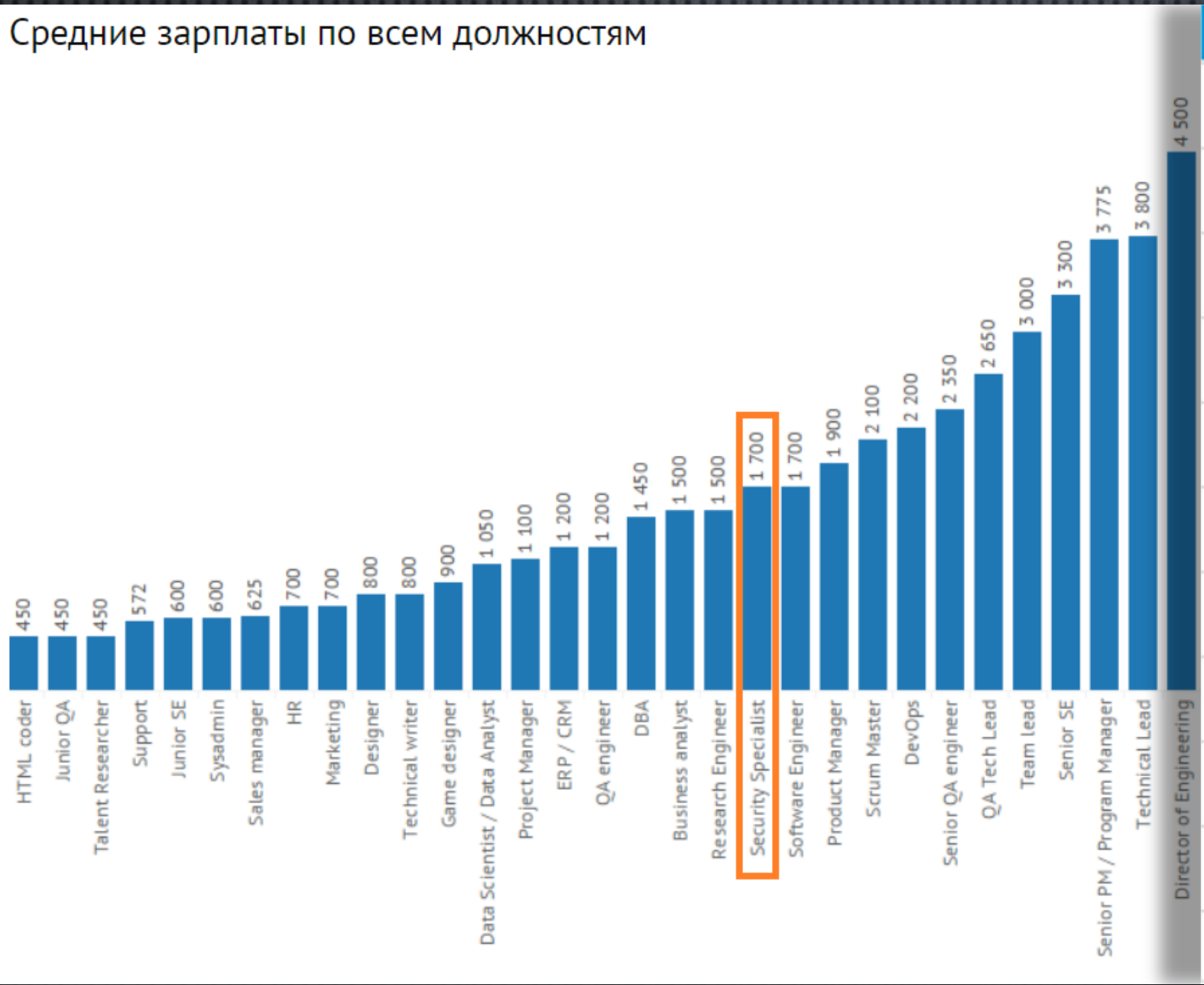
   Ap5JVb-qhTAHy-HyeyS2-wqeQEK-YtHQeK-w7NUmZ-11RBUq-fuu4Wa-zpv8dS-zeQNGS

If you already purchased your key, please enter it below.
Key: _



https://www.zdnet.com/article/it-jobs-in-2020-preparing-for-the-next-industrial-revolution/

Средние зарплаты по всем должностям



#		Average GROSS Salary
1.	Computer Architect	US$ 144,718
2.	IT Researching	US$ 126,833
3.	Consulting, Speaker	US$ 123,561
4.	SAP Consulting	US$ 121,500
5.	SAP Developer	US$ 108,999
6.	Software Engineer	US$ 104,229
7.	Hardware Engineer	US$ 103,607
8.	Network Manager	US$ 100,584
9.	Security Specialist	US$ 97,077
10.	SAP Administrator	US$ 96,000
11.	Computer Engineer	US$ 92,747

https://dou.ua/lenta/articles/salary-report-dec-2017/

http://www.averagesalarysurvey.com/it-telecommunication-ii/ukraine/

ТЯЖКО ТА ДОВГО?


CLOUD
amazon web services
Microsoft
Google Cloud Platform
THREAT INTELLIGENCE
THE MEDIA TRUST
PHISHME
WEBROOT
THREAT CONNECT
mnemonic
THREATQUOTIENT
ANOMALI
ThreatSTOP
Recorded Future
VIRTUALIZATION
openstack
vmware
hp
NUTANIX
The Enterprise Cloud Company
nuagenetworks
From Nokia
CITRIX
Juniper CONTRAIL
NEC
MIRANTIS
big switch networks
FUJITSU
cisco
ARISTA
intel
ENTERPRISE SECURITY
THALES
gemalto
security to be free
savvius
TITUS
IONIC
AREA 1
DIGITAL GUARDIAN
FOURV SYSTEMS
proofpoint
PHISHME
Attivo NETWORKS
PROTECTWISE
TRAPX SECURITY
VENAFI
TANIUM
tenable network security
SKYSEA Client View
NUBEVA
E8 SECURITY
GURUCUL
PREDICTIVE SECURITY ANALYTICS
BeyondTrust
GUIDANCE SOFTWARE
Symantec
VECTRA
esentire
Corvil
BACKBOX
tripwire
PICUS SECURITY
RAPID7
ziften
exabeam
HOB
Cyber Security
IntelliGO
Canon
SD-WAN
riverbed
TALARI Network
nuagenetworks
From Nokia
ECESSA
CLOUDGENIX
silver peak
vmware
CITRIX
viptela
Software Defined WAN
velocloud
IDENTITY& ACCESS MANAGEMENT
Centrify
CYBERARK
DUO
SECUREAUTH
RSA
gemalto
security to be free
Microsoft
okta
altipeak security
Ping Identity
SyferLock
AUTHOMATE
Entrust Datacard
SWIVEL
NETWORKING
AVAYA
vmware
NSX
ForeScout
Sonus
Extreme
ARISTA
BRADFORD NETWORKS
plenarylogic
GARLAND
Gigamon
PulseSecure
Interface Masters
NIAGARA NETWORKS
cisco
AlaxalA
ixia
Allied Telesis
RAD
Network Critical
portnox
saasyan
SECURITY ANALYTICS
splunk>
LogRhythm
BlackStratus
SIFT SECURITY
plixer
EIQ
RSA
ArcSight ESM
Logsign
IBM Security
QRadar
ALIEN VAULT
Infoscience
LogicMonitor

Потрібно:

- Написати політики\стандарти
- Розібратися з інфраструктурою
- Розібратися з логами
- Вививчити мережевий стек
- Розібратися з Firewall-ами
- Розібратися з IDS
- Розібратися з SIEM-ом
- Встановити та підтримувати антивірусні рішення
- Організувати доставку ЛОГів з різних джерел до SIEм-у
- І багато-багато-багато іншого

ДОРОГО?

Picture source: https://www.linkedin.com/pulse/security-operations-center-soc-built-shared-branden-rowe/

ПРАКТИКА

Nessus™

Report generated by Nessus™

Live Results Scan

Mon, 17 Sep 2018 17:57:16 EDT

TABLE OF CONTENTS

Hosts Executive Summary

Collapse All | Expand All

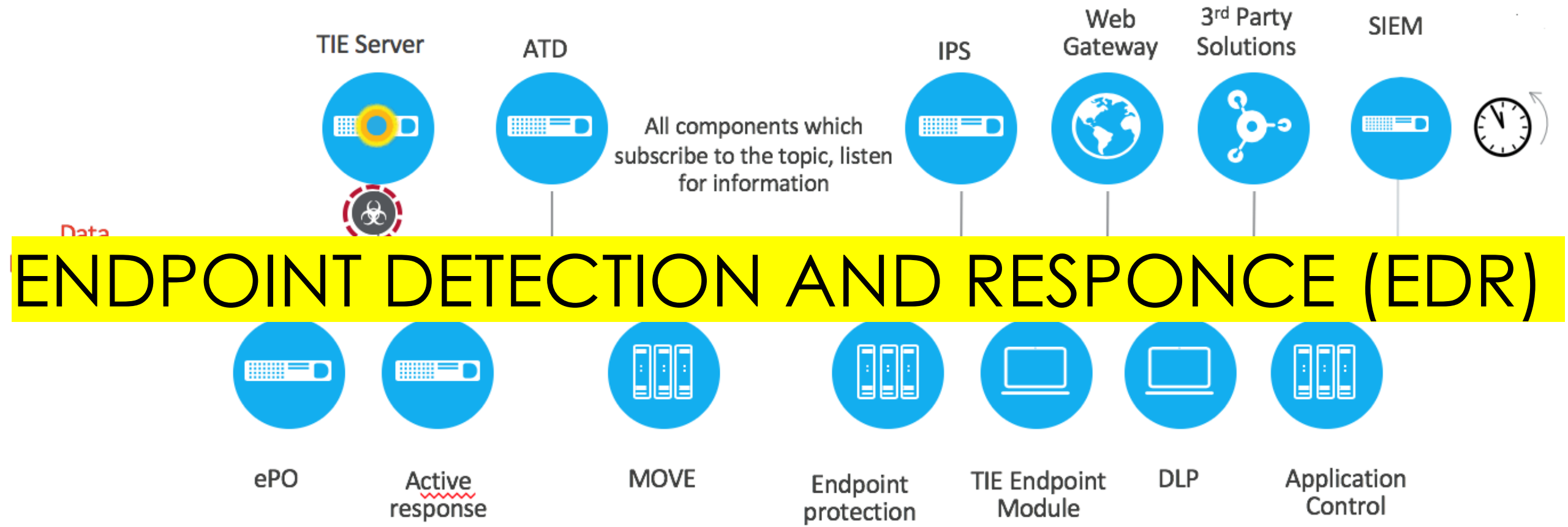
localhost

1	6	1	0	37
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
CRITICAL	10.0	56584	[Offline] Mozilla Foundation Unsupported Application Detection (macOS)
HIGH	9.3	108375	[Offline] Mozilla Firefox < 59 Multiple Vulnerabilities (macOS)
HIGH	9.3	108585	[Offline] Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities (macOS)
HIGH	9.3	109867	[Offline] Mozilla Firefox < 60 Multiple Critical Vulnerabilities (macOS)
HIGH	9.3	110806	[Offline] Mozilla Firefox < 61 Multiple Critical Vulnerabilities (macOS)
HIGH	9.3	117291	[Offline] Mozilla Firefox < 62 Multiple Critical Vulnerabilities (macOS)

СКАНЕРИ ВРАЗЛИВОСТЕЙ АБО МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ

IDS/IPS СИСТЕМИ ВИЯВЛЕННЯ МЕРЕЖЕВОГО ВТОРГНЕННЯ



ENDPOINT DETECTION AND RESPONCE (EDR)

NGFW

NEXT GENERATION FIREWALL

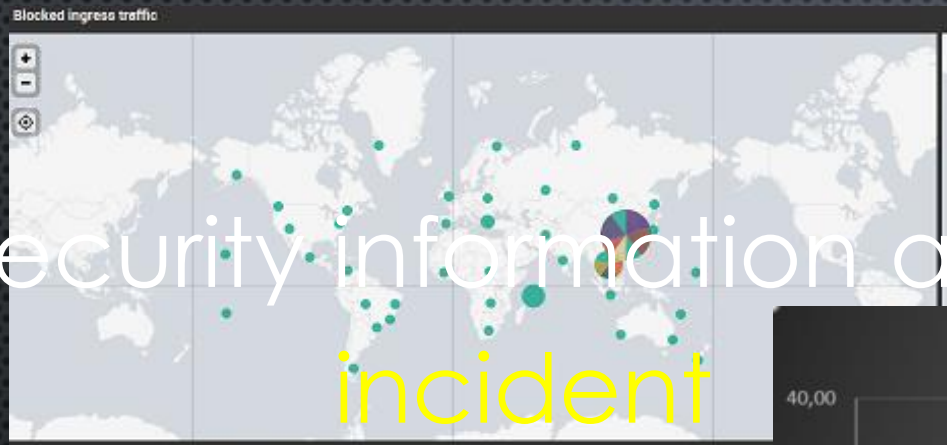

ALIEN VAULT
BlackStratus
Netsurion
EventTracker
Actionable Security Intelligence
exabeam
FireEye
FORTINET
LogRhythm
ManageEngine
McAfee
MICRO FOCUS
IBM
QRadar
RAPID7
RSA
SECURITY
SECURONIX
solarwinds
splunk>
tripwire
Trustwave
Venustech

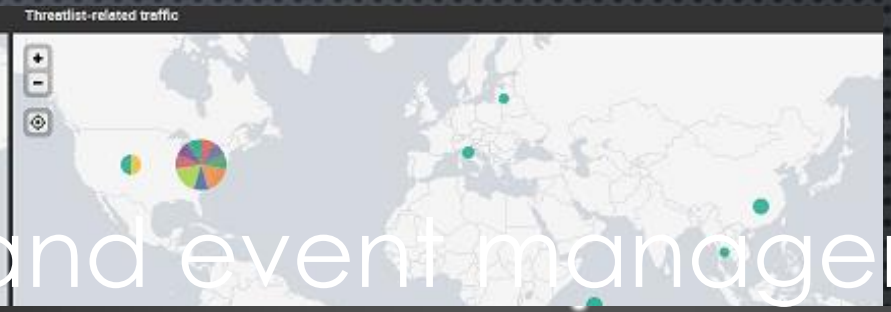
ЩО ТАКЕ SIEM?

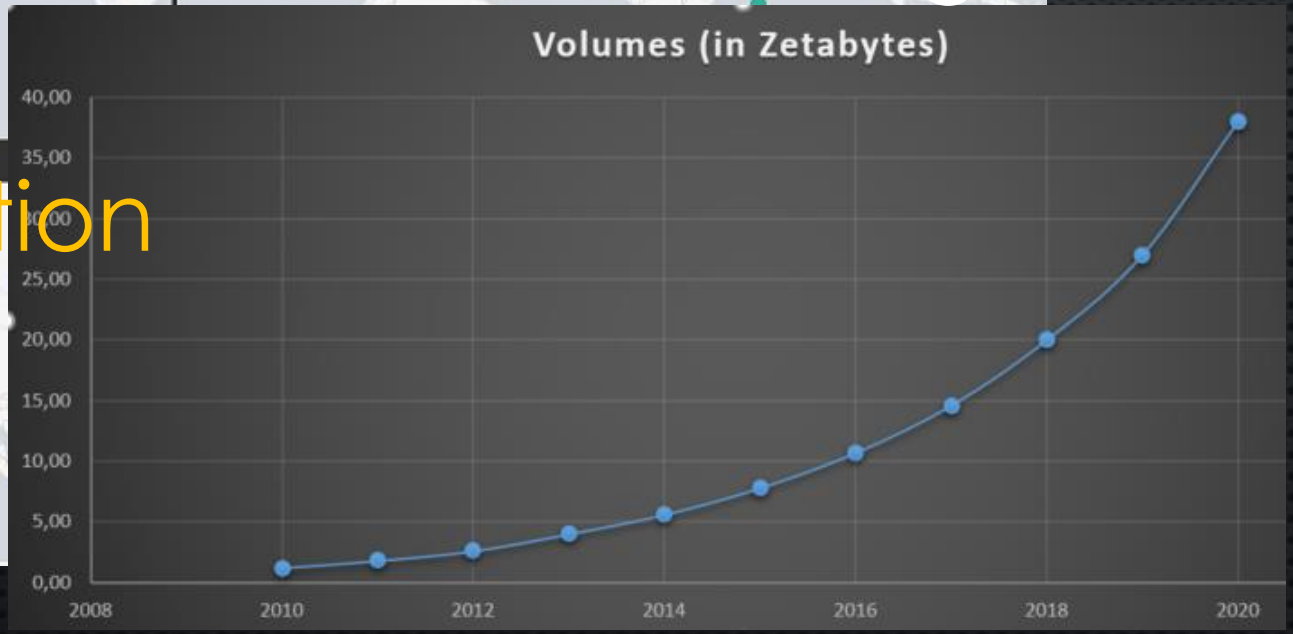
Security information and event management

incident

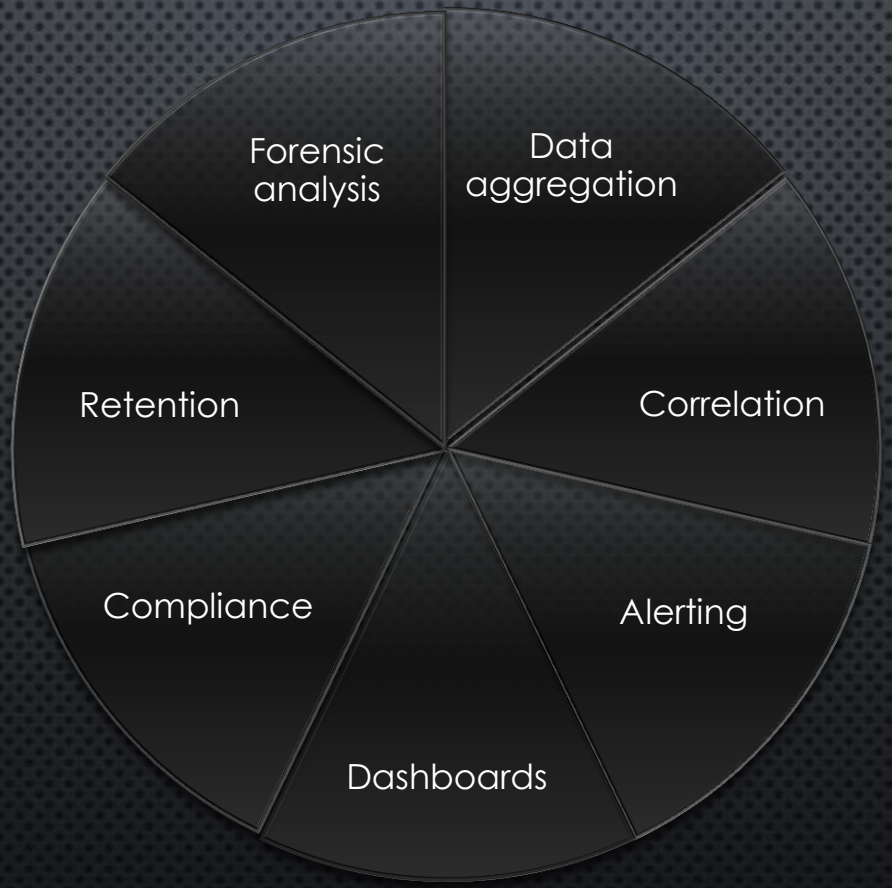
investigation



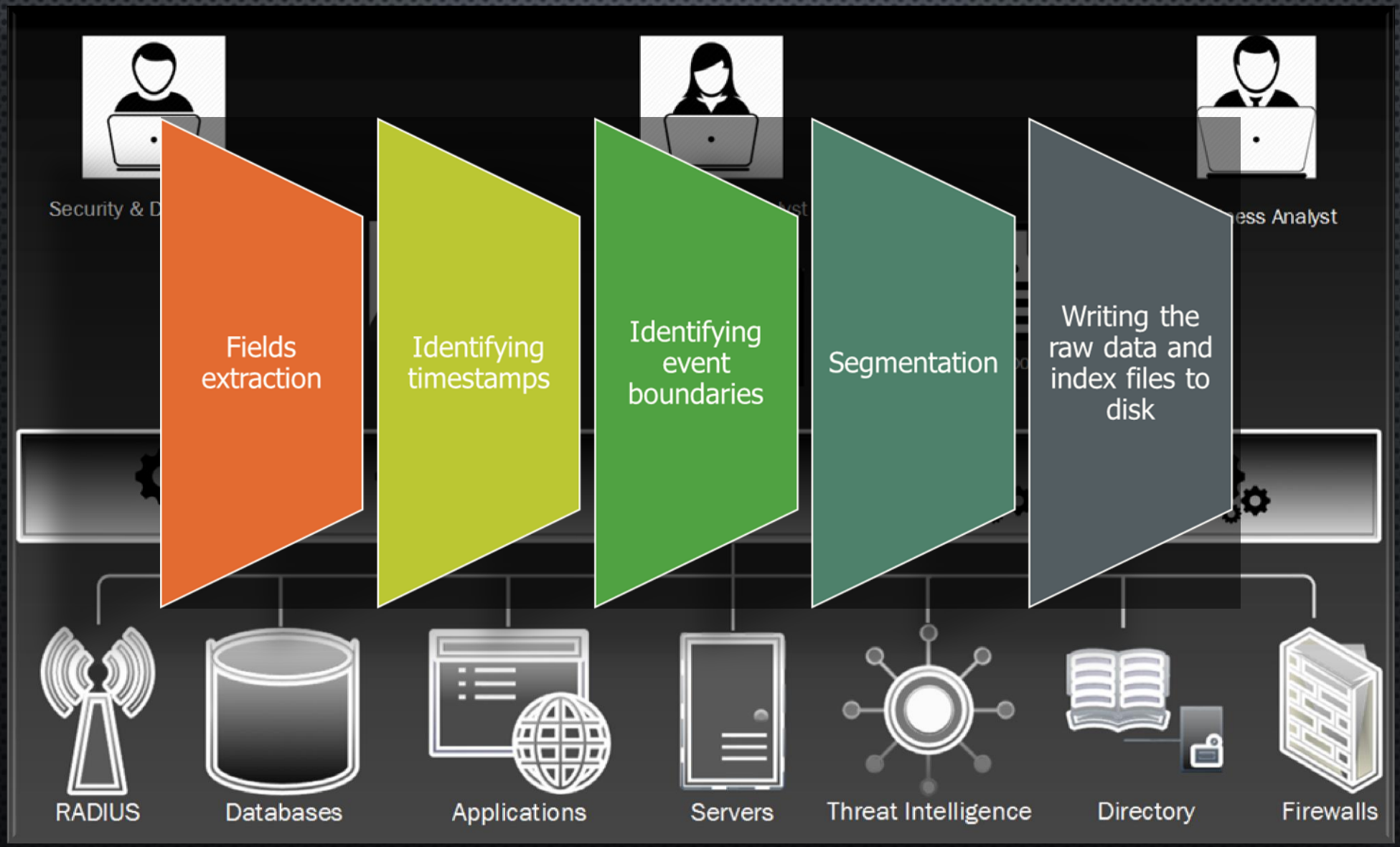




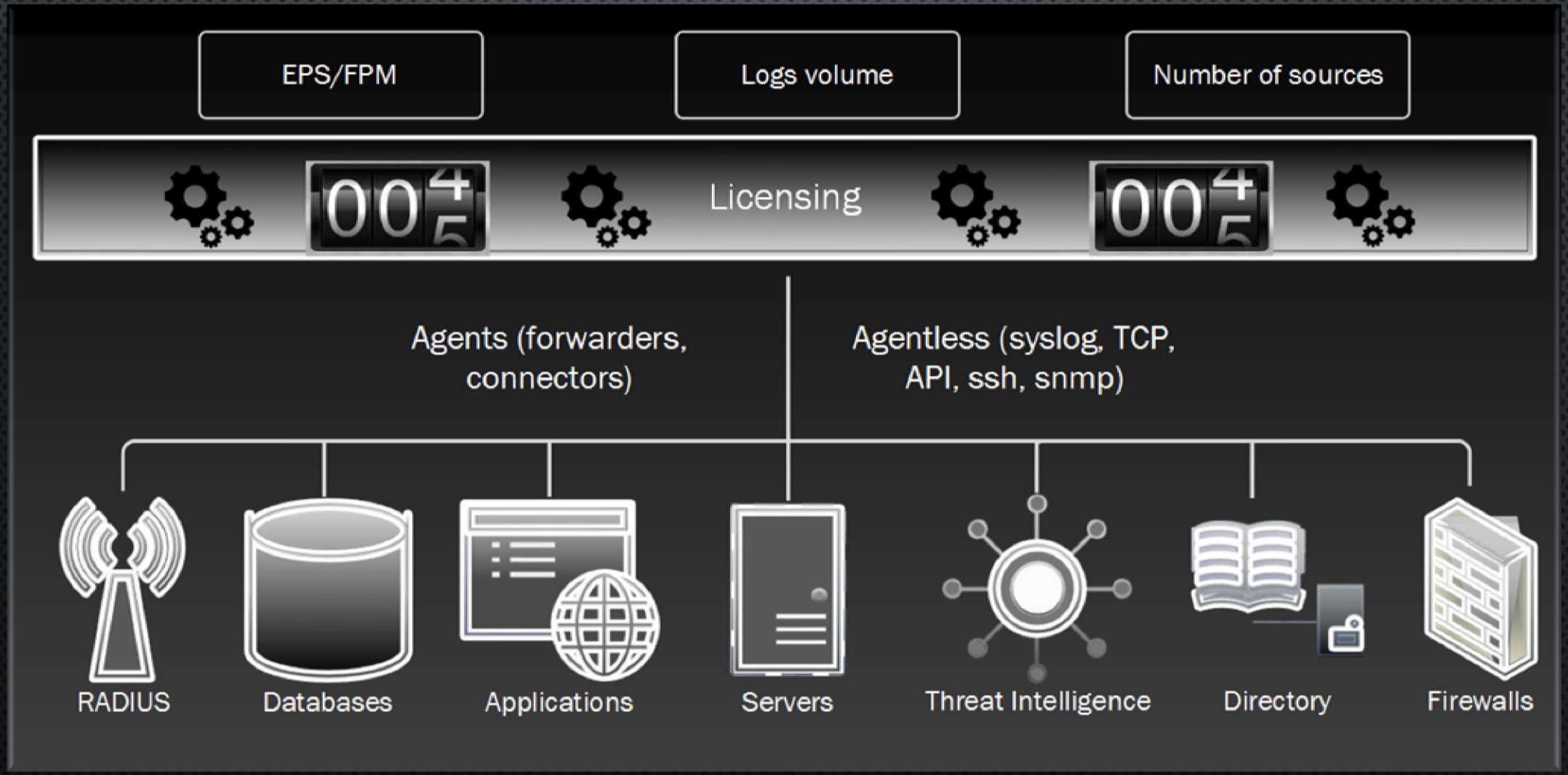
МОЖЛИВОСТІ


Forensic analysis
Data aggregation
Retention
Correlation
Compliance
Alerting
Dashboards

МОЖЛИВОСТІ


Security & D
ess Analyst
Fields extraction
Identifying timestamps
Identifying event boundaries
Segmentation
Writing the raw data and index files to disk
RADIUS
Databases
Applications
Servers
Threat Intelligence
Directory
Firewalls

ЛІЦЕНЗУВАННЯ



MAGIC QUADRANT FOR SIEM

https://en.wikipedia.org/wiki/Magic_Quadrant


Cloud/Hosting Security
algosec
FORTY CLOUD
CloudLock
nclouds Think Automation
CATO NETWORKS
porticor
Data/Information Security
gemalto security to be free
netwrix
Actifile
IMPERVA
Mobile Security
Mobiwol
Skycure
SecuredTouch
CODEPROOF
TRUSTLOOK
Identity/Fraud Security
comsignTRUST
FORTSCALE INTELLIGENT CYBER INSIGHT
hermetic
observe it
SOCURE
Industrial Security
FIRMITAS
Indegy
CyberX
SecureOT The SCADA Security Company
ics
SCADAfence
Security Intelligence/Analytics
eclectic iq
CYFORT
SenseCy Sensing Cyber
IMUBIT
TREND MICRO
sparkcognition
Cycurity Cyberspace Intelligence
Security Technology
Venture Scanner
Purchase landscape report
with all 413 companies
info@venturescanner.com
Risk Assessment/Compliance
WIREDNATION
PivotPoint SECURITY
KERNEL
SAINT
CYBERKOV
CARVE SYSTEMS, LLC
Threat Detection/Mitigation
GuardiCore
Cyberint
perimeterx
cybereason
NOPSEC
FIRELAYERS
SKYBOX SECURITY
Endpoint Security/Firewalls
SentinelOne
BUFFERZONE
MORPHISEC
namogoo
PANDA SECURITY
deepinstinct
Application Security
AMAEYA
waratek
IMMUNIO
AppliCure
PREVOTY
CONTRAST SECURITY
CHECKMARX
Email Security
GreatHorn
CLOUDMASK
SOLEBIT
penta
PineApp
mailcleaner
Brand Protection
brandprotect
NetNames
MASSIVE REPUTATION & PR
i-Sight
OpSec
MarkMonitor PART OF THOMSON REUTERS
ecommnets
Computer Forensics
Cymmetria
MIJO
illusive
ELCOMSOFT PROACTIVE SOFTWARE
DataResolve Technologies
Security Hardware
MAGAL S3 Security, Safety, Site management
FRONTBLADE SYSTEMS
Aerobyte
Cybermoon innovation focused company
SnoopWall RECLAIM YOUR PRIVACY
viprinet


THE PEOPLE

ДЕКІЛЬКА ПРИКЛАДІВ

```
[**] [116:59:1] (snort_decoder): Tcp Window Scale Option found with length
[Priority: 3]
09/29-17:52:43.726408 192.168.198.133:36130 -> 192.168.198.132:1
TCP TTL:40 TOS:0x0 ID:23250 IpLen:20 DgmLen:60
**U*P**F Seq: 0xF842185F  Ack: 0xA5E94B67  Win: 0xFFFF  TcpLen: 40  UrgPtr
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK

[**] [1:1228:7] SCAN nmap XMAS [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/29-17:52:43.726408 192.168.198.133:36130 -> 192.168.198.132:1
TCP TTL:40 TOS:0x0 ID:23250 IpLen:20 DgmLen:60
**U*P**F Seq: 0xF842185F  Ack: 0xA5E94B67  Win: 0xFFFF  TcpLen: 40  UrgPtr
TCP Options (5) => WS: 15 NOP MSS: 265 TS: 4294967295 0 SackOK
[Xref => http://www.whitehats.com/info/IDS30]

[**] [1:2466:7] NETBIOS SMB-DS IPC$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
09/29-17:53:35.987658 192.168.198.1:61290 -> 192.168.198.133:445
TCP TTL:64 TOS:0x0 ID:42494 IpLen:20 DgmLen:130 DF
***AP*** Seq: 0x354E3DEE  Ack: 0xB621EF9B  Win: 0xFFFF  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1184479449 276837
```

Suricata Alerts by Priority

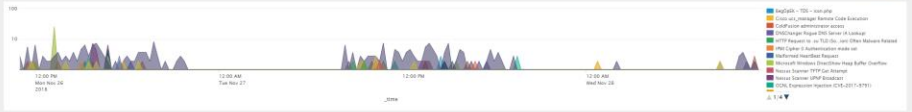
Classification of priority: 1 - critical; 2 - potentionat high; 3 - other; 4 - vulnerable apps; 5 - ssl/tls, password alerts; 6 - mining; 7 - exchange data; 8 - mobile threats; 9 - Adware/PUP 10 - CnC Trackers/IP-Echelon

Critical Signatures	High/Medium Signatures	Low Signatures	"Vuln.Apps" Signatures	"SSL/TLS" Signatures
102 events (15 unique signatures)	44573 events (352 unique signatures)	9601 events (24 unique signatures)	2031 events (2 unique signatures)	347 events (4 unique signatures)

"Mining" Signatures	"Exchange Data" Signatures	"Mobile Threats" Signatures	"Adware\PUP" Signatures	"CnC Trackers/IP-Echelon" Signatures
978 events (5 unique signatures)	0 events (0 unique signatures)	5 events (1 unique signatures)	10 events (3 unique signatures)	73 events (13 unique signatures)

Suricata Alerts by Priority between -24h@h AND now

src	dest	host	signature	src_port	dest_port	id	classification	ruleset	priority	score	severity	revising	earliest	latest	count
52.31.104.117		sensorsa	Win32/InstallCore CnC Activity Win32/InstallCore Gen A Checkin	59121 59134	80	2826896 2830147	A Network Trojan was detected	MALWARE TROJAN	1 10	50	high	Not_Treated Treated	2018-11-28 11:54	2018-11-28 11:57	6
52.31.104.117		sensorsa	Win32/InstallCore CnC Activity Win32/InstallCore Gen A Checkin	62271	80	2826896 2830167	A Network Trojan was detected	MALWARE TROJAN	1 10	50	high	Not_Treated Treated	2018-11-28 08:56	2018-11-28 08:57	7
18.213.157.181	vmpolv-mtw1		Win32/DealPly Checkin	57440	80	2031622	A Network Trojan was detected	MALWARE	1	50	high	Not_Treated	2018-11-28 00:56	2018-11-28 00:56	1
54.201.155.7	vmpolv-dp1		Win32/Adstop Checkin	56723	80	2823965	A Network Trojan was detected	MALWARE	1	50	high	Not_Treated	2018-11-28 13:02	2018-11-28 13:02	1
52.31.104.117	vmpolv-dp1		Win32/InstallCore Gen A Checkin	56722 56757	80	2830167	A Network Trojan was detected	MALWARE	1	50	high	Not_Treated	2018-11-28 13:02	2018-11-28 13:03	2
2.18.12.206	vmpolv-dp1		Win32/Agent.QP Requesting Payload	50719	80	2833374	A Network Trojan was detected	TROJAN	1	50	high	Not_Treated	2018-11-27 16:24	2018-11-27 16:24	1
119.188.108.12	sensorsa		PUP/Sogou A Reporting Checkin via UDP	11116	8000	2812313	A Network Trojan was detected	MALWARE	1	50	high	Not_Treated	2018-11-28 14:03	2018-11-28 14:03	4
113.114.92.64	vmpolv-dp1		Suspicious HTTP Credential Post to IP Address - Possible Successful Phish	49468 49865 50142 50195 50850 51022 51031 51236 51252 51271 51276 51290 51291 51334 51349 51357 51418 51467 52756 52916 52917 53066 53362 53468 53911 54028 54057 56210 58915 60502 60504 60824 61516 61586	8080	2828624	A Network Trojan was detected	INFO	1	0	high	Not_Treated	2018-11-27 16:00	2018-11-28 16:44	46
113.114.92.64	vmpolv-dp1		Suspicious HTTP Credential Post to IP Address - Possible Successful Phish	56883 58933	8080	2828624	A Network Trojan was detected	INFO	1	0	high	Not_Treated	2018-11-27 18:19	2018-11-27 18:40	2
113.114.92.64	vmpolv-dp1		Suspicious HTTP Credential Post to IP Address - Possible Successful Phish	49158 52326 53506 57851 58089 58607 59255 60847 60865 61014	8080	2828624	A Network Trojan was detected	INFO	1	0	high	Not_Treated	2018-11-28 11:40	2018-11-28 16:46	11



Alerts trend by Source for specified Priority between -24h@h AND now

Alerts trend by Destination for specified Priority between -24h@h AND now

IP: 192.168.68.71

Suricata - All events by Priority between -24h@h AND now

No results found.

IP: 192.168.68.71

All detected activity related to defined source (Last 24 hours)

src	user_values	event_count	dest_ip_avg	event_definition	earliest	latest
	TUDELA5 dstop	413		WinEventLog:Security (An account was successfully logged on. Network (), e. connection to shared folder on this computer from elsewhere on network.))	2018-11-27 16:02:28	2018-11-28 16:31:29
	TUDELA5 dstop	324		WinEventLog:Security (An account was successfully logged on)	2018-11-27 16:14:44	2018-11-28 16:58:32
		108		suricata (WinHttp AutoProxy Request wpad.dat Possible BadTunnel)	2018-11-27 16:09:43	2018-11-28 16:31:27
	dstop	80		WinEventLog:Security (The domain controller attempted to validate the credentials for an account)	2018-11-27 19:57:16	2018-11-28 11:57:46
	dstop	80		win_vmp1:wwtt (An account was successfully logged on)	2018-11-27 19:57:17	2018-11-28 11:57:48
		46		suricata (Hola VPN Activity - X-Hola:)	2018-11-27 16:04:11	2018-11-28 16:57:24
	alexnl	31		WinEventLog:Security (A logon was attempted using explicit credentials)	2018-11-27 16:03:35	2018-11-28 16:54:56
		10		pos ()	2018-11-28 13:16:17	2018-11-28 13:16:30
		3		suricata (Known Tor Relay/Router (Not Exit) Node Traffic group 212)	2018-11-27 16:03:53	2018-11-27 17:46:53
		2		suricata (TLS possible TOR SSL traffic)	2018-11-27 16:03:53	2018-11-27 17:46:53

IP: 192.168.68.71

Source identification

nt_host	office	owner	fullname	position	bunit	priority	category	client_level	managed_objects	last_logon	bad_pwd_last	managedBy	room	phone	pwd_last_set
tudela				Junior Security Engineer	CoE - Critical Services	low	offices	1		2018-11-27 09:38:59		osurk	523	7406	2018-11-27 10:11:36

Test

CURRENT RESULTS: MAY 11 AT 10:34 PM

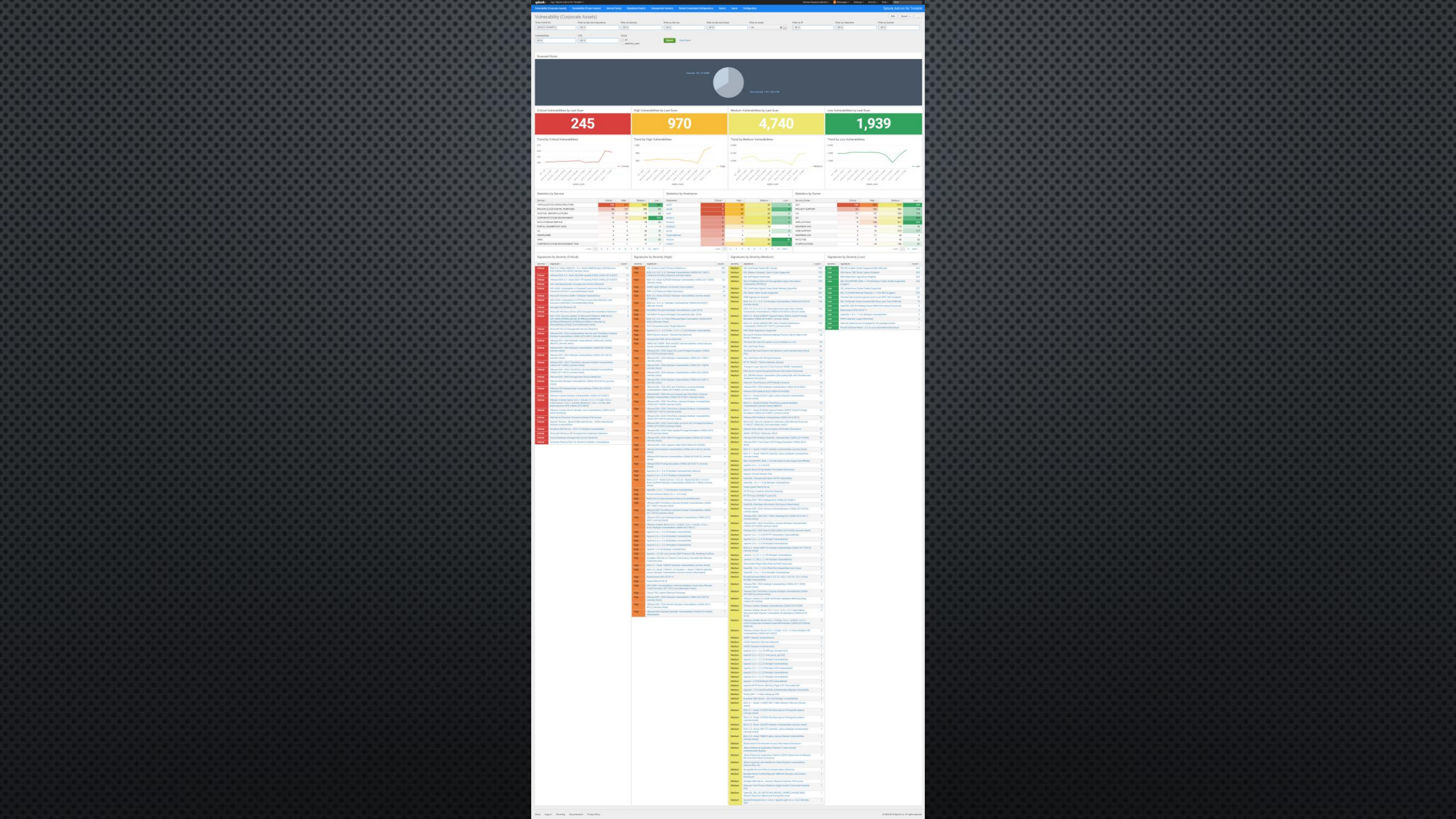
Configure | Audit Trail | Launch | Export | Filter Vulnerabilities

Severity	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE…	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201…	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA…	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20…	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-…	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libldb / li…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : nss-util (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : samba (CES…	CentOS Local Security Checks	1

Host Details

IP:	192.168.56.102
DNS:	st91.i
MAC:	08:00:27:db:3e:a2
OS:	Linux Kernel 3.10.0-327.4.5.el7.x86_64 on CentOS Linux release 7.2.1511 (Core)
Start:	May 11 at 10:34 PM
End:	May 11 at 10:39 PM
Elapsed:	6 minutes
KB:	Download

Vulnerabilities


Vulnerability (Corporate Assets)
Scanned Hosts
Critical Vulnerabilities by Last Scan
245
High Vulnerabilities by Last Scan
970
Medium Vulnerabilities by Last Scan
4,740
Low Vulnerabilities by Last Scan
1,939
Trend by Critical Vulnerabilities
Trend by High Vulnerabilities
Trend by Medium Vulnerabilities
Trend by Low Vulnerabilities
Statistics by Service
Statistics by Hostname
Statistics by Owner
Signatures by Severity (Critical)
Signatures by Severity (High)
Signatures by Severity (Medium)
Signatures by Severity (Low)

2. Feature Engineering and Selection

Edit | Export | ...

Feature Engineering

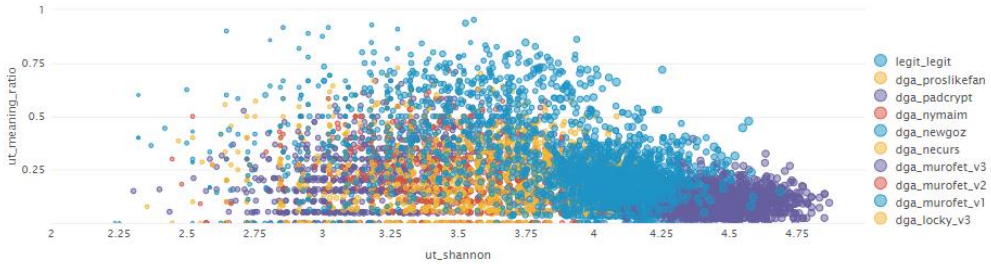
Detecting DGAs may require additional features that are not present in the raw table of domain names. Additional features can be any meaningful additional information that help to characterize the dataset with regards to the analytics goal, ideally in a very distinct manner. In this case we derive features from the pure domain name strings that allow to shape indicators of a generated domain name. As part of data preprocessing we save the computed results after using some SPL and methods from the URL Toolbox App:

Domain dataset enriched with features

domain	class	subclass	ut_consonant_ratio	ut_digit_ratio	ut_domain_length	ut_meaning_ratio	ut_shannon	ut_vowel_ratio	PC_1	PC_2	PC_3
pmnwoqwxuwgujnlbusofytg.ru	dga	murofet_v1	0.800	0.000	26.000	0.269	3.979	0.231	0.057	0.114	0.111
eiopcinmw.ru	dga	locky_v2	0.600	0.000	12.000	0.417	3.418	0.417	0.047	0.115	0.115
ktyrsqsgjl.org	dga	nymaim	0.900	0.000	14.000	0.143	3.379	0.071	0.155	0.728	-0.347
kporwilikmotyds.com	dga	murofet_v2	0.700	0.000	19.000	0.158	3.682	0.263	-0.326	-0.019	-0.150
xqemvapturim.sh	dga	necurs	0.700	0.000	15.000	0.267	3.774	0.267	0.024	0.041	0.044
pzvqxtgb.com	dga	nymaim	0.900	0.000	12.000	0.000	3.585	0.083	-0.428	-0.167	-0.093
xgsqljmoypxbflety.net	dga	fobber	0.900	0.000	21.000	0.286	3.916	0.143	0.569	-0.324	-0.095
wtblfvpjomijxsgmfusgcinr.com	dga	murofet_v1	0.800	0.000	28.000	0.179	4.138	0.179	-0.425	-0.162	-0.085
sptdsbhhrvfsmsm.in	dga	necurs	0.900	0.000	18.000	0.222	3.503	0.056	0.032	0.080	0.089
bnxnjmsuhiyvoclzi.net	dga	fobber	0.800	0.000	21.000	0.381	4.071	0.238	0.538	-0.289	-0.078

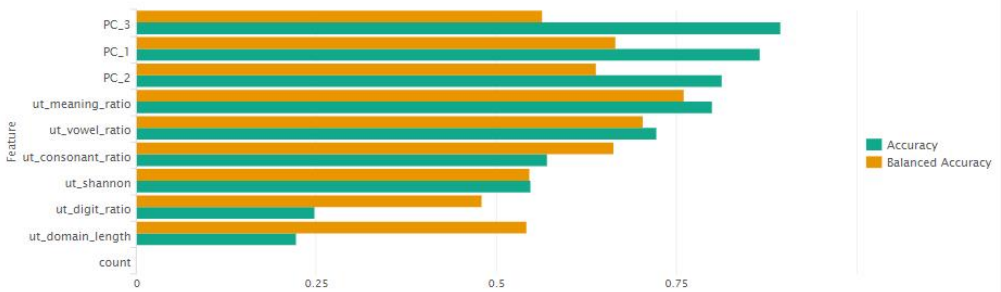
« prev 1 2 3 4 5 6 7 8 9 10 next »

Distribution of classes depending on example feature combination

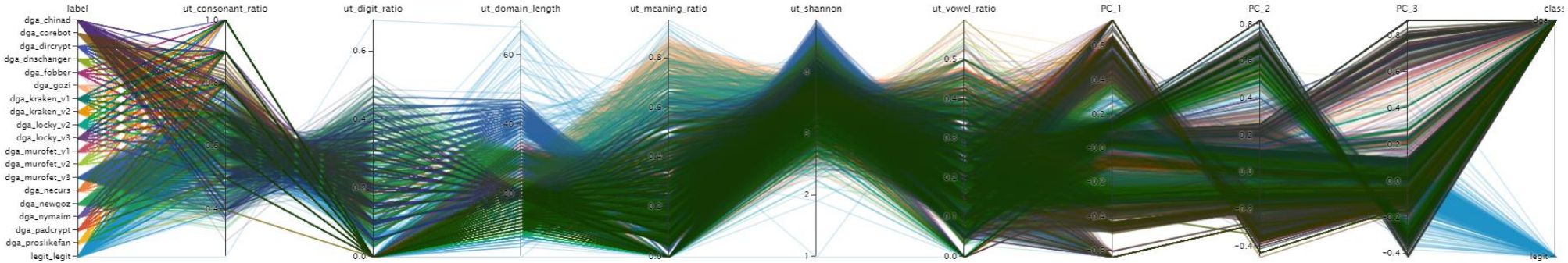


These results may be truncated. This visualization is configured to display a maximum of 10000 results per series, and that limit has been reached. Learn More

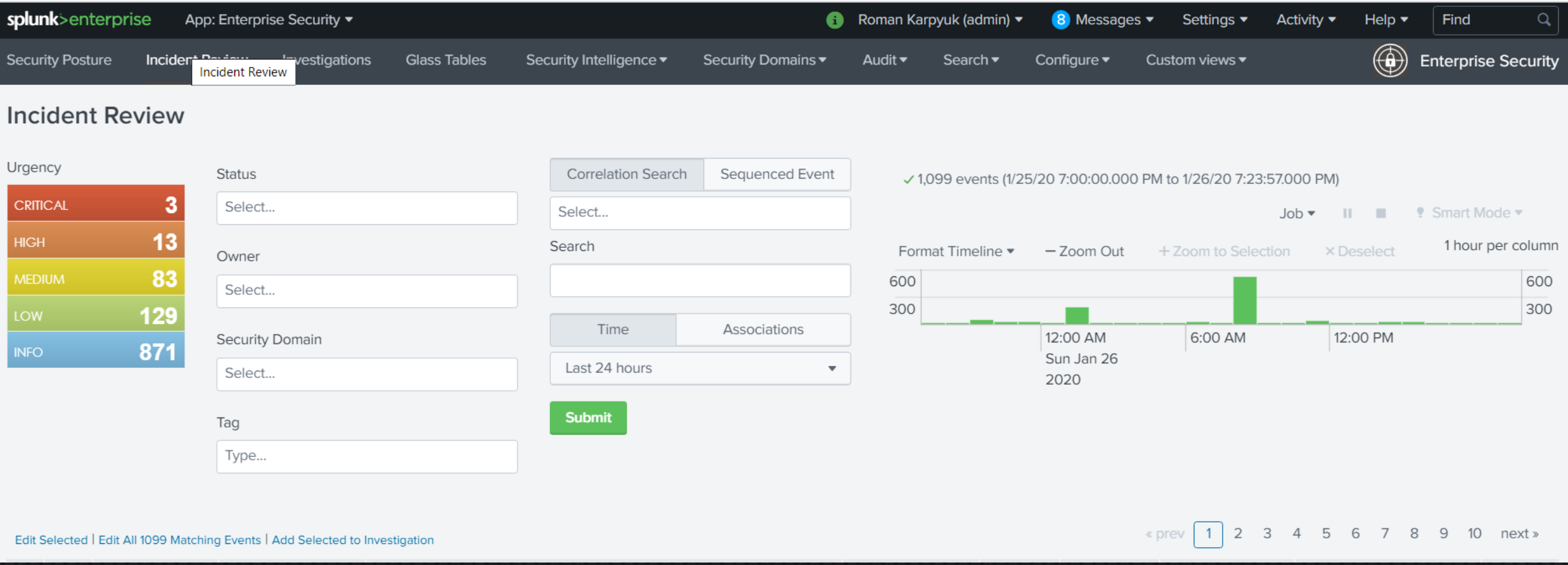
Identify useful features for classification with the analyzefields command



Parallel coordinate chart of classes and top features



Currently showing 19000 / 19000 datapoints | Clear filters


splunk>enterprise
App: Enterprise Security
Roman Karpyuk (admin)
8 Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Investigations
Glass Tables
Security Intelligence
Security Domains
Audit
Search
Configure
Custom views
Enterprise Security
Incident Review
Incident Review
Urgency
CRITICAL 3
HIGH 13
MEDIUM 83
LOW 129
INFO 871
Status
Select...
Owner
Select...
Security Domain
Select...
Tag
Type...
Correlation Search
Sequenced Event
Select...
Search
Time
Associations
Last 24 hours
Submit
✓ 1,099 events (1/25/20 7:00:00.000 PM to 1/26/20 7:23:57.000 PM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
600
300
600
300
12:00 AM
Sun Jan 26
2020
6:00 AM
12:00 PM
Edit Selected | Edit All 1099 Matching Events | Add Selected to Investigation
« prev
1
2
3
4
5
6
7
8
9
10
next »

i	Time	Security Domain	Title	Urgency	Status	Owner	Source	User	Actions
>	1/24/20 2:13:22.000 PM	Network	[ML] Finds Anomaly of IDS Event per "Likely TDS redirecting to exploit kit" for Last Hour	Medium	In Progress				
>	1/24/20 2:10:16.000 PM	Threat	Threat Activity Detected (51.75.52.127 --> ,. Collection: sans|51.75.52.0-51.75.52.255	Medium	New	unassigned			
>	1/24/20 2:09:41.000 PM	Access	[ML] Anomaly Failed Logins with One or More Success on Source - " :" for Last Hour	Medium	New	unassigned			
>	1/24/20 2:09:41.000 PM	Access	[ML] Anomaly Failed Logins with One or More Success on Source - for Last Hour	Medium	New	unassigned			
>	1/24/20 2:09:41.000 PM	Access	[ML] Anomaly Failed Logins with One or More Success on Source - " for Last Hour	High	In Progress				
>	1/24/20 1:14:23.000 PM	Network	[ML] Finds Anomaly of IDS Events on Host " " for Last Hour	Medium	In Progress				
>	1/24/20 1:10:25.000 PM	Threat	Threat Activity Detected (101.248.141.65 -->). Collection: emerging_threats_ip_blocklist|101.248.0.0/15	Medium	New	unassigned			
>	1/24/20 1:10:22.000 PM	Threat	Threat Activity Detected (101.249.0.108 --> . Collection: emerging_threats_ip_blocklist|101.248.0.0/15	Medium	New	unassigned			
>	1/24/20 1:10:22.000 PM	Threat	Threat Activity Detected (101.249.18.213 -->). Collection: emerging_threats_ip_blocklist|101.248.0.0/15	Medium	New	unassigned			
>	1/24/20 1:10:22.000 PM	Threat	Threat Activity Detected (101.249.37.130 --> ,. Collection: emerging_threats_ip_blocklist|101.248.0.0/15	Medium	New	unassigned			
>	1/24/20 1:00:55.000 PM	Access	Account Deleted by ykharchpr	Unknown	New	unassigned			
>	1/24/20								

Дякую за Увагу