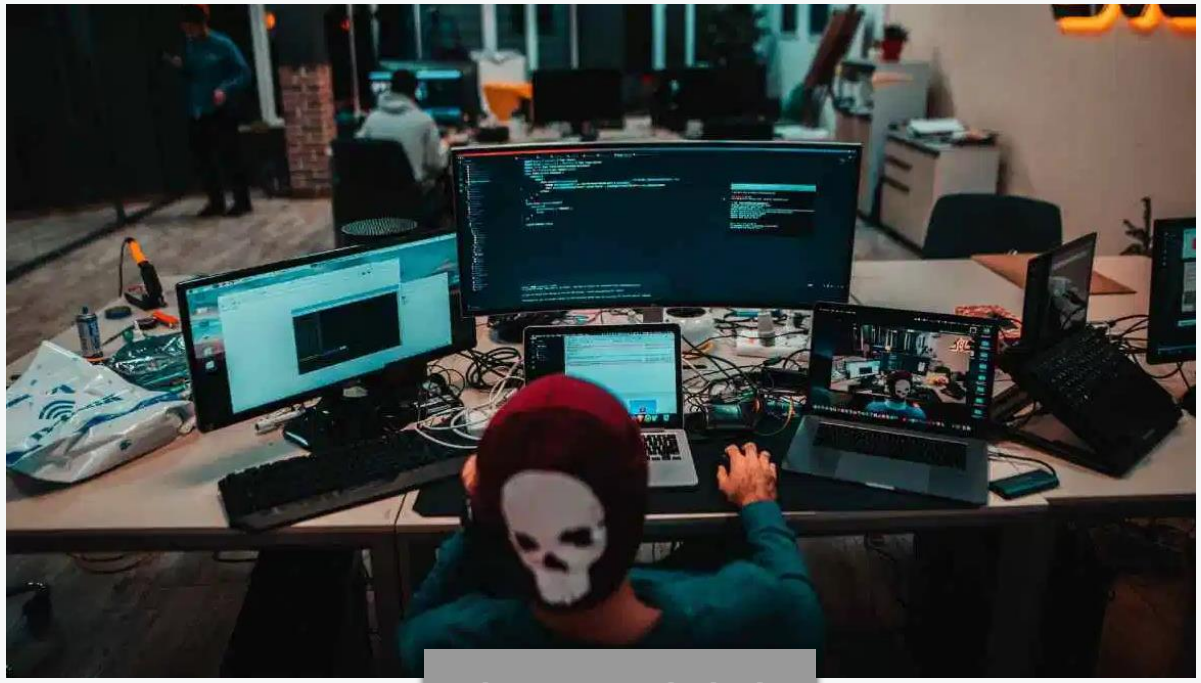


OPEN SOC

Security High School

#SHS2k23

BEEHACKERS

Ramón Salado

Analista de Seguridad [CEO BeeHackers]

ex Administración General del Estado

Docente Másteres | FPO | FP | Certificaciones

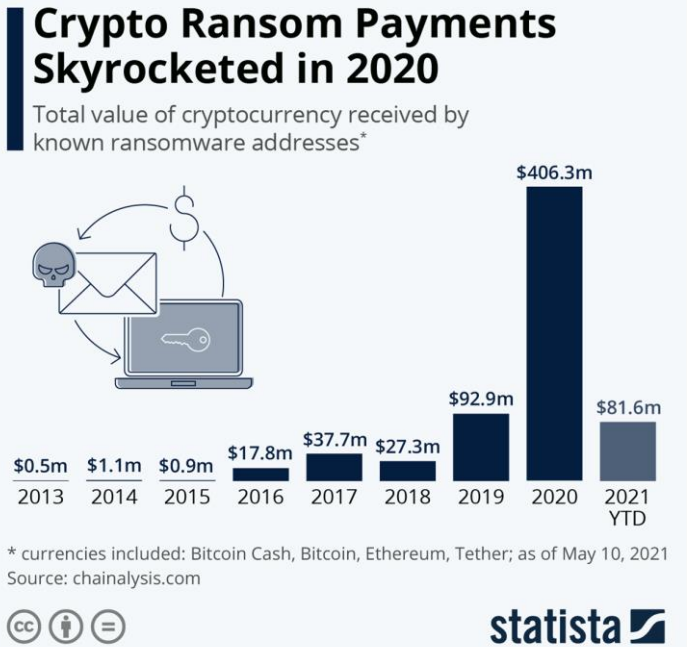
CoLeader OWASP Sevilla

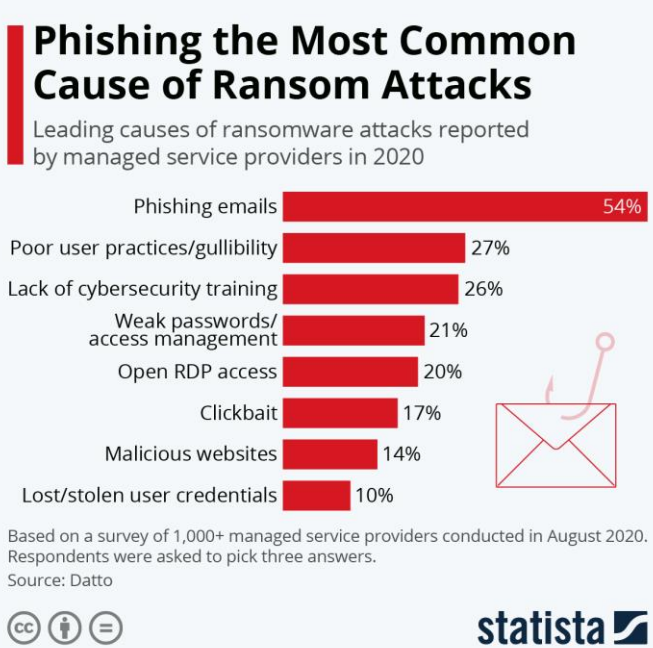
13 años de experiencia en Sistemas y Seguridad

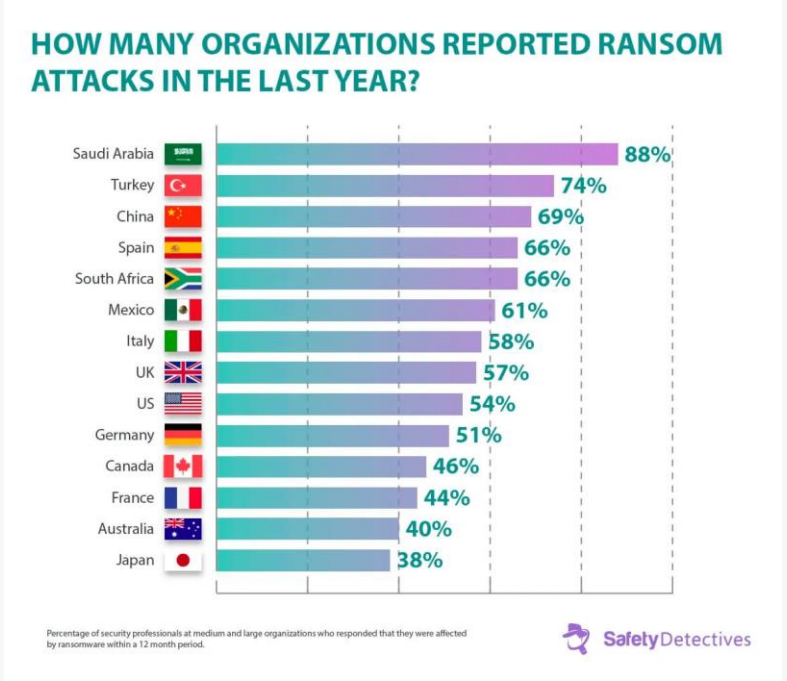
Libros, Publicaciones, Conferencias

Estado de la CiberSeguridad

Estado de la CiberSeguridad



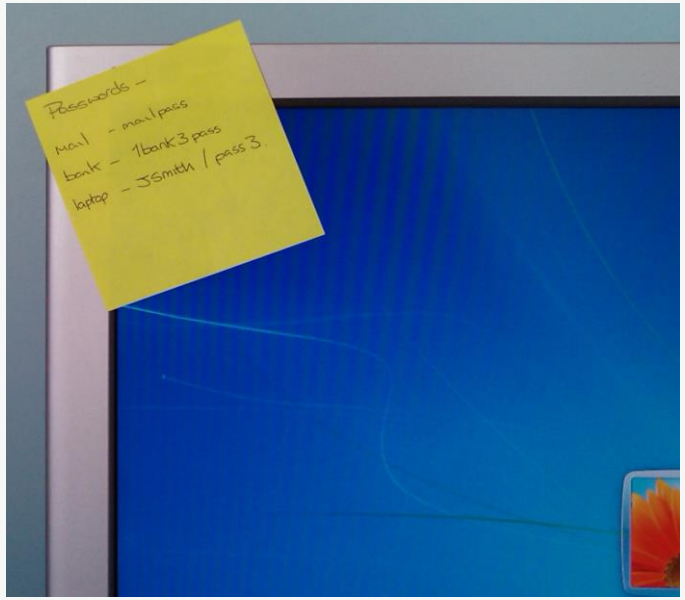




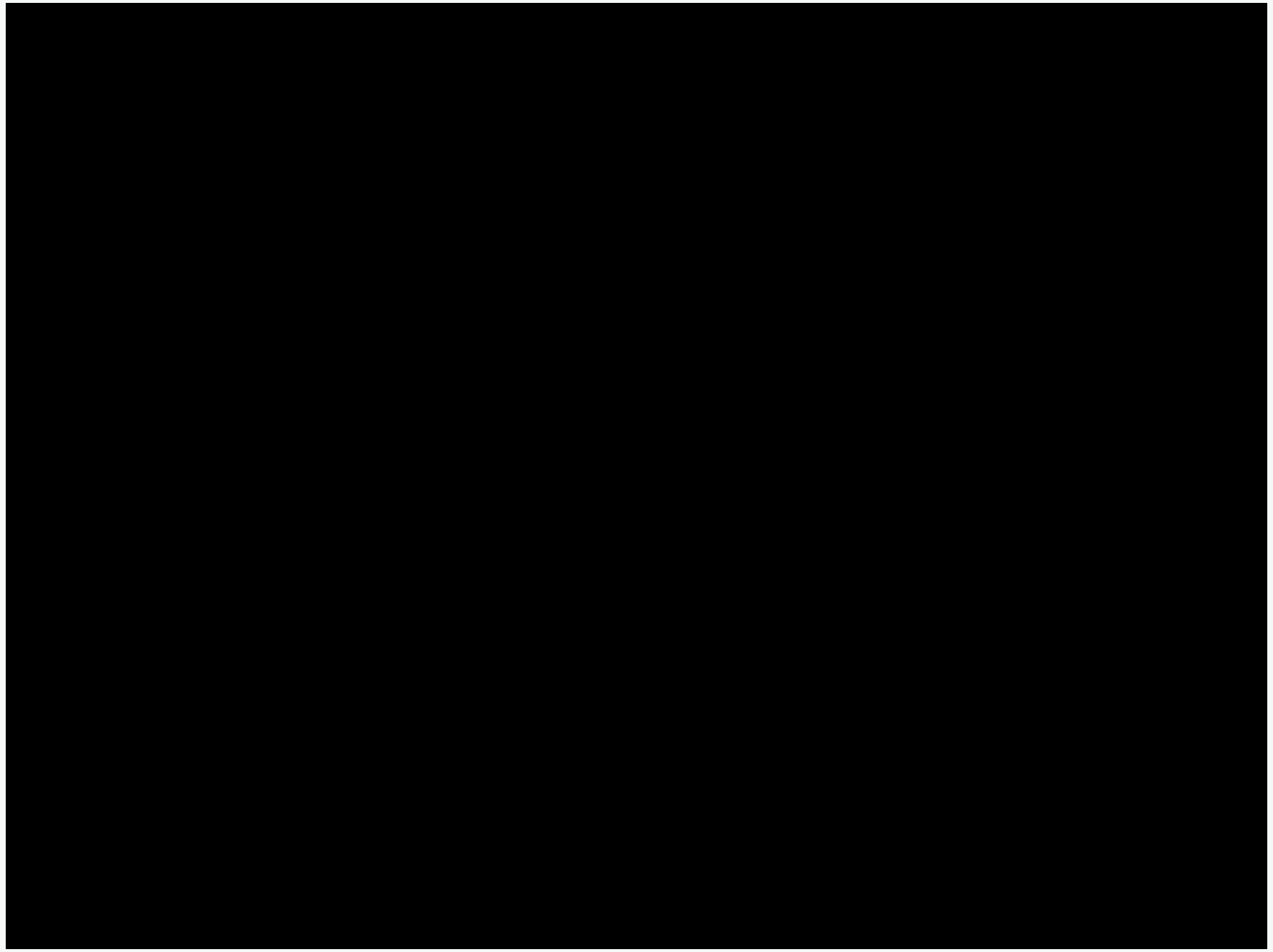
Estado de la CiberSeguridad

19.194.622	3.308
IMPACTOS SOBRE CLIENTES EN 30 DÍAS	IMPACTOS SOBRE ROUTER DOMÉSTICO EN 30 DÍAS

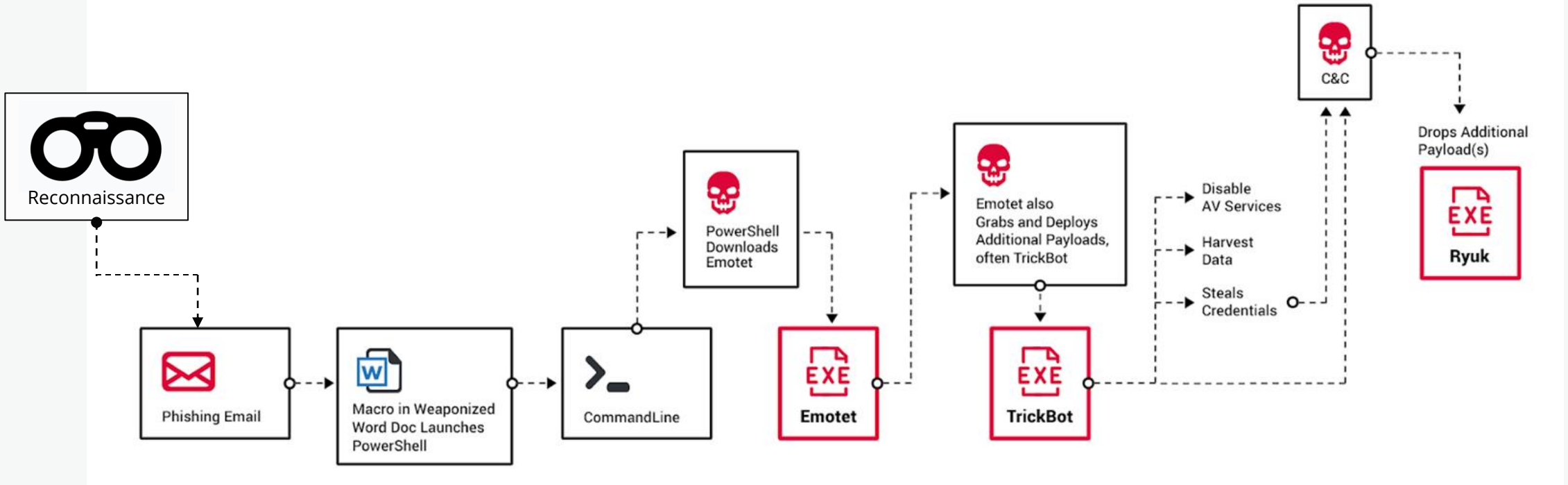
Estado de la CiberSeguridad

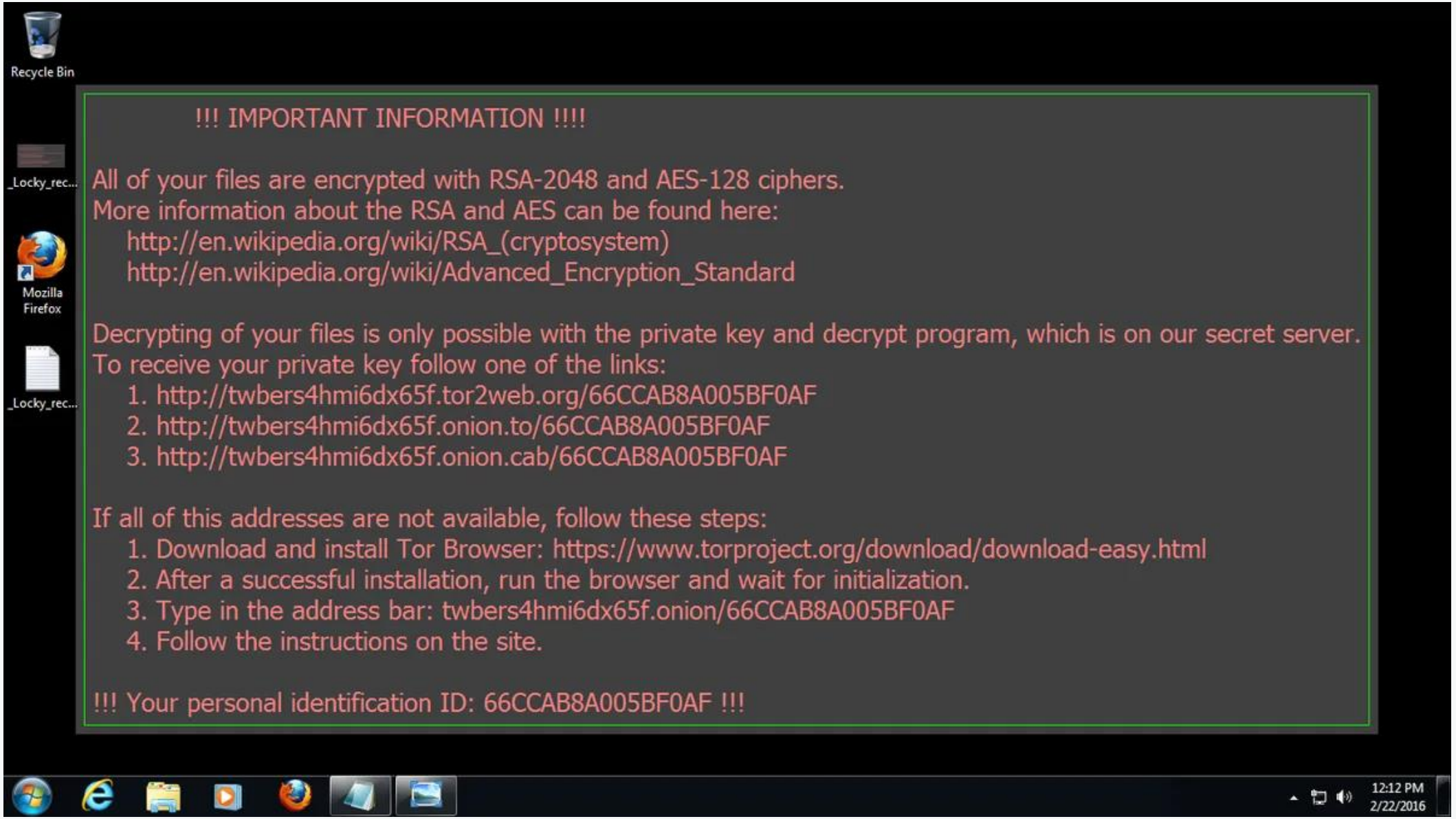


Estado de la CiberSeguridad

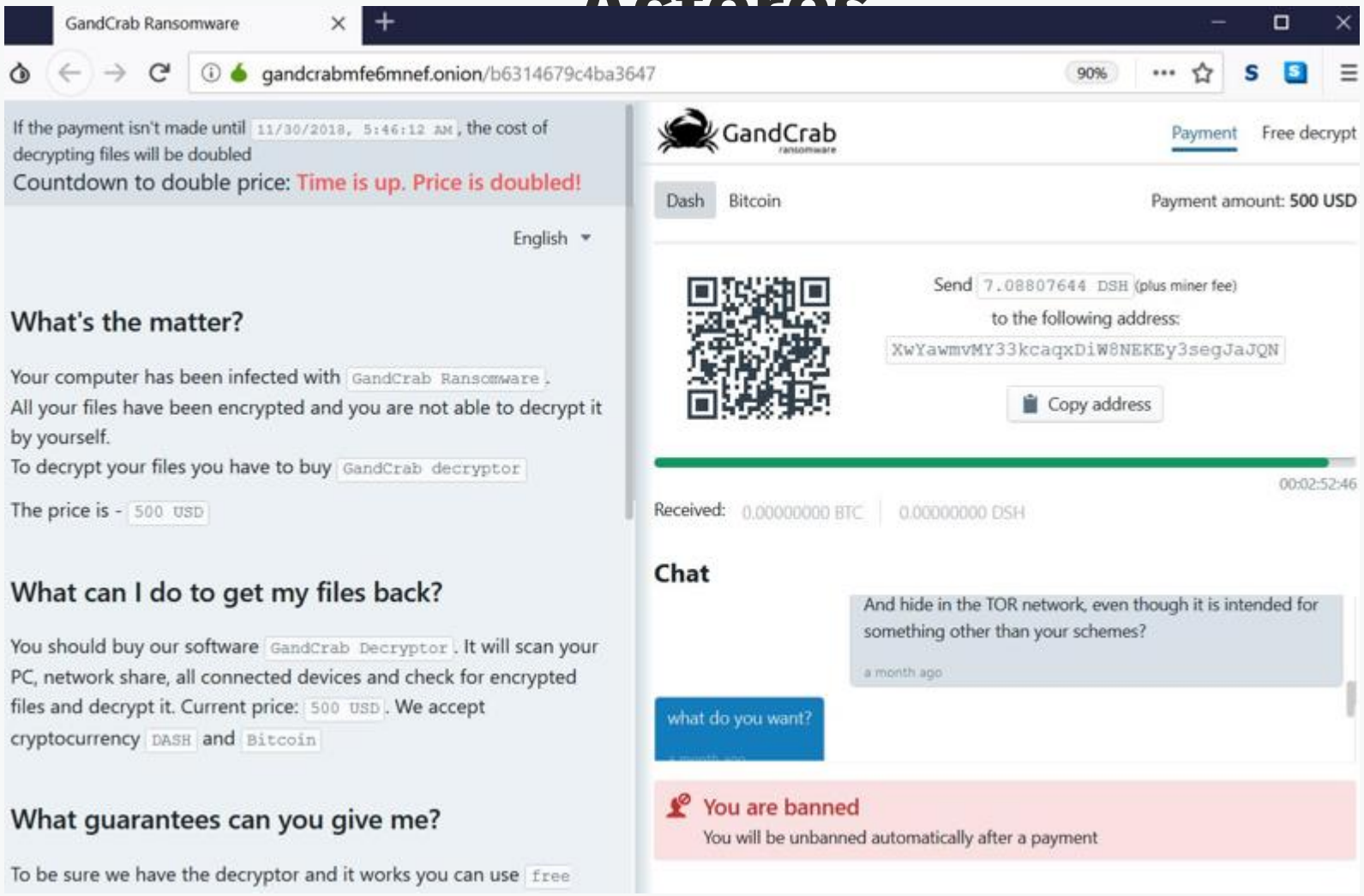


Actores


Reconnaissance
Phishing Email
Macro in Weaponized Word Doc Launches PowerShell
CommandLine
PowerShell Downloads Emotet
Emotet
Emotet also Grabs and Deploys Additional Payloads, often TrickBot
TrickBot
Disable AV Services
Harvest Data
Steals Credentials
C&C
Drops Additional Payload(s)
Ryuk
Día -97
Día D

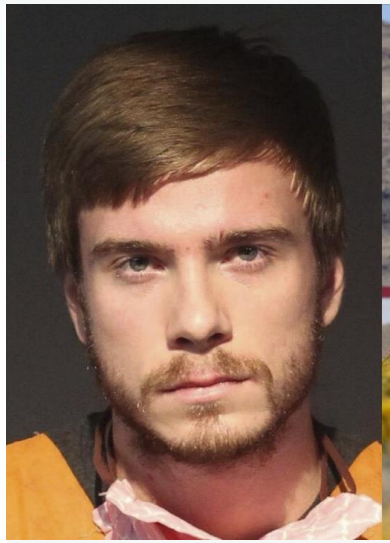

Recycle Bin
_Locky_rec...
Mozilla Firefox
_Locky_rec...
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://twbers4hmi6dx65f.tor2web.org/66CCAB8A005BF0AF
2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: twbers4hmi6dx65f.onion/66CCAB8A005BF0AF
4. Follow the instructions on the site.
!!! Your personal identification ID: 66CCAB8A005BF0AF !!!
12:12 PM
2/22/2016

Actores

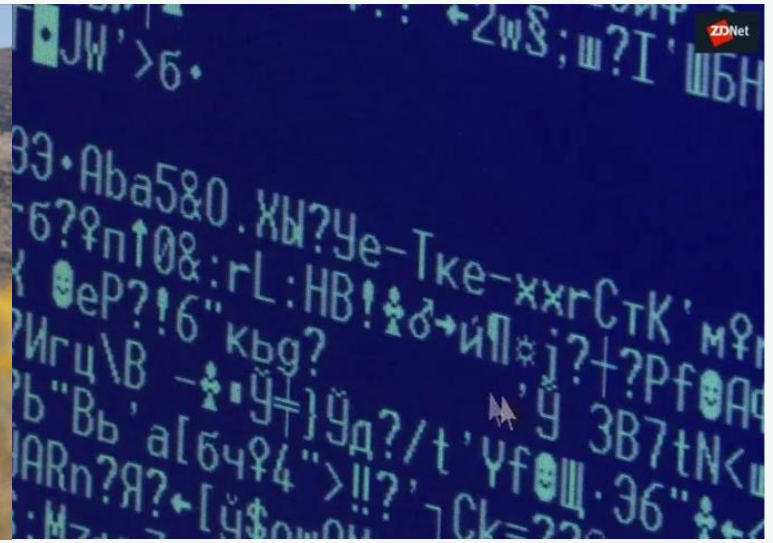

GandCrab Ransomware
gandcrabmfe6mnef.onion/b6314679c4ba3647
90%
If the payment isn't made until 11/30/2018, 5:46:12 AM, the cost of decrypting files will be doubled
Countdown to double price: Time is up. Price is doubled!
English
What's the matter?
Your computer has been infected with GandCrab Ransomware.
All your files have been encrypted and you are not able to decrypt it by yourself.
To decrypt your files you have to buy GandCrab decryptor
The price is - 500 USD
What can I do to get my files back?
You should buy our software GandCrab Decryptor. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt it. Current price: 500 USD. We accept cryptocurrency DASH and Bitcoin
What guarantees can you give me?
To be sure we have the decryptor and it works you can use free
GandCrab
Payment
Free decrypt
Dash
Bitcoin
Payment amount: 500 USD
Send 7.08807644 DSH (plus miner fee)
to the following address:
XwYawmvMY33kcaqxDiW8NEKEy3segJaJQN
Copy address
00:02:52:46
Received: 0.00000000 BTC 0.00000000 DSH
Chat
And hide in the TOR network, even though it is intended for something other than your schemes?
a month ago
what do you want?
You are banned
You will be unbanned automatically after a payment

Actores

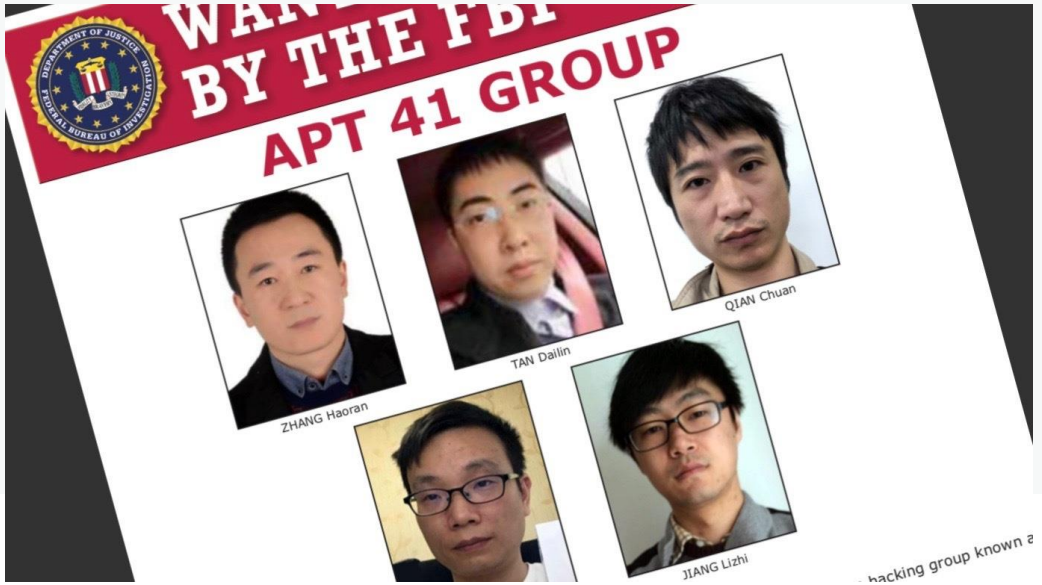

WANTED
BY THE FBI
MAKSIM VIKTOROVICH YAKUBETS
Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud;
Intentional Damage to a Computer
DESCRIPTION
Aliases: Maksim Yakubets, "AQUA"
Date(s) of Birth Used: May 20, 1987
Place of Birth: Ukraine
Hair: Brown
Eyes: Brown
Height: Approximately 5'10"
Weight: Approximately 170 pounds
Sex: Male
Race: White
Citizenship: Russian
REWARD
The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.




TESLA
Egor Igorevich Kriuchkov


ZDNet

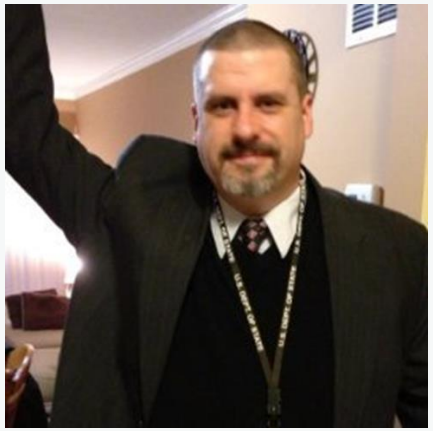

ПРОДУКТЫ


APT 41 GROUP
ZHANG Haoran
TAN Dailin
QIAN Chuan
JIANG Lizhi

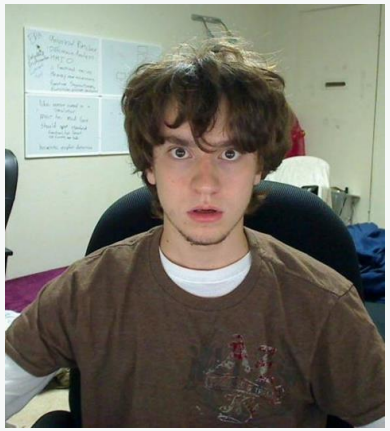

Everybody needs a hacker

Hackers

Barnaby Jack



Kyle Lovett



George Hotz

Steve Wozniak

TerraVisión

Sector

English | Contacto | Tu Ayuda en Ciberseguridad | Agenda | Sala de prensa | Encuestas | Mapa web

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protege tu empresa | Eventos | Otras actividades | Conoce INCIBE | España Digital 2026

Inicio / Sala Prensa / Notas Prensa / La demanda de talento en ciberseguridad doblará a la oferta en 2024, hasta alcanzar la cifra de más de 83.000 profesionales necesarios en el sector

- Notas de prensa
- Boletines
- 10 Aniversario INCIBE

La demanda de talento en ciberseguridad doblará a la oferta en 2024, hasta alcanzar la cifra de más de 83.000 profesionales necesarios en el sector

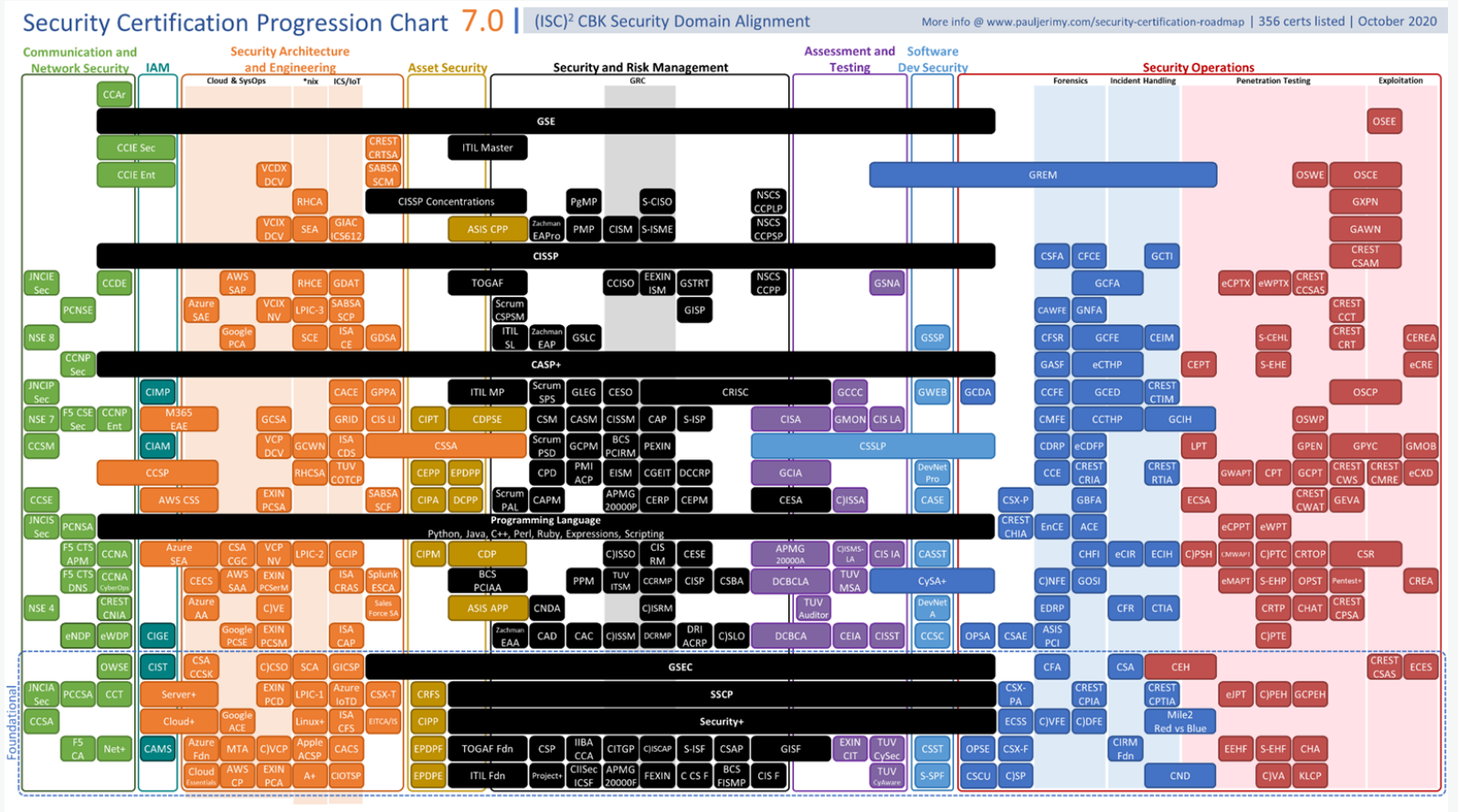
Publicado el 01/03/2022

Únicamente 2 de cada 10 personas empleadas en ciberseguridad readaptan su carrera laboral desde otras áreas profesionales.

Sector


YELLOW TEAM
ORANGE TEAM
RED TEAM
PURPLE TEAM
BLUE TEAM
GREEN TEAM
Software coders and Architects "The Builders"
Facilitate Interaction and Education
Offensive Security "The Breakers"
Integrating defensive tactics with offensive results
Defensive Security "The Defenders"
Enhance security automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management

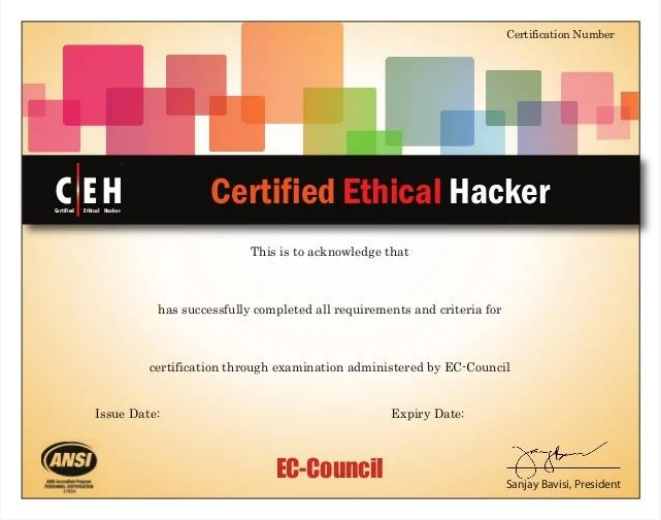
Sector


Security Certification Progression Chart 7.0
(ISC)² CBK Security Domain Alignment
More info @ www.pauljerimy.com/security-certification-roadmap | 356 certs listed | October 2020
Communication and Network Security
IAM
Security Architecture and Engineering
Cloud & SysOps
*nix
ICS/IoT
Asset Security
Security and Risk Management
GRC
Assessment and Testing
Software Dev Security
Security Operations
Forensics
Incident Handling
Penetration Testing
Exploitation
Foundational
GSE
CISSP
CASP+
Programming Language
Python, Java, C++, Perl, Ruby, Expressions, Scripting
GSEC
SSCP
Security+

Sector


CERTIFICATE OF COMPLETION
PROUDLY PRESENTED TO
John Doe
eJPT
eLearnSecurity
Junior Penetration Tester
eJPT v1.0
EXAM VERSION
05/25/2020
DATE
1234567
CERTIFICATION ID
Richard McLain PRESIDENT
eJPT
eLearn Security


Burp Suite Certified PRACTITIONER
Certificate:
Burp Suite Certified Practitioner
Name:
Astik Rawat
Issue date:
13 March 2022
Valid until:
13 March 2027
Token:
7991EF7CA8216513
Burp Suite Certified Practitioner
This certification, created by PortSwigger's Web Security Academy, demonstrates that I have the ability to:
Detect and prove the full business impact of a wide range of common web vulnerabilities.
Adapt attack methods to bypass broken defences, using knowledge of fundamental web technologies.
Quickly identify weak points within an attack surface, and perform out-of-band attacks to attack them.
PortSwigger are the creators of the Web Security Academy and Burp Suite, the world's leading toolkit for web security testing.
PortSwigger
Web Security Academy
Burp Suite


Certification Number
C|EH
Certified Ethical Hacker
This is to acknowledge that
has successfully completed all requirements and criteria for
certification through examination administered by EC-Council
Issue Date:
Expiry Date:
ANSI
EC-Council
Sanjay Bavisi, President

Sector

OWASP Open Web Application Security Project | Sevilla CHAPTER

HACK & BEERS

Sector


HACKTHEBOX


10 10
1110
0101 01
01 010
01
Try
Hack
Me


VULNHUB
VULNERABLE BY DESIGN


LETSDEFEND
BLUE TEAM TRAINING PLATFORM


CyberDefenders
Less Hype, More Value
cyberdefenders.org

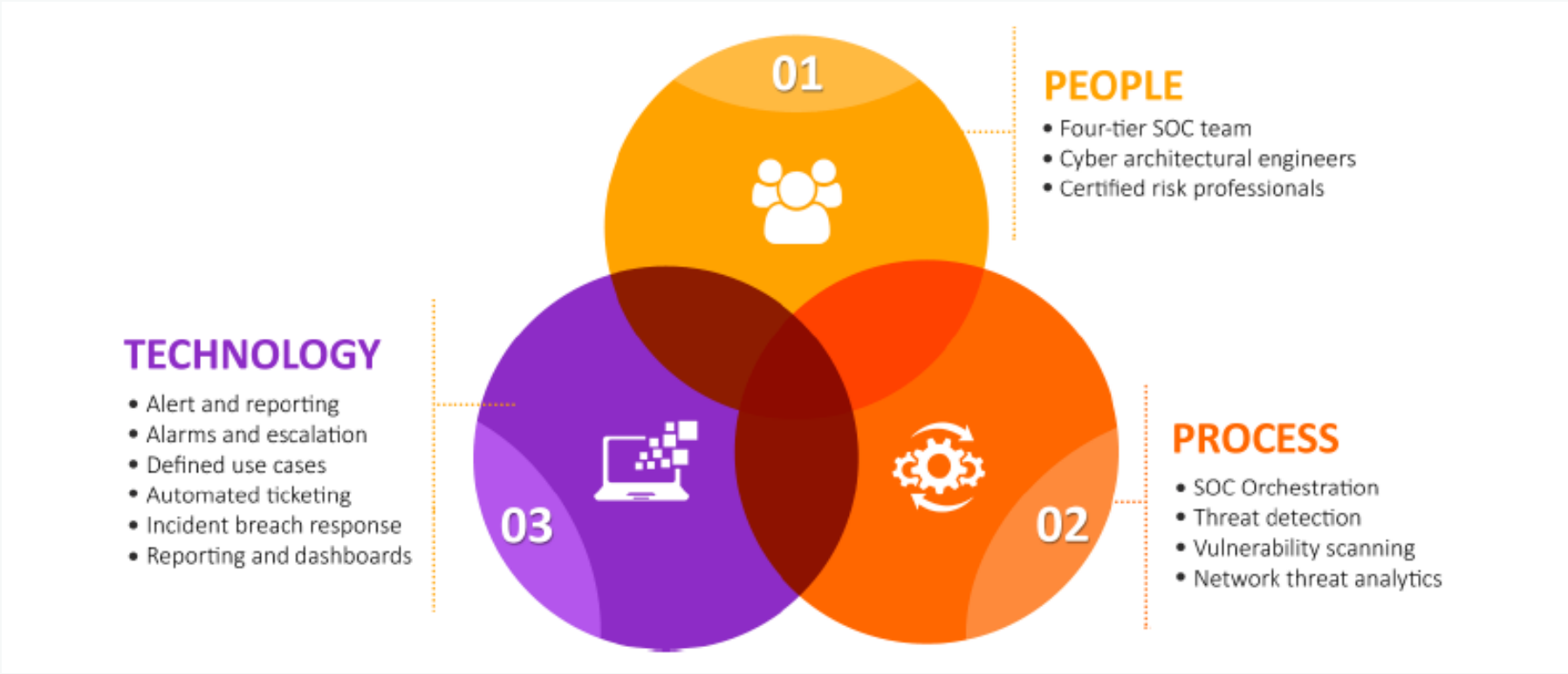

BLUE TEAM
LABS ONLINE
Powered by Security Blue Team


OWASP
JUICE SHOP
PROJECT

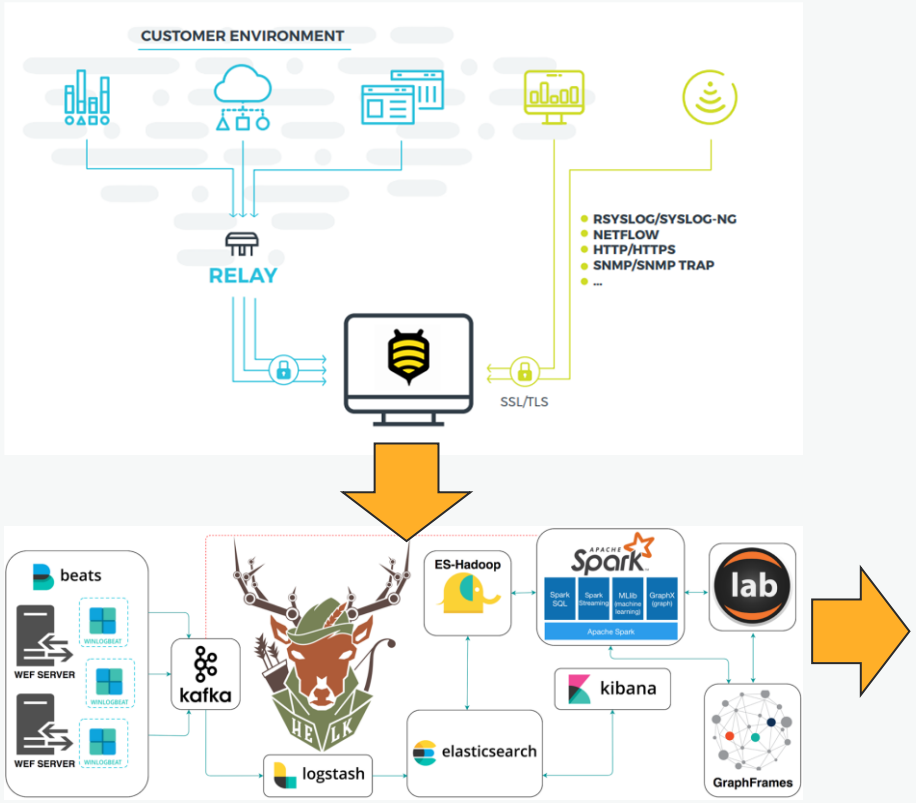

bWAPP
an extremely buggy we

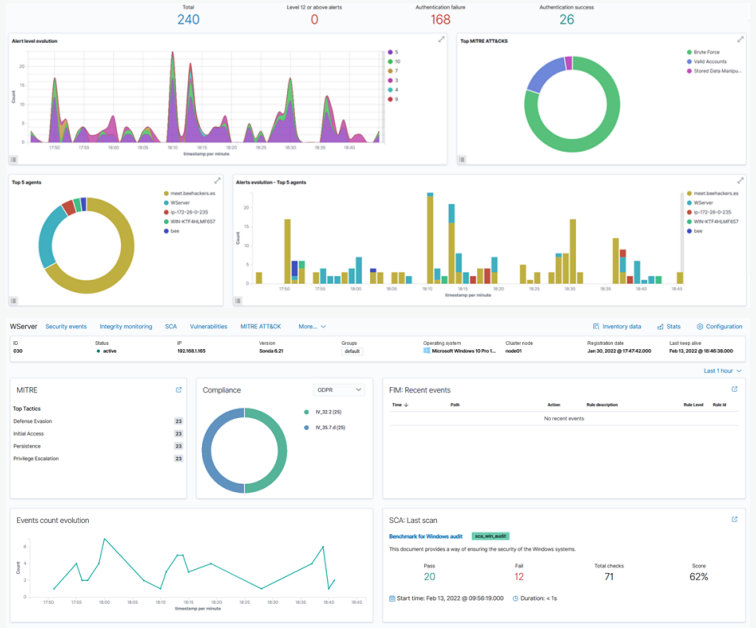

metasploitable2

SOC

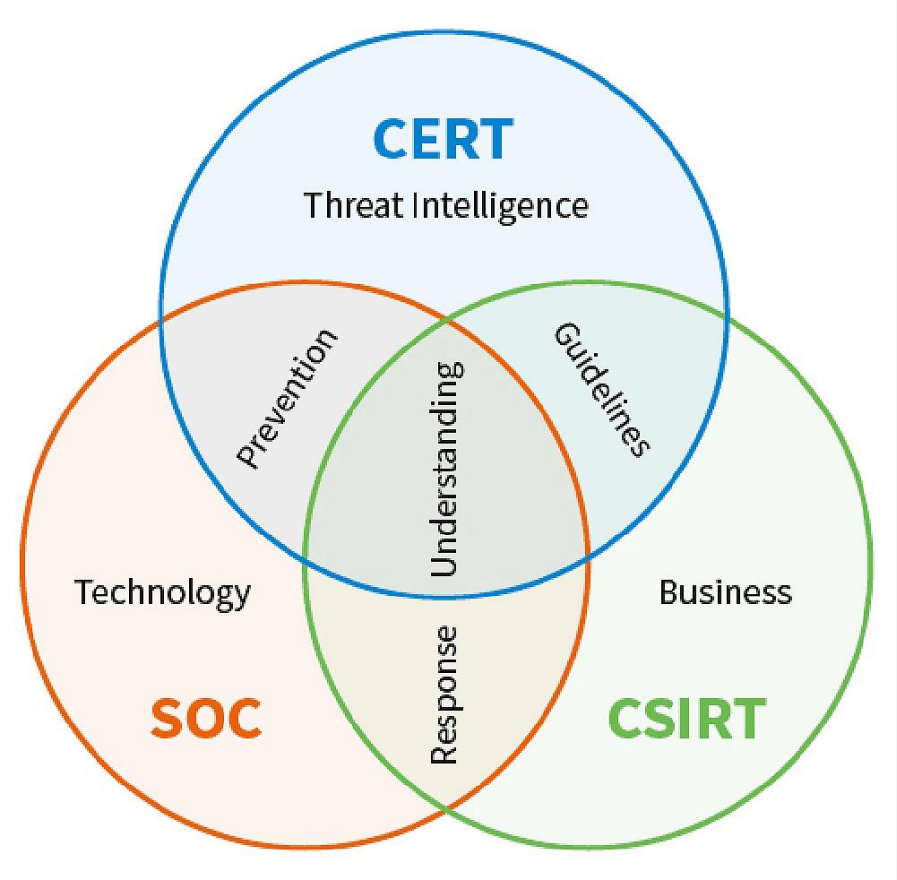

01
PEOPLE
• Four-tier SOC team
• Cyber architectural engineers
• Certified risk professionals
TECHNOLOGY
• Alert and reporting
• Alarms and escalation
• Defined use cases
• Automated ticketing
• Incident breach response
• Reporting and dashboards
03
02
PROCESS
• SOC Orchestration
• Threat detection
• Vulnerability scanning
• Network threat analytics

SIEM


CUSTOMER ENVIRONMENT
RELAY
RSYSLOG/SYSLOG-NG
NETFLOW
HTTP/HTTPS
SNMP/SNMP TRAP
...
SSL/TLS
beats
WEF SERVER
WEF SERVER
WINLOGBEAT
kafka
logstash
ES-Hadoop
elasticsearch
Spark
Apache Spark
lab
kibana
GraphFrames


Total
240
Level 12 or above alerts
0
Authentication failure
168
Authentication success
26
MITRE
Compliance
FIM: Recent events
Events count evolution
SCA: Last scan

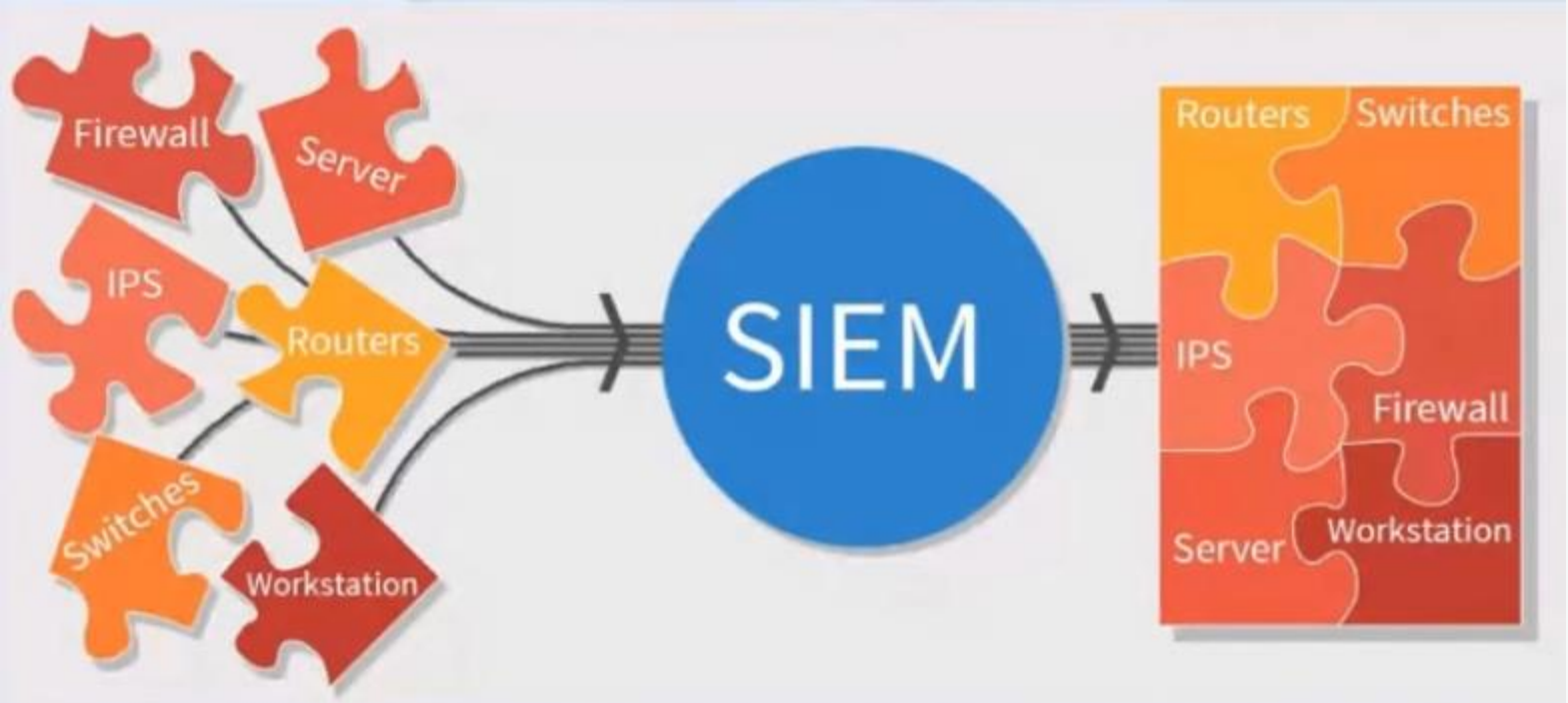
SOC


CERT
Threat Intelligence
Prevention
Understanding
Guidelines
Technology
Business
Response
SOC
CSIRT

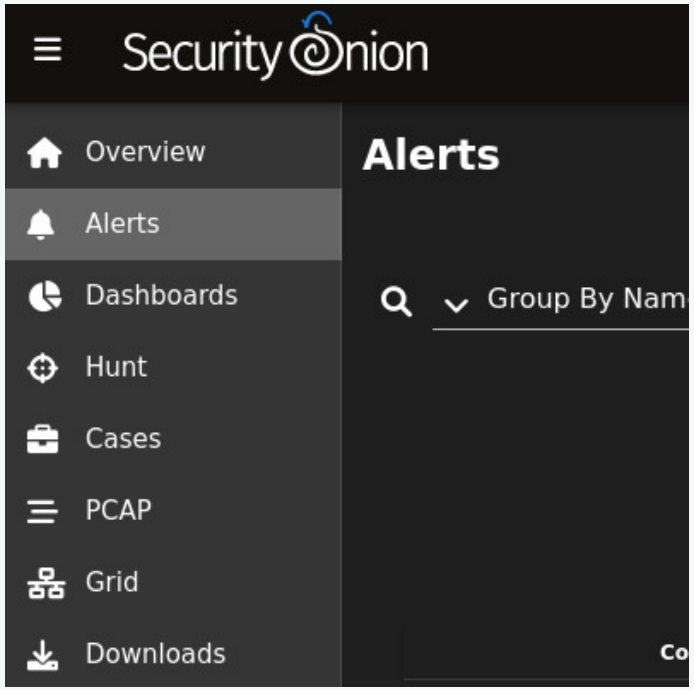
SOC

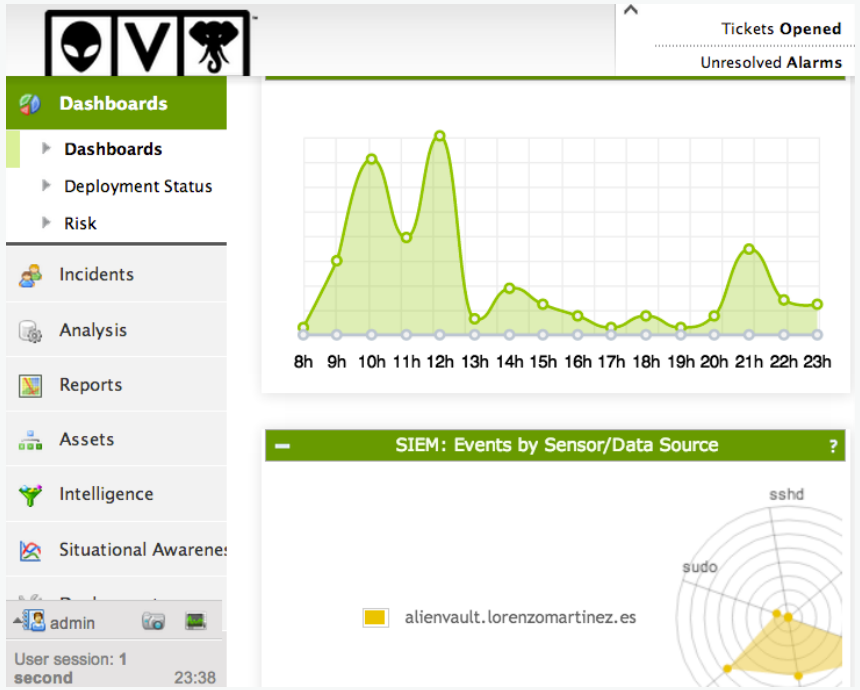
Figure 3. Event management efficiency: Getting from raw events to actionable alerts through repeatable workflow

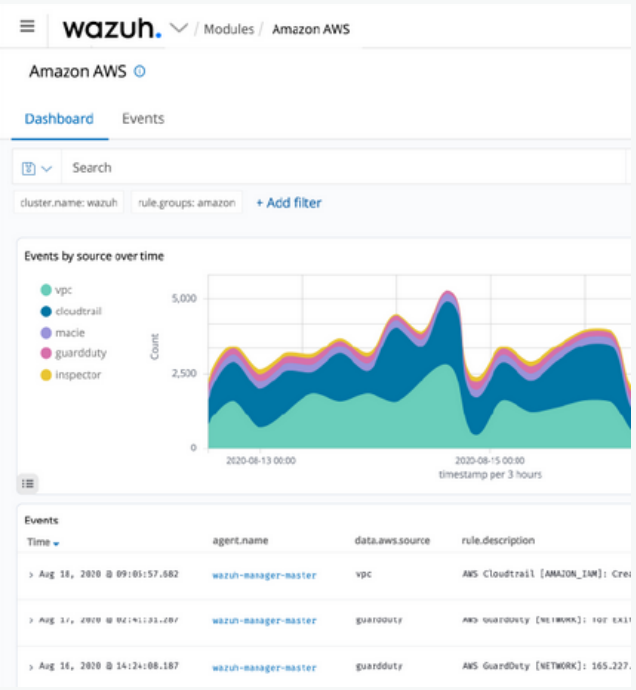
SIEM


Firewall
Server
IPS
Routers
Switches
Workstation
SIEM
Routers
Switches
IPS
Firewall
Server
Workstation

SIEM
Open Source



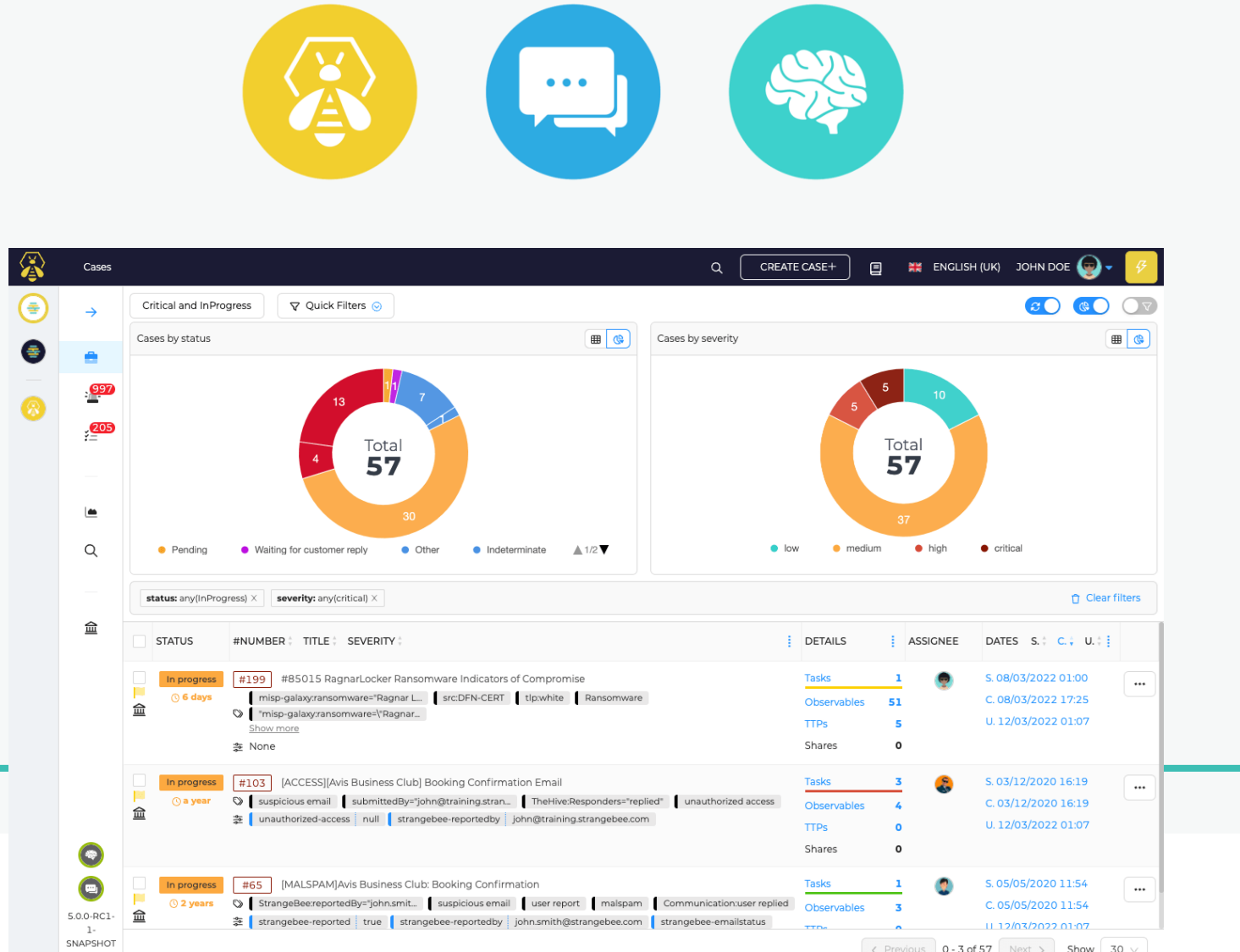




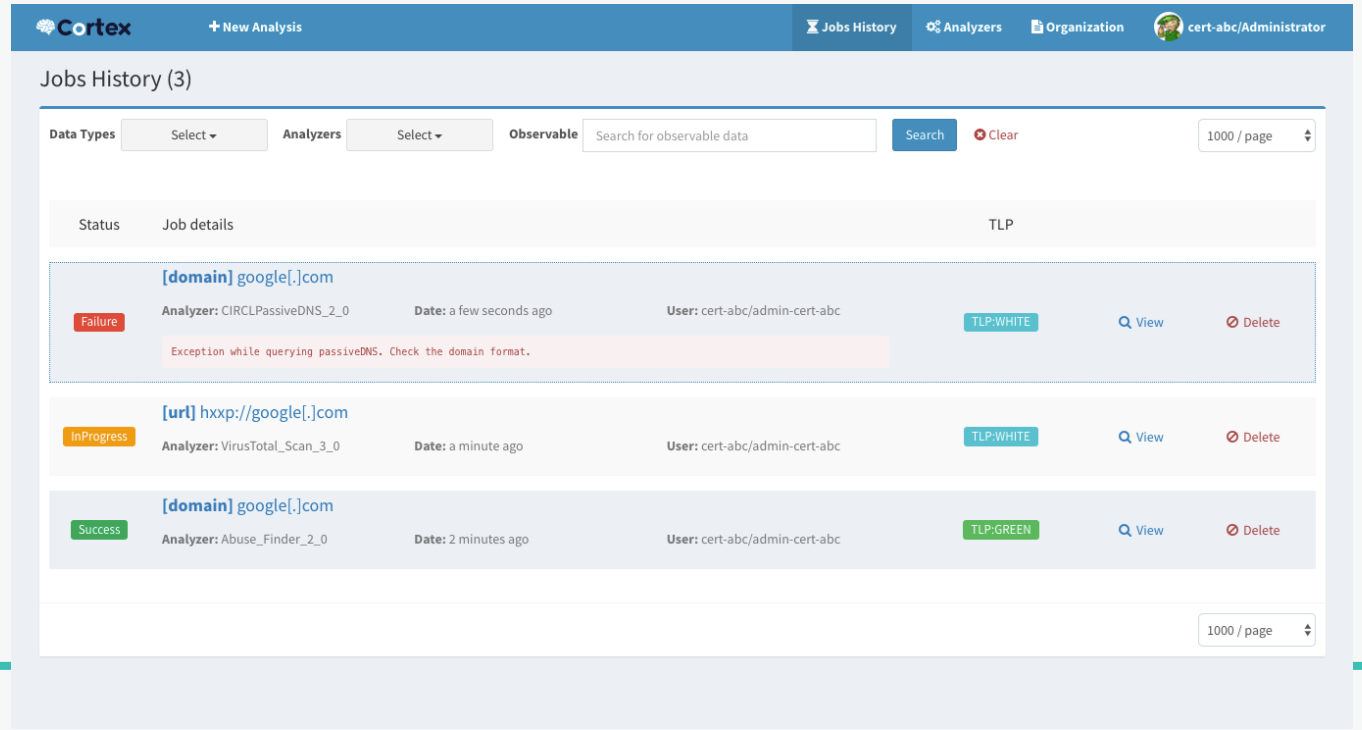
RoadMap

- ❏ Visita guiada por la plataforma
- ❏ Instalación de Agentes (en Windows y Linux)
- ❏ Eventos de Seguridad
- ❏ Integridad
- ❏ Normativa
- ❏ Mitre Att&ck
- ❏ módulo de Vulnerabilidades
- ❏ API de VirusTotal
- ❏ HoneyPots

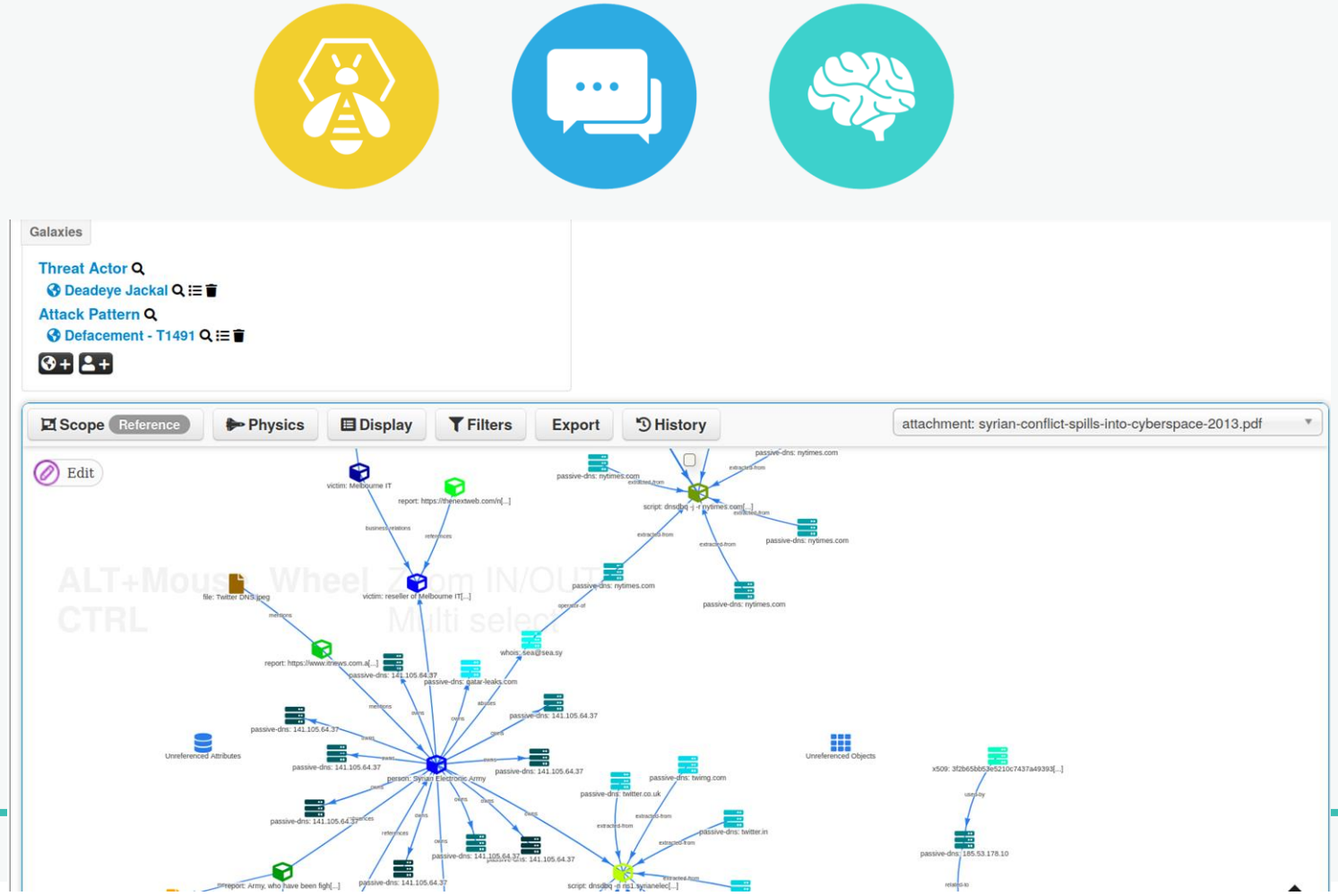
THREAT HUNTING



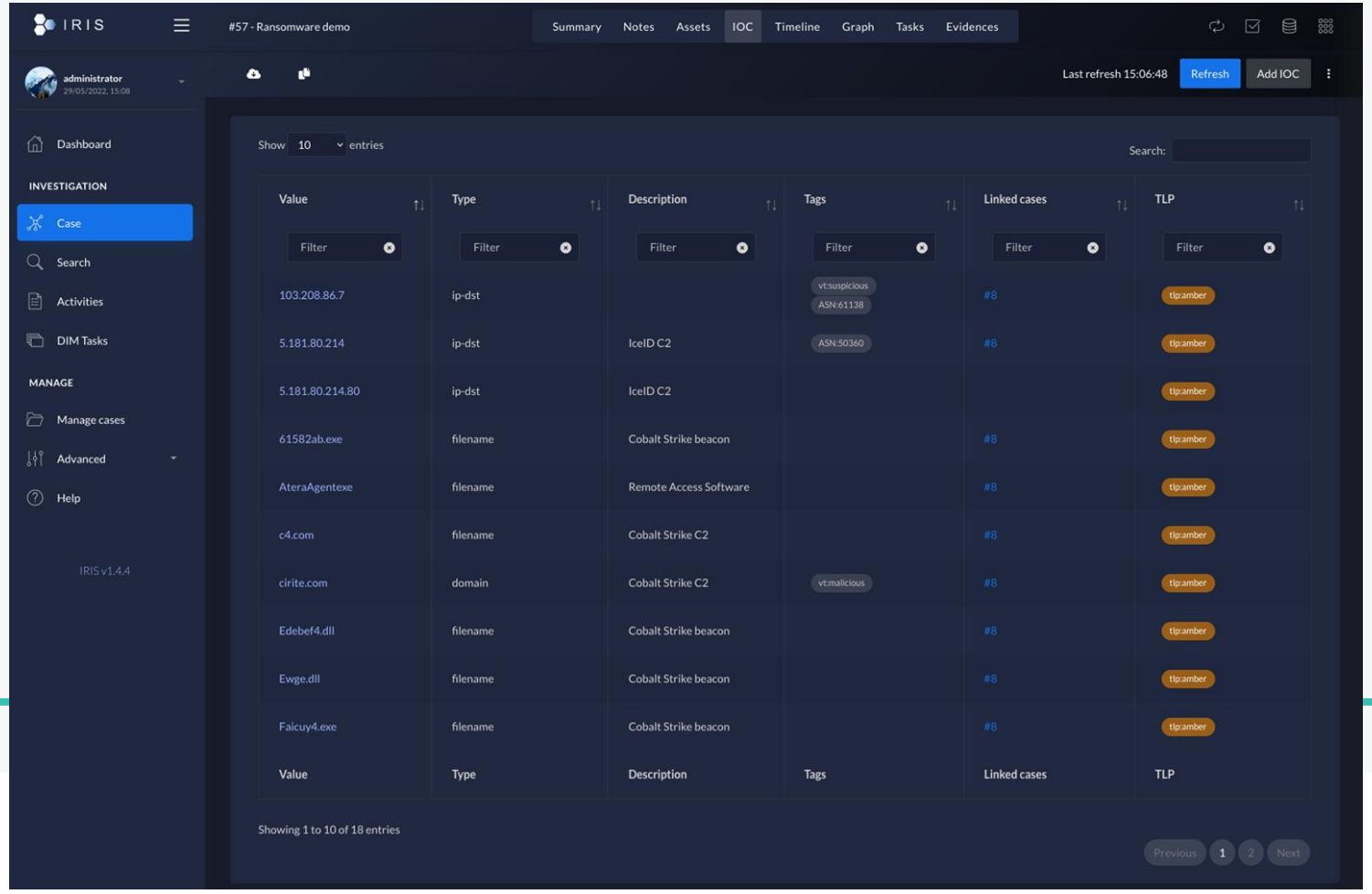
THREAT HUNTING



THREAT HUNTING

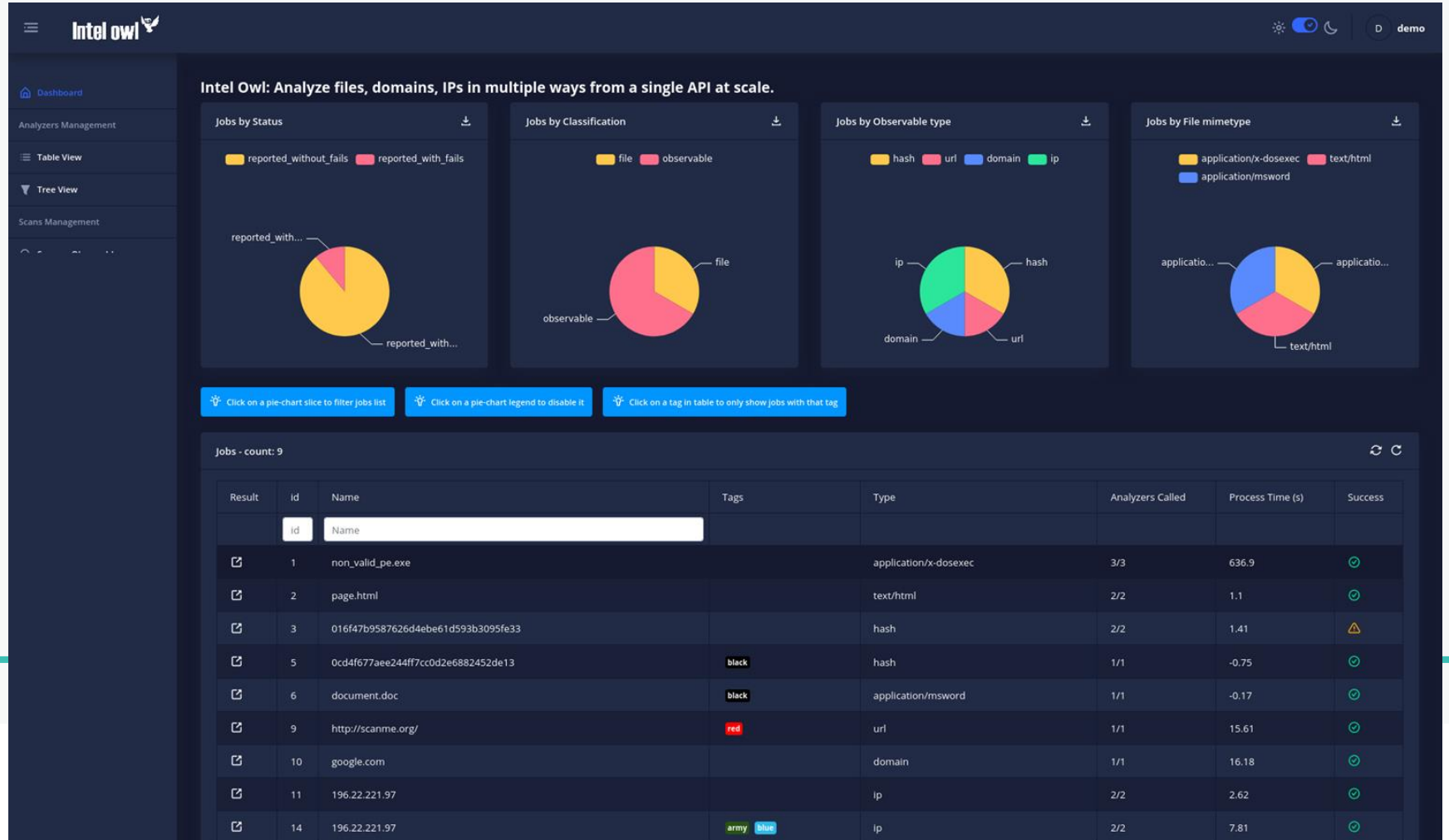


THREAT HUNTING



THREAT HUNTING

Intel owl



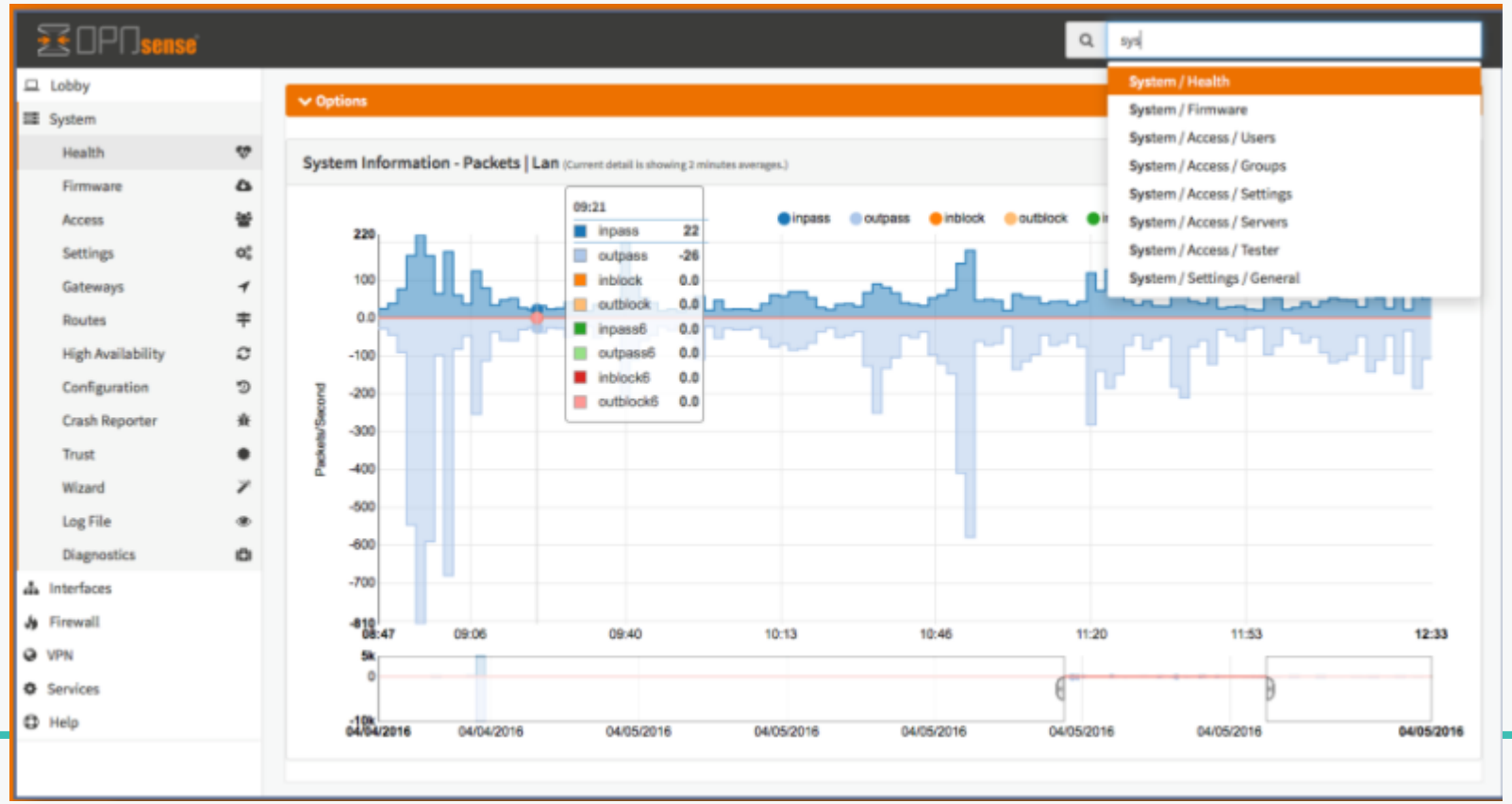
THREAT HUNTING


```
rule SMB_Worm_Tool_Generic {
    meta:
        description = "Generic SMB Worm/Malware Signature"
        author = "Florian Roth"
        reference = "http://goo.gl/N3zx1m"
        date = "2015/02/08"
        hash = "db6cae5734e433b195d8fc3252cbe58469e42bf3"
        score = 70
    strings:
        $mz = { 4d 5a }

        $s1 = "%s\\Admin$\\%s.exe" fullword ascii
        $s2 = "SVCHOST.EXE" fullword wide

        $a1 = "LoadLibrary( NTDLL.DLL ) Error:%d" fullword ascii
        $a2 = "\\svchost.exe" fullword ascii
        $a3 = "msvcrt.bat" fullword ascii
        $a4 = "Microsoft@ Windows@ Operating System" fullword wide
```

THREAT HUNTING

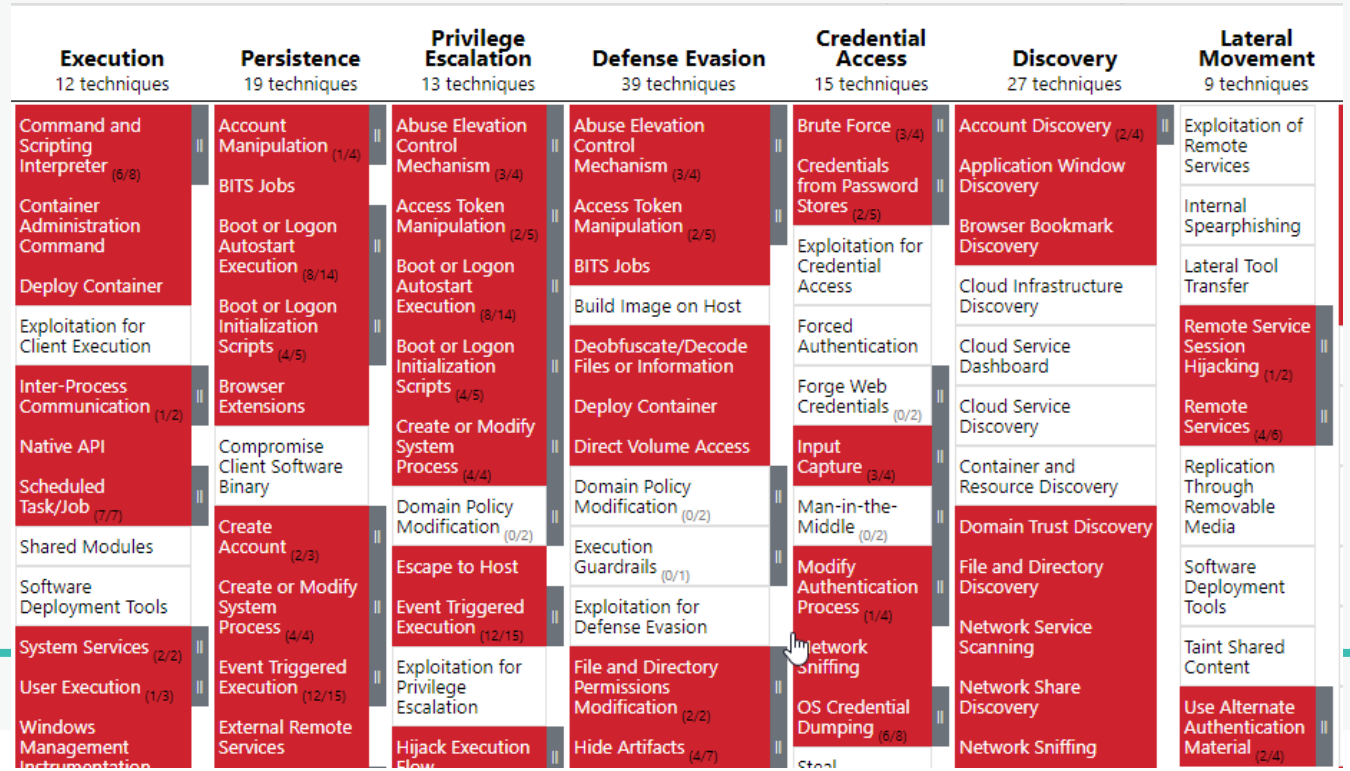

```
  GNU nano 2.9.3                                                  snort.conf

# Step #1: Set the network variables.  For more information, see README.variables
#####################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 172.16.200.130

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
```

THREAT HUNTING



THREAT HUNTING

Atomic Red Team

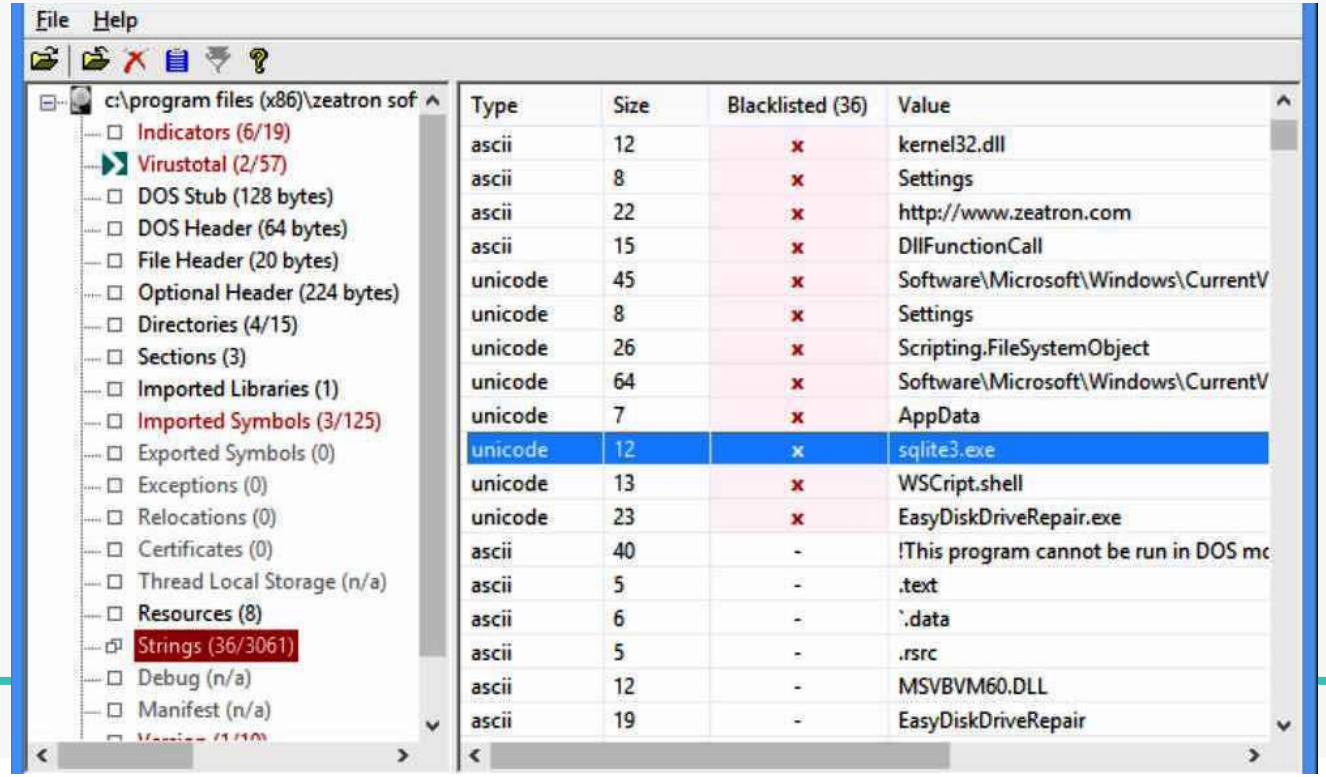


Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques
Command and Scripting Interpreter (6/8)	Account Manipulation (1/4)	Abuse Elevation Control Mechanism (3/4)	Abuse Elevation Control Mechanism (3/4)	Brute Force (3/4)	Account Discovery (2/4)	Exploitation of Remote Services
Container Administration Command	BITS Jobs	Access Token Manipulation (2/5)	Access Token Manipulation (2/5)	Credentials from Password Stores (2/5)	Application Window Discovery	Internal Spearphishing
Deploy Container	Boot or Logon Autostart Execution (8/14)	Boot or Logon Autostart Execution (8/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Exploitation for Client Execution	Boot or Logon Initialization Scripts (4/5)	Boot or Logon Initialization Scripts (4/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (1/2)
Inter-Process Communication (1/2)	Browser Extensions	Create or Modify System Process (4/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (4/6)
Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (3/4)	Cloud Service Discovery	Replication Through Removable Media
Scheduled Task/Job (7/7)	Create Account (2/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Software Deployment Tools
Shared Modules	Create or Modify System Process (4/4)	Event Triggered Execution (12/15)	Domain Policy Modification (0/2)	Modify Authentication Process (1/4)	Domain Trust Discovery	Taint Shared Content
Software Deployment Tools	Event Triggered Execution (12/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (2/4)
System Services (2/2)	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping (6/8)	Network Service Scanning	
User Execution (1/3)			File and Directory Permissions Modification (2/2)	Steal	Network Share Discovery	
Windows Management Instrumentation			Hide Artifacts (4/7)		Network Sniffing	

THREAT HUNTING

PeStudio

Malware Initial Assessment Tool



THREAT HUNTING

Otras Herramientas

VirusTotal

THREAT fox by ABUSE.ch

ANY RUN

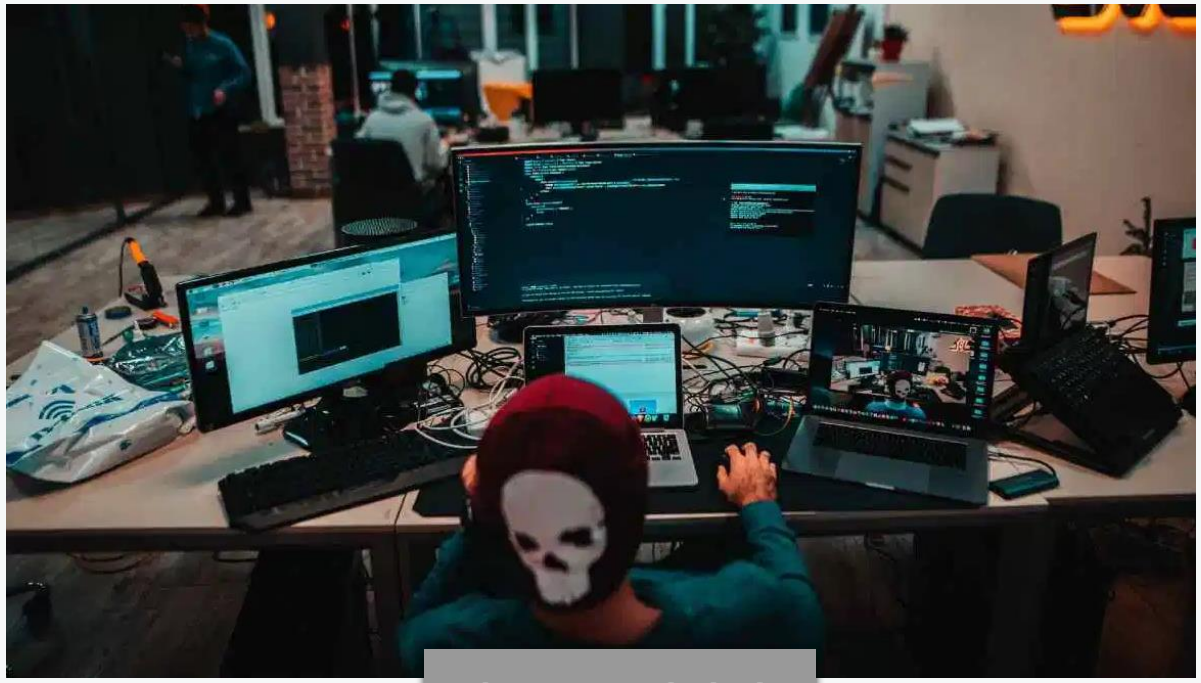
IntelligenceX

cape

DarkFeed
DeepWeb Intelligince Feed

OPEN THREAT EXCHANGE

GRACIAS!



OPEN SOC

Security High School

#SHS2k23

BEEHACKERS