HACKER Threat Intelligence SECURITY

What You should Know

53%

Attacks Infiltrate Unnoticed

68%

Of Ransomware Attacks Unnoticed

91%

Of Attacks Did Not Generate an Alert

DRS
HACKER Threat Intelligence SECURITY

What you should know TOO

- How exposed is your company, data, staff,... on the Internet ?
- What are your Vulnerabilities ?
- Where are your IT Security holes ?
- What is or has been Stolen from you ?
- Have you already been hacked ?
- Any inside Risks, leaking to the outside ?
- ...

DRS
HACKER Threat Intelligence SECURITY

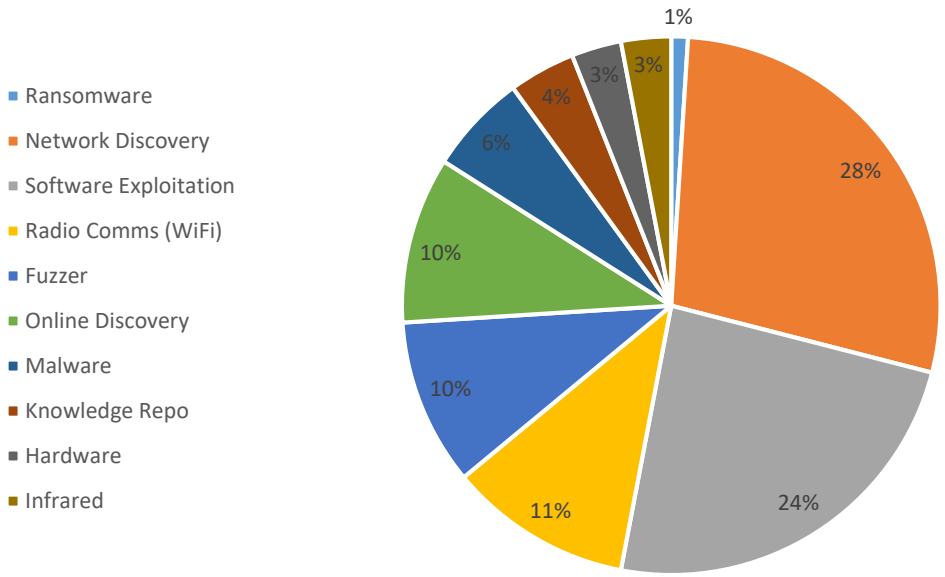
Are You Tiered of:

- ✓ **Hot Air and Promising Sales Speeches, but no results ?**
- ✓ **No integration of Your Constrains – Budget, Staff, Knowledge, Strategy,… ?**
- ✓ **Product orientated Recommendations ?**
- ✓ **Fed-up of Standardized & None Personalised IT Security Reports ?**
- ✓ **Superficial, Useless & none aggregated IT Security Reports ?**
- ✓ **No Real Life Security Solutions ?**
- ✓ **…**

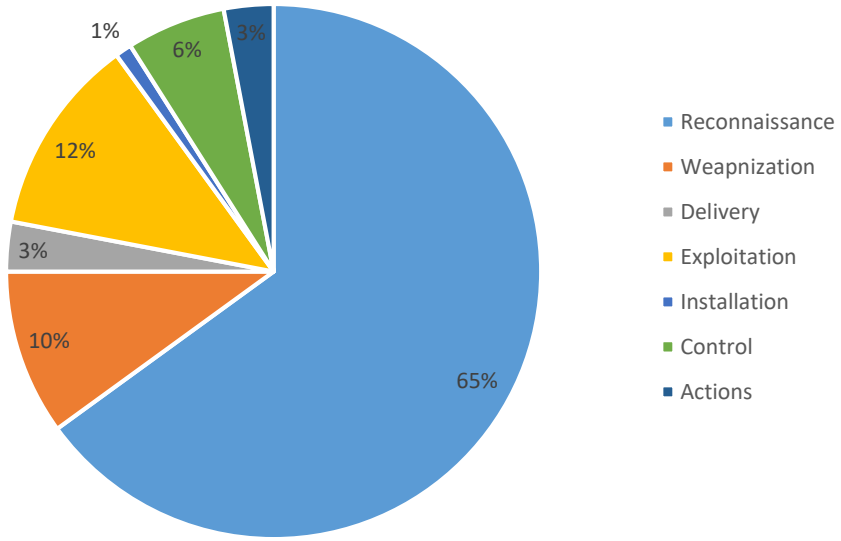
DRS
HACKER Threat Intelligence SECURITY

WHAT you have to face !

Exploitation Families



Kill Chain (Hacker Step by Step)



Multiple Malware groups have been accumulating access & maintaining persistence on target networks for several months with either dormant or activated malware.

As the global market is mainly focusing on COVID-19, less priorities is given to the Cybersecurity!

By so increased EXPLOITATIONS

97% of your IT is much more exposed.

DRS
HACKER Threat Intelligence SECURITY

WHOM you fight against ?

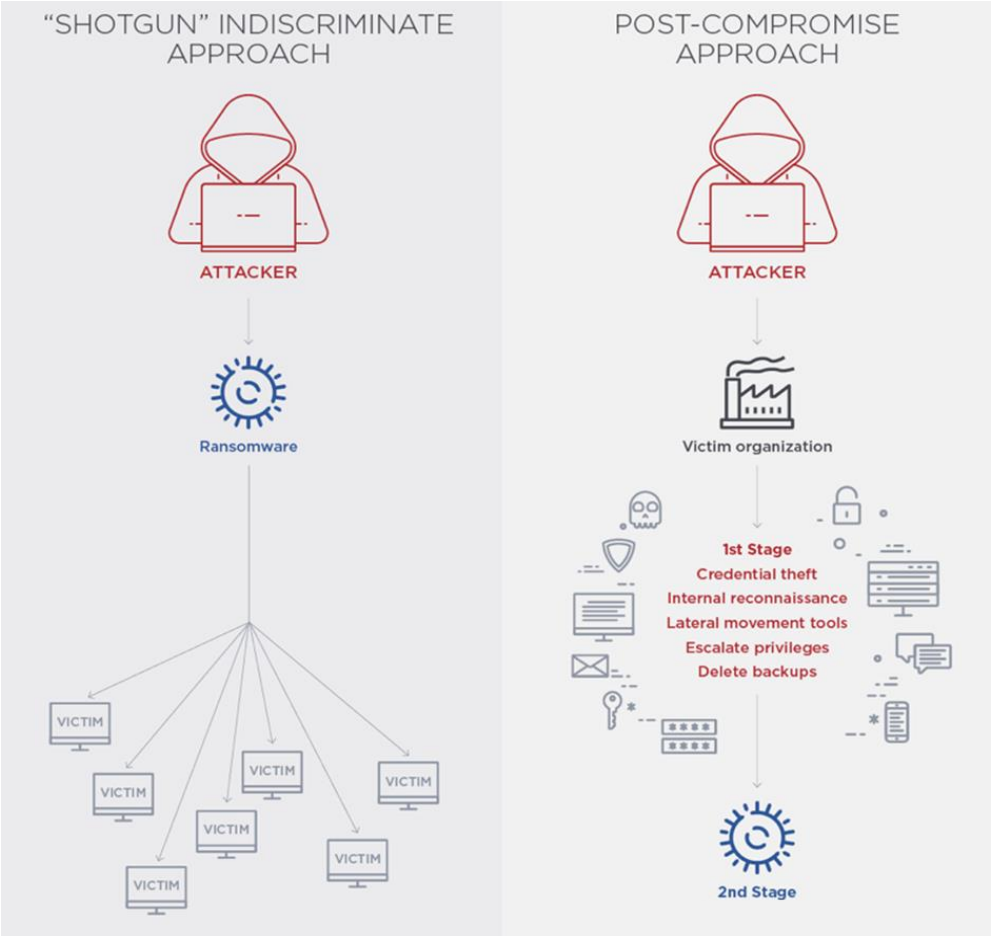
TWO Hacker types you have to face:

The left one is unpredictable and goes for the mass and the end-user trust abusing.

The right one is structured, highly skilled, not in a hurry, deceptive,… What he goes for is your Business GOLD. These are the ones that bring down any organization.

BUT THE WORST IS:

YOU CONTRIBUTE BY 80% FROM THE INSIDE



DRS
HACKER Threat Intelligence SECURITY

OUR VISION

We use the same tools and techniques as the hackers use to attack you,
BUT without impacting you;

We empower your IT & Threat Intelligence !

DRS
HACKER Threat Intelligence SECURITY

What is actually DRS© - THE DIFFERENCE

HDV©

Hacker
Diagnostic
View

HRV©

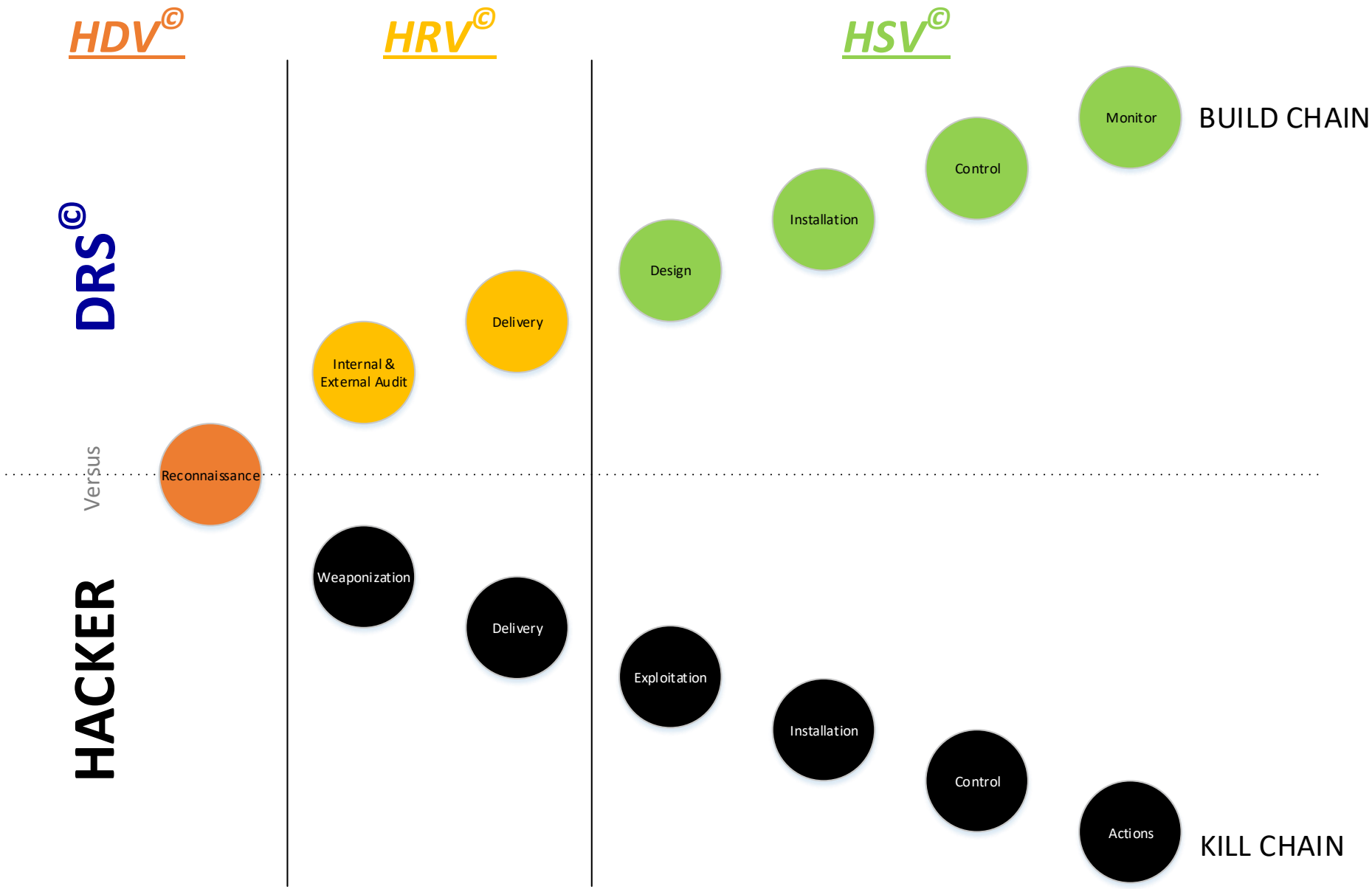
Hacker
Remediation
View

HSV©

Hacker
Strategic
View

DRS
HACKER Threat Intelligence SECURITY

How *DRS©* works



DRS
HACKER Threat Intelligence SECURITY

Hacker Diagnostic View© How HDV© works - Step 1

We scan you passively (Publicly available information) to collect the following information:

A Records
Account on External Site
Affiliate - Company Name
Affiliate - Domain Name
Affiliate - Domain Whois
Affiliate - Email Address
Affiliate - Internet Name
Affiliate - IP Address
Affiliate - Web Content
Affiliate Description - Abstract
Affiliate Description - Category
AnalysisTools
API
Archives
ASN Lookup
Bank Information
Banner Grabbing
BGP AS Membership
BGP AS Peer
Bitcoin Address
Bitcoin Balance
Blacklisted Affiliate IP Address
Blind Elephant Scan
Blogs
Breached Usernames
BuilWith
Business Records
Certificates
Classifieds
Co-Hosted Site - Domain Name
Co-Hosted Site - Domain Whois
Components
Cookies
Country Name
Credit Cards
Cross Dependencies
CVE
Dark Web Layer 3, 4a & 4b
Dating
Deep Web Layer 1 & 2
DeHashed
Digital Currency
DNS entries
DNS SRV Record
Domain Name
Domain Profiler
Domain Profiler & mapping
Drupal Security Scan
Email Address
Email breaches domain(s)
Email Breaches exactis
Email Breaches Facebook
Email Breaches Instagram
Email Breaches LinkedIn
Email Breaches PDL
Email Breaches Tempora Botnet
Email Breaches verifications.io
Email Breaches YouveBeenScraped
Email Gateway (DNS 'MX' Records)
Email HACKED
Email Total Breaches
Emulation
Encoding / Decoding
Engines
Exploits
Exploits & Advisories
Exposed Data Buckets
Exposed Source Code
Externally Hosted JavaScript
Find Hosts Records (Subdomains)
Find shared DNS Servers
Forums
Geolocation
Hacked Email Address
Hash
Hashes analysis
Historic Interesting File
Host Pairs
Hoster & Provider
HTTP Headers
HTTP Status Code
Human Name
IBAN Number
Identified Endpoints
Identified Software / OS
Identified User Software
Identified User with private adrs.
Indicators to be analyzed
Instant Messaging
Interesting File
Internet Name
IP Address
IRC
Joomla Security Scan
Layer 1 & Layer dependency mapping
Layer 1 mapping
Leak Site URL
Leaked Documentation Images / Videos / Docs
Linked URL - External
Linked URL - Internal
Login(s) identified
Malicious Affiliate
Malicious Affiliate IP Address
Malicious Affiliate IP Address
Malicious File
Malicious IP Address on same Subnet
Malicious IP on Same Subnet
Metadata
Mobile
MX records
Name Server (DNS 'NS' Records)
Netblock Membership
Nikto
Non-Standard HTTP Header
Open TCP & UDP Port
Open TCP Port Banner
OpenVAS
Open TCP Port
OpSec
Osint Data
OWASP
People Search
PGP Public Key
Physical Location
Public Code Repository
Public Records
Pwnd mails mapping
Raw Data from RIRs/APIs
Raw DNS Records
Raw File Meta Data
Scanned IP(s)
Search Engine's Web Content
Security holes on the Service Providers level
Service Providers
Similar Domain
Similar Domain - Whois
Social Media Presence
Software Used
SQL Injection
SSL Cert. Security Issus
SSL Certificate - Issued by
SSL Certificate - Issued to
SSL Certificate - Raw Data
SSL Certificate Host Mismatch
SSL Host Mismatch
Sslyzr
SubDomains
Suppliers
Telephone Numbers
Terrorism
TLS Scan
Traceroute
Trackers
Training
Translation
Transportation
Untrusted Certificates
URL (Accepts Uploads)
URL (Form)
URL (Purely Static)
URL (Uses a Web Framework)
URL (Uses Flash)
URL (Uses JavaScript)
URL Crazy
Username
Vulnerability in Public Domain
Web Content Type
Web Server
Web Technology
Website Usability and Performance
What web Analysis
Wikipedia Page Edit
WordPress Security Scan
Zone Transfer
Zoom Eyes Vulnerabilities

What Hackers can see and find on the Internet, we collect for You & analyse it!

DRS
HACKER Threat Intelligence SECURITY

Hacker Diagnostic View© *How HDV© works - Step 1*

You receive as deliverables :

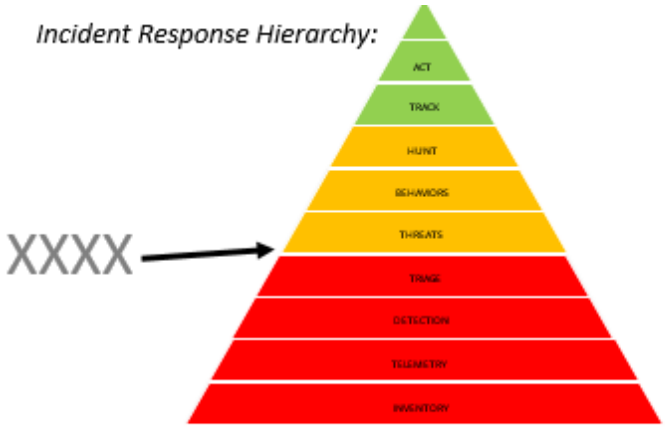
DRS
HACKER Threat Intelligence SECURITY

HDV© Report

BSI Ranking:

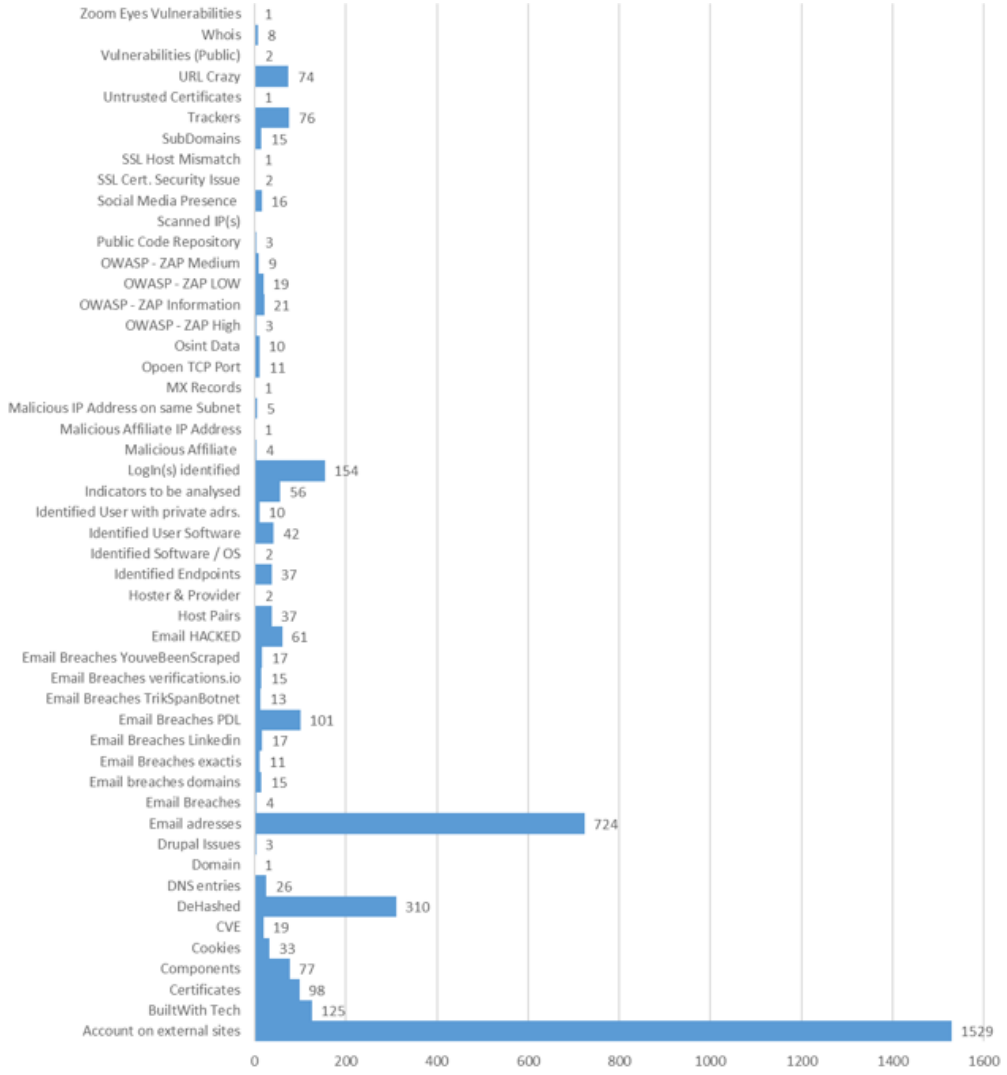
M

Incident Response Hierarchy:



A - D	100% - 88,6%		Can you collaborate with trusted partners to disrupt adversary campaigns?	"During incident response, I operate at the same tempo as the adversary to protect my business assets."
		ACT	Can you deploy proven countermeasures to evict and recover?	
		TRACK	During an intrusion, can you observe adversary activity in real time?	
E - M	***84,8% - 54,4%***	HUNT	Can you detect an adversary that is already embedded?	***"When my red team emulates a real-world adversary, I detect their intrusion at multiple points along the kill chain."***
		BEHAVIORS	Can you detect adversary activity within your environment?	
		THREATS	***Who are your adversaries? What are their capabilities?***	
N - Z	50,6% - 5%	TRIAGE	Can you accurately classify detection results?	"I detect hygiene issues and operator activity that does not follow best practices."
		DETECTION	Can you detect unauthorized activity?	
		TELEMETRY	Do you have visibility across your assets?	
		INVENTORY	Can you name the assets you are defending?	

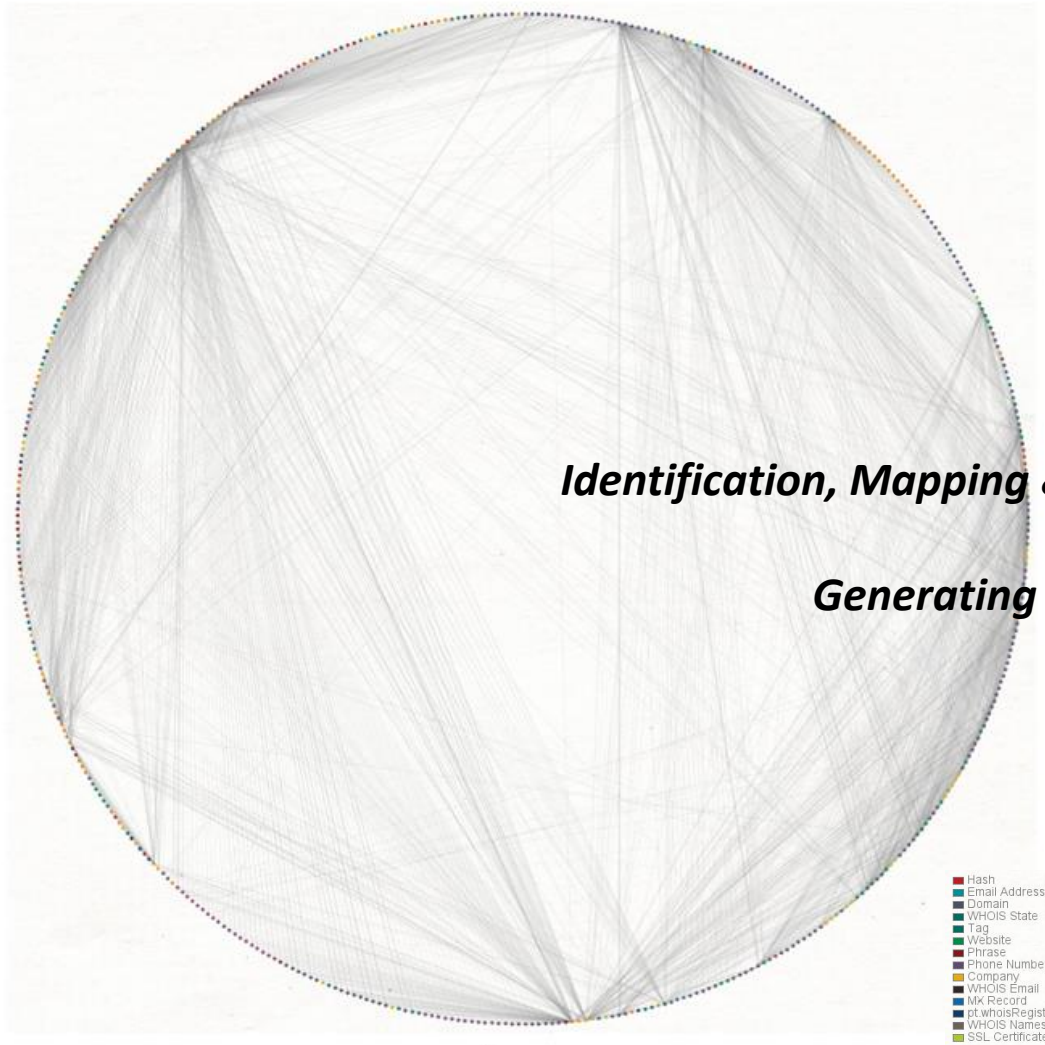
A	100			N	53,6
B	96,2			O	48,8
C	92,4			P	43,0
D	88,6			Q	39,2
E	84,8			R	33,4
F	81,0			S	31,6
G	77,2			T	27,8
H	73,4			U	24,0
I	69,6			V	20,2
J	65,8			W	16,4
K	62,0			X	12,6
L	58,2			Y	8,8
M	54,4			Z	5,0



DRS
HACKER Threat Intelligence SECURITY

HDV© Report

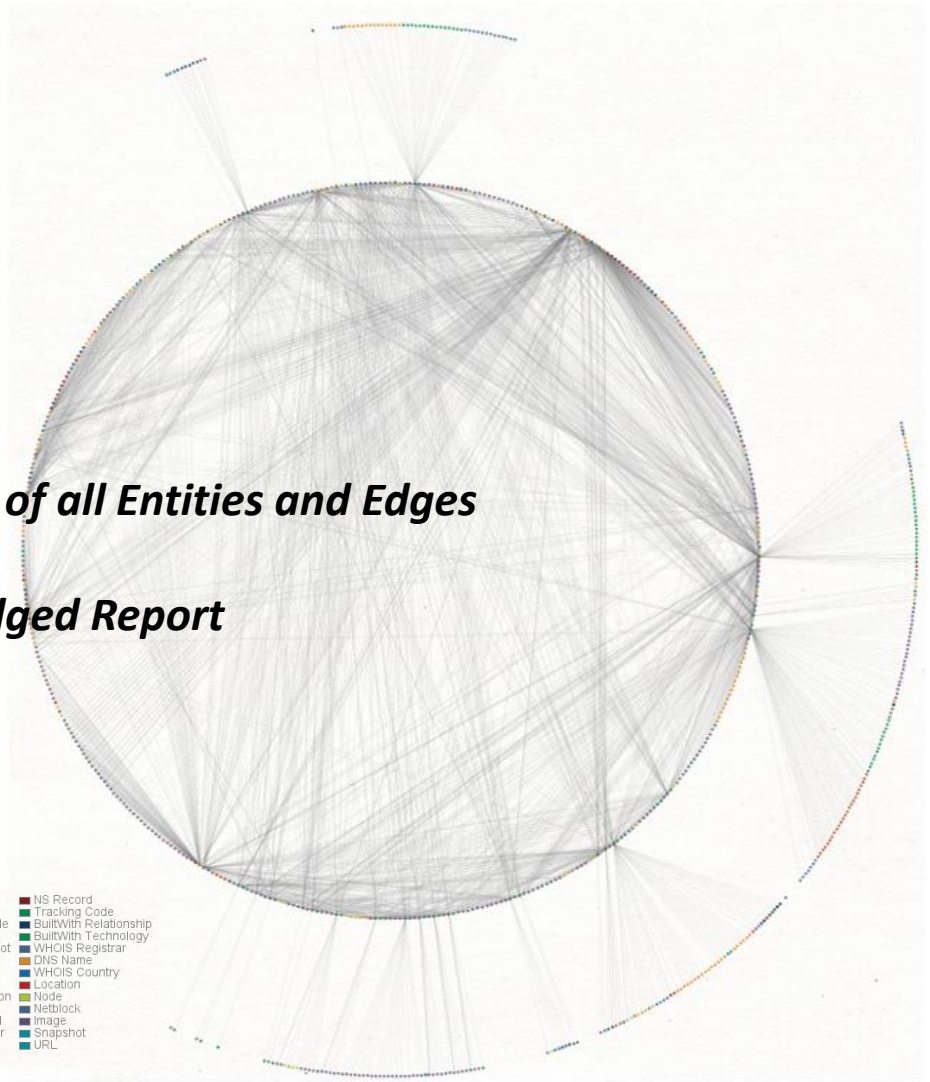
L1 XXXX Domain Profile



1.452 Entities
5.317 Links

3.349 Edges
473 Nodes

L1 & L2 XXXX Domain Profile



1.764 Entities
4.718 Links

3.180 Edges
660 Nodes

Identification, Mapping & Linking of all Entities and Edges

Generating a full-fledged Report

DRS
HACKER Threat Intelligence SECURITY

Hacker Diagnostic View© *How HDV© works - Step 1*

NOW, YOU SEE & YOU KNOW

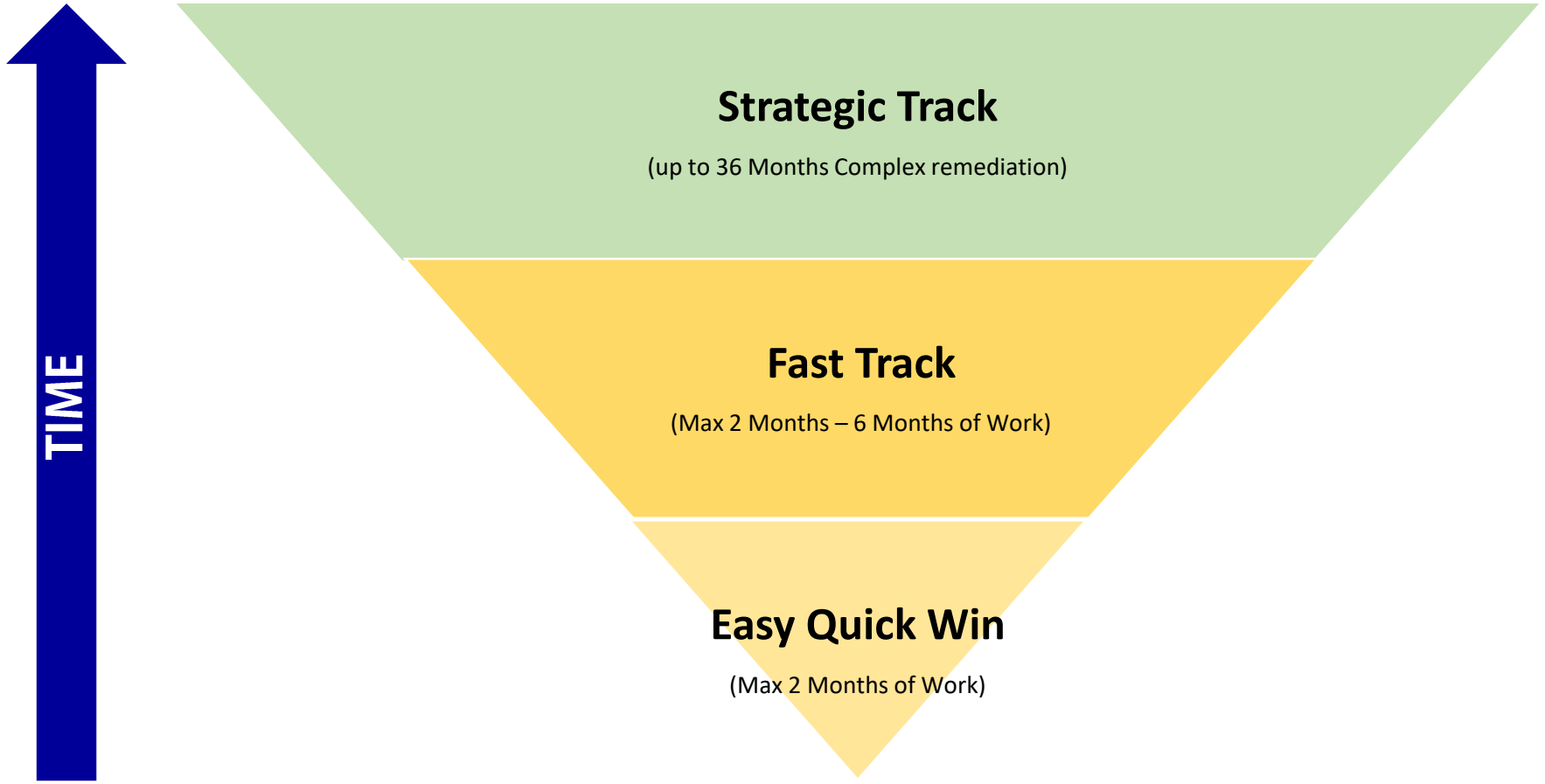
THIS IS WHAT THE HACKERS IDENTIFY, COLLECT & USE

DRS
HACKER Threat Intelligence SECURITY

Hacker Remediation View©: *How HRV© works – Step 2*

Based up on the HDV© an ***Internal and External analysis of your complete IT will be undergone***.

All information and findings will be ***integrated in a Risk vs Impact vs Resources report***, it will also include a ***3 track Remediation plan***:



DRS
HACKER Threat Intelligence SECURITY

Hacker Remediation View©: *How HRV© works – Step 2*

1. Mapping of your available IT experts and their skills towards the HDV©.
2. Inventory all your IT Infrastructure, Software and Hardware.
3. Establish a Delta analysis report that will include your time constraints, budget limitations, skills availability, to establish the best strategy, to fill the « gap(s) » facing your IT Security Risks.
4. This Delta analysis report does also mitigate the likelihood of the identified IT Security Risks.
5. All is done in concertation with the your top management, the IT management and your IT staff or partner, aligned to your IT Strategy.

Hacker Strategic View© *How HSV© works - Step 3*

Once HRV© has been approved, ***the implementation phase*** will be launched.

Here we can assist you by providing your with:

- Project Management
- Real Channel Experts
- Knowledge transfer
- High value for your investment
- …

We are Solution orientated, builders, who fully integrate your needs and constraints !

DRS
HACKER Threat Intelligence SECURITY

Pricing of the DRS© Pack

Module 1 - HDV© **:** By number of IPs & domains which are expected to be analysed.

Module 2 - HRV© **:** Based up on the findings of the HDV we establish a personalised offer.

Module 3 - HSV© **:** This is the implementation phase where we can assist you, up on demand.

Pack - DRS© **:** Recurrent; every year, every 6 months or quarters. (HDV + HRV + HSV + Recurrent)

We don't waste your money for marketing, fancy fliers, sales staff, transport costs, posh web-sites,…. **YOU GET REAL VALUE FOR MONEY** and a full transparency of what we do; up to the point that all your data is stored on an encrypted secured & dedicated external hard drive, with all your data, that will be handed over to you at the end of the mission.

WE DON'T KEEP ANY DATA OF YOU AFTER THE MISSION.

DRS
HACKER Threat Intelligence SECURITY

OUR Motivation

Fight the adversity with the ***DRS©*** skills

=

YOU BEING AN ACTIVE CYBERSECURTY PLAYER

YOU having the CONTROL on your threats

YOU becoming more AGILE

YOU enjoying a HIGH ROI

DRS
HACKER Threat Intelligence SECURITY

Who are we ?

Christoph Pellkofer

Christoph or the "*4-Neuron*"

Founding Partner
christoph.pellkofer@cpe-drs.com
+32/491/46.47.69
LinkedIn

Catherine de Lavergne

Catherine or the "*Lecturer*"

CoFounding Partner
catherine.delavergne@cpe-drs.com
+32/494/46.90.49

Luc de Couville

Luc or the "*Diplomat*"

CoFounding Partner
luc.decouville@cpe-drs.com
+32/473/81.39.20
LinkedIn

Romane Devezeaux

Romane or the "*Sniffer*"

CoFounding Partner
romane.devezeaux@cpe-drs.com
+32/491/13.98.17

DRS
HACKER Threat Intelligence SECURITY

Some References 2019 - 2020

CHU Saint-Pierre
UMC Sint-Pieter

sodexo
QUALITY OF LIFE SERVICES

esa

MUTUALITÉS
LIBRES

Crelan

daoust

fluxys

P&V
Avec vous
quoi qu'il arrive

GHdC
GRAND HÔPITAL
de CHARLEROI

Lhoist

OncoDNA
THE CANCER THERANOSTIC COMPANY

GROUPE
JOLIMONT

CHR Liège
CITADELLE
CHATEAU
ROUGE
SAINTE
ROSALIE
VOTRE SANTÉ, NOTRE MÉTIER

Vivalia
Votre santé, notre quotidien

MUTUALITÉ
CHRÉTIENNE

Belfius
Commercial Finance

IPG
• ANATOMOPATHOLOGIE
• GÉNÉTIQUE CLINIQUE
• BIOLOGIE MOLÉCULAIRE
ET CELLULAIRE

brussels
airport

NIPPON
GASES
The Gas Professionals

Clinique St Pierre
OTTIGNIES

anaisdigital

FEDERALE
Assurance

arvesta
Experts in the field

YUZZU

Hôpital
Erasme
ULB

European Council
Council of the European Union

C.H.U. de Charleroi

EpiCURA
mon hôpital

sonaca

THALES

AVEVE

THALYS

DRS
HACKER Threat Intelligence SECURITY

Thank you
For your time
&
Trust in us

DRS
HACKER Threat Intelligence SECURITY