VESNX

Cybercrime Assistance and Legal Representation

Epic: Matching clients to legal services

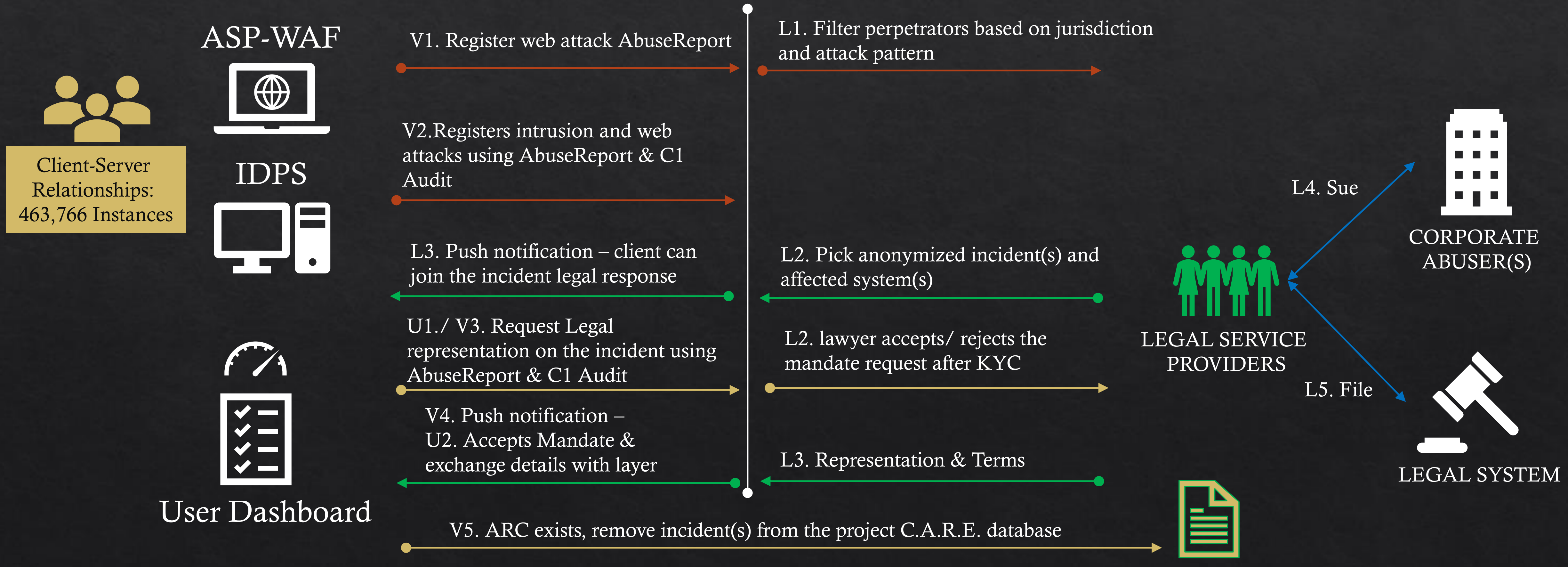
Version 0.2 - 23 April 2023

Actors & Interactions GDPR Compliant

Incentive for clients to use the service
Put an end to abuse and secure justice. Experience the power of a legal solution tailored to protect them and stop cybercriminals in their tracks.

Project C.A.R.E. DATABASE

Selective Case Acquisition & Collaborative Opportunities
Leverage our database to handpick cases that suit your expertise and connect with potential victims for joint legal action against the same perpetrator.



Client-Server Relationships: 463,766 Instances

ASP-WAF

IDPS

User Dashboard

V1. Register web attack AbuseReport

V2.Registers intrusion and web attacks using AbuseReport & C1 Audit

L3. Push notification – client can join the incident legal response

U1./ V3. Request Legal representation on the incident using AbuseReport & C1 Audit

V4. Push notification – U2. Accepts Mandate & exchange details with layer

L1. Filter perpetrators based on jurisdiction and attack pattern

L2. Pick anonymized incident(s) and affected system(s)

L2. lawyer accepts/ rejects the mandate request after KYC

L3. Representation & Terms

LEGAL SERVICE PROVIDERS

L4. Sue

CORPORATE ABUSER(S)

L5. File

LEGAL SYSTEM

V5. ARC exists, remove incident(s) from the project C.A.R.E. database

Attorney-Client relationship (ARC)

Expanding Opportunities: 463,766 Client-Server Instances*

SNAPSHOT

1 Server

7 Days

581 Attackers

4761 Attempts

Utilize our database to uncover prospective cases linked to a sample set of companies engaged in cyber-attacks. The data serves as an essential resource for legal professionals, providing detailed attack information in clear, understandable language. This empowers lawyers to effectively represent impacted clients and pursue compensation or justice from cyber criminals.

Organization	MITRE ATT&CK	Attempts
Del Institute of Technology (Pakistan)	Brute-forcing credentials (T1110) Harvesting credentials from web browsers (T1538) Using stolen credentials (T1078)	4
Vietserver services technology company limited (Vietnam)	Network scanning tools (T1046), Port scanning (T1595), Searching for sensitive files or information (T1083).	4
Oracle BMC (USA)	Exploitation of vulnerable software (T1212.004) Use of password cracking tools (T1110)	28
Enix Ltd (United Kingdom)	Brute-forcing credentials (T1110) Harvesting credentials from web browsers (T1538) Using stolen credentials (T1078)	2
G-Core Labs S.A. (Singapore)	Sensitive information discovery (T1552)	12
Chang Way Technologies Co. Limited (Hong-Kong)	Service or protocol identification (T1016) Exploitation of remote services (T1210) Exploitation for defense evasion (T1020) Exploitation for credential access (T1212) Network service scanning (T1046)	328
Stanford University (USA)	Network scanning tools (T1046)	6
Google LLC (USA)	Sensitive information discovery (T1552) Obfuscated files or information (T1027)	2

** On 22.04.2023, we had 463,766 instances of the community version of the ASP-WAF Firewall. The data shown here are for instance located in Belgium 81.241.141.182*

Sample Paragraph from automated abuse reporting

Effortless Comprehension for Accurate Filing

Our automated system generates clear paragraphs that legal professionals can easily comprehend, ensuring the legitimacy of each filing.

Straightforward content reduces the risk of overlooking genuine abuse or false positives.

By providing accessible information, we enable law firms to assess cases for accurate and efficient reporting confidently.

We have detected an attempt by your server with the IP address 205.213.108.197 to access our e-commerce application's .env file at https://www.vesnx.com/.env on Sat 22 April 2023 14:37:02 UTC. It appears that you made a clumsy attempt to mask this by using an invalid user agent *“Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/111.0.0.0+Safari/537.36”*. We have also observed that you are using a third-party data center WiscNet 605 Science Drive Madison WI 53711.

The .env file is an essential component of web applications that stores configuration information such as environment variables that the application requires during runtime. It may contain sensitive information such as authentication tokens and secret keys, which should not be publicly accessible.

Hackers often try to read the .env file to obtain such sensitive information to compromise the application or its underlying infrastructure. This unauthorized access could allow them to use stolen API keys or database credentials to make unauthorized API calls or modify the application's data. We acknowledge that Google indexes the internet, but the .env file is not published, and it is the only file you have attempted to access. We have identified that the IP address belongs to Google as the DNS server managing the IP address belongs to cache.google.com.

WE ARE HERE TO MAKE A DIFFERENCE

VESNX SA

29 Bd Grande-Duchesse Charlotte
1331 Luxembourg
Luxembourg

Business ID: B 218.421
VAT ID: LU30481579

www.asp-waf.com
info@asp-waf.com

www.vesnx.com
info@vesnx.com

Sales: +352 661 464 633
Technical: +352 661 464 601