REPLY
SYTEL

WHAT CAN THE INTERNET SEE ABOUT YOUR NETWORK?

SYTEL REPLY'S REVE@L:VERIFY TOOL WILL SHOW YOU.

Today, an ever-increasing number of information sources concerning the exposed attack surface of Enterprise IP networks are being created and stored in Open Source Intelligence (OSINT) databases. The contents of these OSINT databases can be searched via simple web-based or API-based interfaces, making data retrieval simple. Sytel Reply has developed a tool to let you see what information is stored in OSINT databases about your network.

Some of it may surprise you!

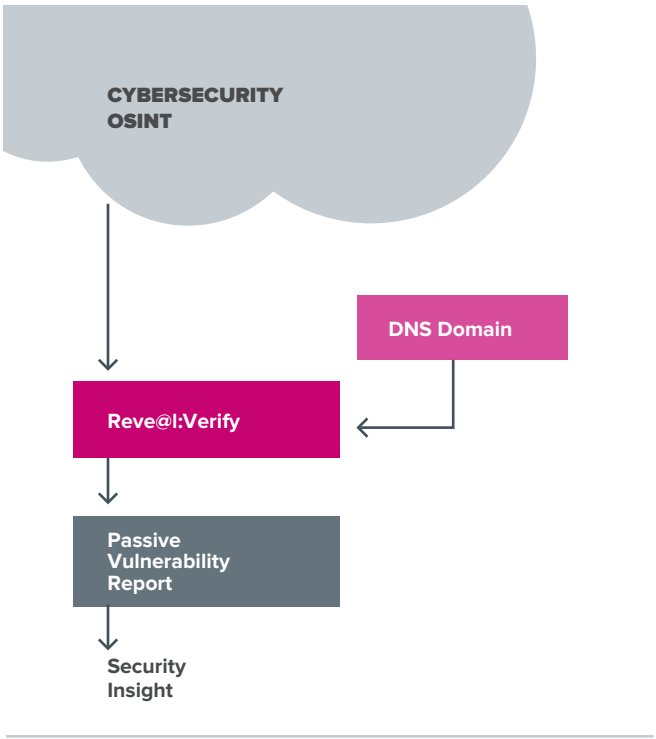
REVE@L:VERIFY

There is a wide range of information available to attackers about any IP network connected to the Internet. If you know where to look, then this information can be easily gathered from a number of **Open Source Intelligence (OSINT)** sources.

When information from a number of sources, concerning a particular targeted network, is aggregated, it is possible to create a high-level picture of the level of network security in the target.
The fact that this information already exists in OSINT sources means that the time taken to collate this information can be performed in a number of minutes.

By harvesting the information from OSINT sources, no actual traffic needs to be sent directly to the target network, resulting in a technique that is both legal, stealthy and available for anyone to analyse your network without you being able to detect them.

To leverage the information present in the OSINT sources, Sytel Reply has developed **Reve@l:Verify**, a unique tool designed to provide a wide-ranging picture of the security posture of any network.
All that **Reve@l:Verify** needs is the specification of the network of interest (DNS domain), via a simple web interface.



Once it has collated and enriched information from OSINT databases, **Reve@l:Verify** produces a Passive Vulnerability Report that can help you to:

- Identify where network security best practices are not being followed;
- Improve your network security situational awareness;
- Identify what information you are inadvertently providing to people who want to attack you;
- Analyse suppliers' and partner networks' security;
- Analyse potential clients' network security;
- Analyse potential company acquisitions' network security.

THE CHALLENGE

The proliferation of freely available OSINT information about IP addresses, email addresses, open TCP/UDP ports and application banners visible to the Internet, means that you are subject to the following challenges:

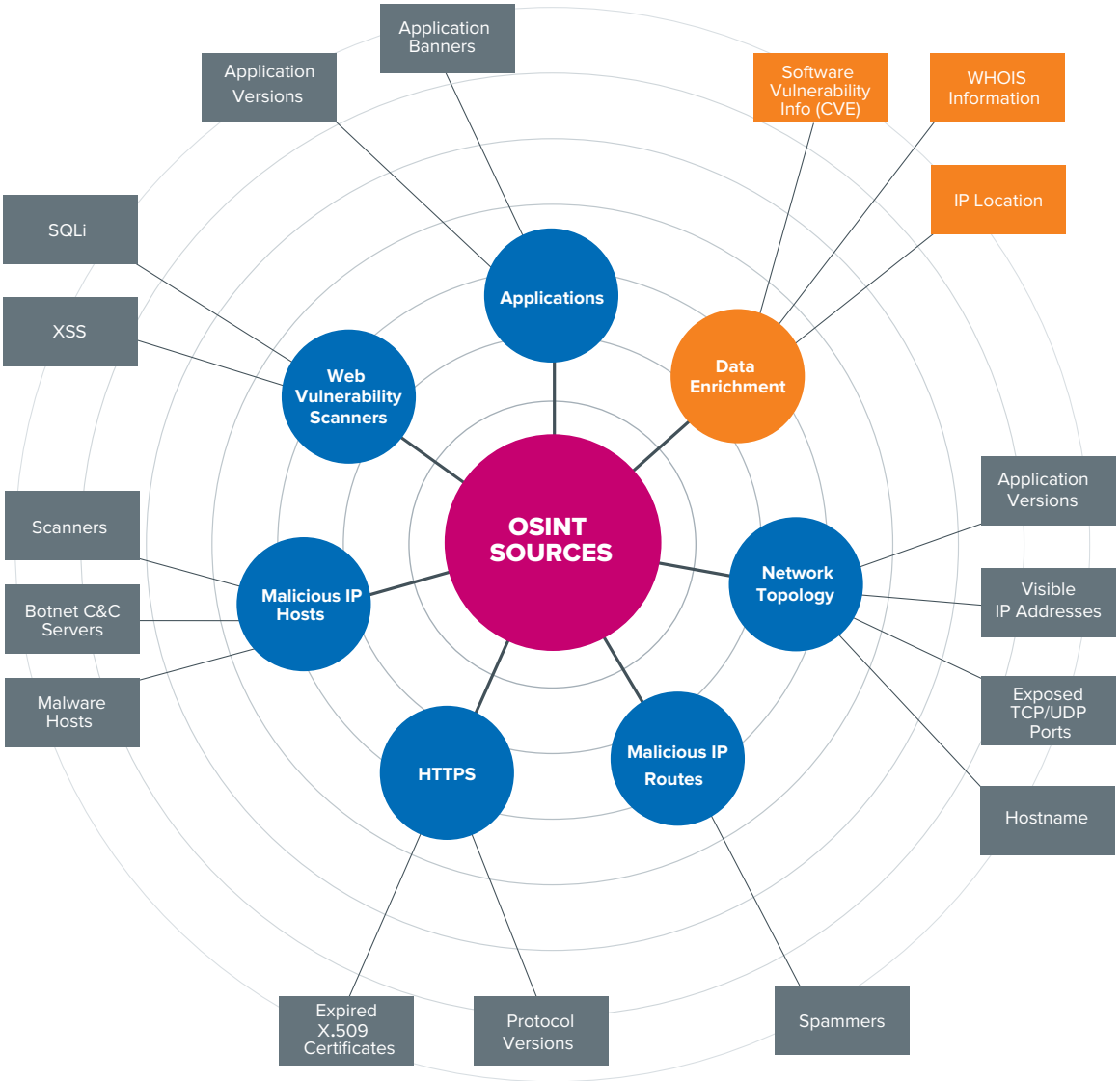
- Attackers are able to more easily profile your network with stealth and identify the weak points in your network without even sending probe traffic to your network;
- A lack of situational awareness concerning what network infrastructure information you are inadvertently leaking to the Internet;
- Potential damage to your brand reputation if people searching OSINT databases discover and make public a vulnerable attack surface that you have not managed to secure.

THE SOLUTION

By automating the collection and analysis of data from a number of OSINT sources of cybersecurity-related information together into a single place, **Reve@l:Verify identifies and ranks potential vulnerabilities in your network** and shows you the attack surface you are exposing to the internet. By analyzing the exposed attack surface, you can identify weaknesses in your internal security architecture such as a lack of creation, adoption or accurate auditing of security policies and best practice guidelines.

THE REVE@L:VERIFY VIEW

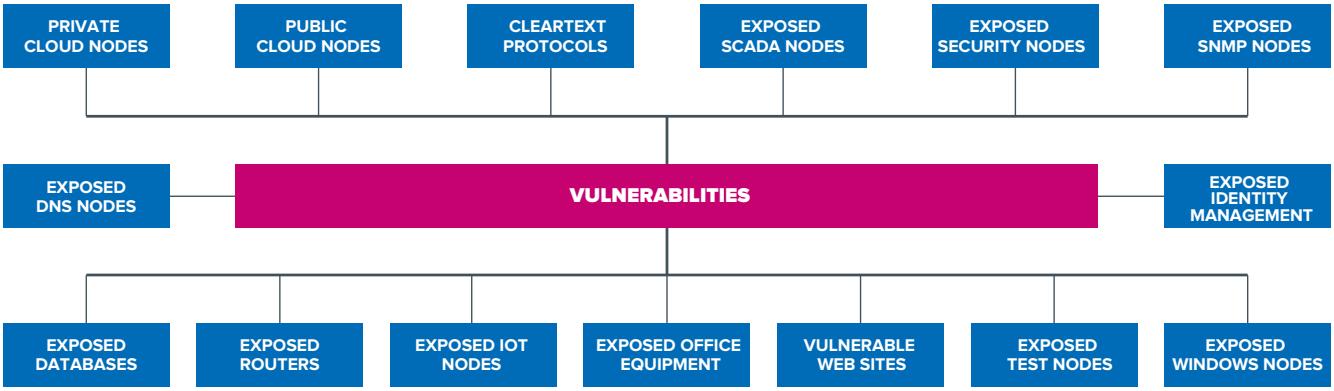
Reve@l:Verify is able to collect OSINT information from an ever increasing number of sources that currently include:



Cybersecurity OSINT Sources used by Reve@l:Verify

REVE@L:VERIFY VULNERABILITY REPORTING

Reve@l:Verify uses OSINT information in order to produce a **customised report detailing the potential vulnerabilities present in your network.** Each vulnerability is identified as presenting a High, Medium or Low risk to your network and data confidentiality, integrity and availability, including recommended remediation steps and relevant ISO27001 that should be considered.



Vulnerabilities Reported by Reve@l:Verify

Examples of vulnerabilities that **Reve@l:Verify** is able to identify include the following:

- URLs of your websites that have recently been identified as being vulnerable to XSS and SQLi attacks;
- User accounts associated with well-known data breaches;
- Assets (identified by IP address, hostname and BGP ASN/name) that are exposing databases to the public internet;
- Assets that are potentially being misused as botnet command and control (C&C) servers or hosting malware;
- Assets that are potentially part of the TOR (The Onion Router) network;
- Assets that are exposing services associated with Big Data infrastructure (e.g. MongoDB, Zookeeper) to the public internet;
- Assets that are exposing services associated with SCADA infrastructure to the public internet;
- Assets that are exposing services associated with Identity Management infrastructure (e.g. LDAP, TACACS+ nodes) to the public internet;
- IP routes in your network that are being hijacked by spammers;
- Web services using poor configuration of SSL and TLS;
- Expired (or soon to expire) X.509 certificates;
- Assets that are exposing services associated with Internet Of Things (IoT) infrastructure (e.g. low power, embedded systems) to the public internet;
- Assets that are potentially office equipment such as printers that are being exposed to the public internet;
- Assets that are potentially exposing TCP/UDP services to the public internet that would be considered poor security practice;
- Assets that are being managed using protocols that allow the transmission of user credentials in the clear across the public internet.

In addition, the **Reve@l:Verify** Report contains an Asset List containing all IP addresses discovered in the specified domain.

REPLY SYTEL

Sytel Reply UK is the Reply Group Company specialising in an open and pioneering consultancy approach that helps clients successfully innovate and transform in today's ever-changing digital world. With a 'Give to Get' mentality, Sytel Reply UK enables clients to grow through the development and delivery of secure, compliant and future-proofed solutions for some of the largest telco and media enterprises worldwide. By bridging the gap between technology and business, Sytel Reply UK focuses on increasing revenue streams and efficiency, whilst reducing costs and time to market.

Founded in 2010, Sytel Reply UK is a focused, dedicated, agile group of talented and experienced technologists and consultants. Sytel Reply UK is part of Reply, a network of highly specialised companies focused on the design and implementation of solutions based on new communication channels and digital media.

www.reply.com