contact@eclipticdynamics.co.uk

OIS makes you and your organisation undetectable on the internet.

Protects your corporate infrastructure, keeping your data private.

Gives you access to the best OSINT tools.

Provides constantly evolving online security.

Gives you a single Ecosystem to conduct sensitive online research.

OIS is a secure and low attribution online environment that allows analysts to conduct sensitive digital research.

It is a complete Open Source Intelligence ecosystem, it provides you with exceptional security and use of the latest OSINT tools.

contact@eclipticdynamics.co.uk

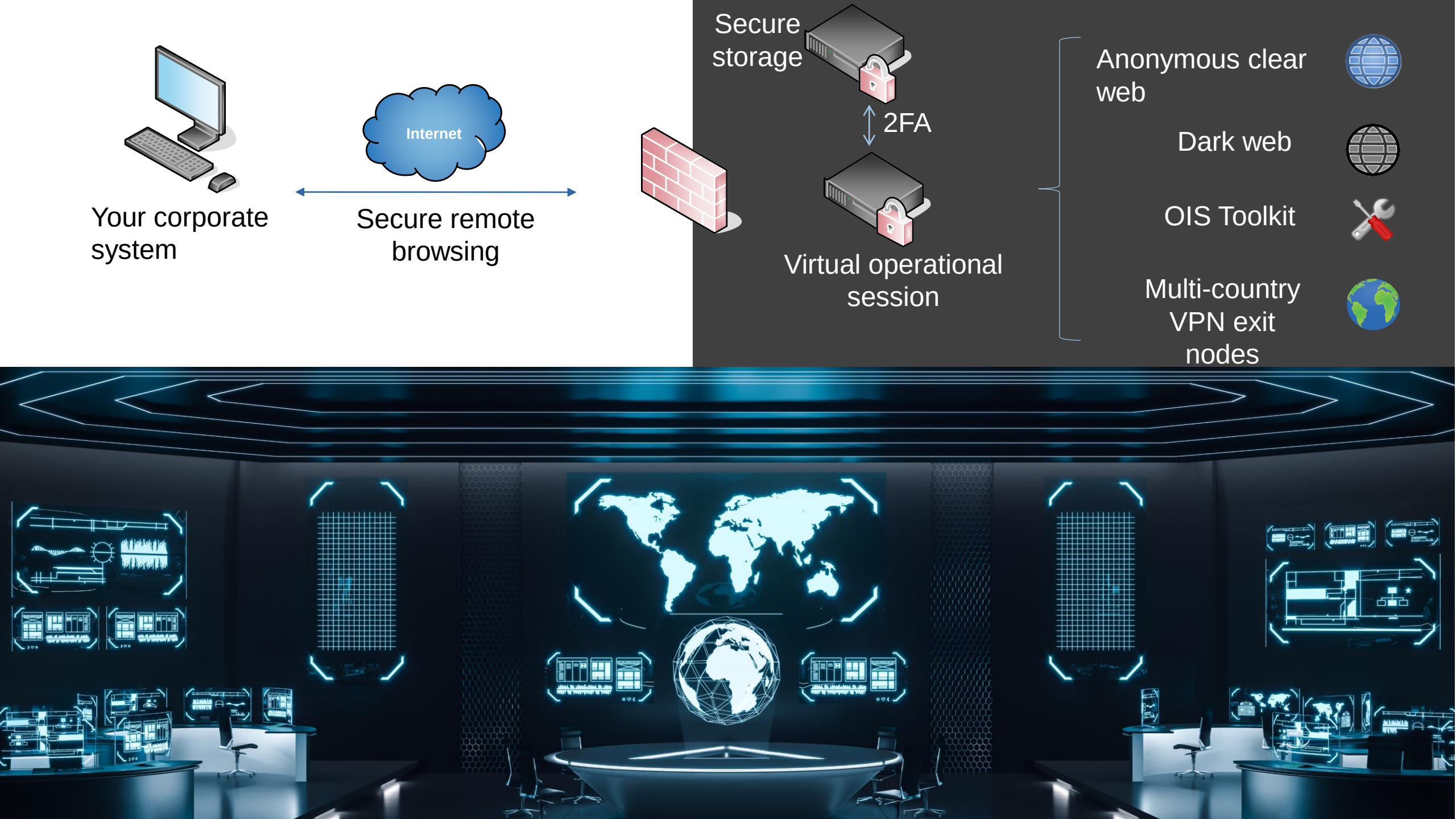
HOW IT WORKS

OIS can be accessed anywhere in the world via a web browser. It does not confine you to a single system; you simply navigate to our website and sign in using your randomly generated credentials. There are no additional software or hardware requirements.

Protection is offered at the local level using encryption protocols between our servers and your browser. This provides protection on open or unknown WiFi networks with the local internet provider only being able to see an encrypted connection and not your internet activity.

Your OIS environment is running on a virtual session on our server, this gives your devices and data additional layers of protection against cyber attacks when compared to simply using a standard Virtual Private Network. We take the risk away from you and your device.

We do not monitor or store the content of any OIS sessions. Every 24 hours, the OIS infrastructure is completely rebuilt to ensure it is updated and to destroy any potential threats. We protect your device and your privacy when they need it most.


Secure storage
2FA
Virtual operational session
Anonymous clear web
Dark web
OIS Toolkit
Multi-country VPN exit nodes
Internet
Your corporate system
Secure remote browsing

No client software required, access OIS via any browser (Firefox, Chrome, Opera recommended) from any device (Windows/MAC/Android/Linux).

Seamless access through most corporate firewalls and proxies (secure port 4443).

Conduct online investigations from a hardened, monitored and patched Linux environment.

OIS operational environment is non persistent and cannot store or access client data.

OIS is a secure and deniable online environment which allows analysts to conduct sensitive digital research.

End to end encryption from your device to OIS.

OIS destroys and rebuilds all machines every 24 hours.

Randomly generated credentials, meaning no link between user and OIS.

Fully scalable from individual to enterprise level.

Anonymous clear web access – up-to-date OSINT bookmarked resources and add ons included.

Secure dark web access (Tor, i2p).

OSINT and case management tools preloaded.

Kill switch to instantly destroy sessions and restore machine to default.

Dial VPN connections to 33 different countries.

OIS is a complete Open Source Intelligence ecosystem providing exceptional security and access to the latest OSINT tools.

Manually select the externally visible operating system.

Spiderfoot provides selector reconnaissance.

Easy to transfer text between OIS and corporate devices.

Simple and easy to capture still images (sections and whole webpages).

Separate, persistent storage infrastructure secured by two factor authentication.

contact@eclipticdynamics.co.uk

VPN software/providers
VPNs have been used for obfuscating online activities for years. They have now become targets for developing and exploiting vulnerabilities. Many popular VPN connection protocols and ciphers have been compromised (one of the most widely used protocols, PPTP, has multiple known and serious security vulnerabilities). If you connect from your trusted network directly to a VPN provider, you must inherently trust this third party - when you connect to a VPN via OIS you are using our system as a "proxy" for your online activities.

DNS Requests
DNS servers convert a requested URL (www.google.co.uk) into an IP address (e.g. 172.217.17.3). DNS service providers (like google) can and do log these requests potentially tracking your internet usage. If you forget to use, or wrongly configure a VPN, this information (along with your real IP address) can still be visible to ISPs.

Browser history collection and tracking
Recent "privacy violations" from social media and tech companies have again highlighted how companies collect, analyse, track and sell online usage. Recent incidents like “super cookies" and compromised Chinese supplied hardware cannot be mitigated against by a VPN as they are linked to specific devices. OIS is providing a trusted portal between your network and the internet.

MAC addresses
Each device on a network has a unique, identifiable "address". Unless you perform MAC address randomisation, a VPN does not provide anonymity from this. The OIS environment randomises all identifiable hardware fingerprints every time the system is rebuilt - either on demand or nightly.

Widespread IP address leak via WebRTC
A "flaw" discovered in 2015 has largely been ignored by browser manufacturers - WebRTC is a standard used for providing voice and video content in a browser (eliminating the need for plugins or extensions like Flash). If you do not disable this (and double check after every browser update) and your VPN provider has not blocked this functionality, your true IP address will be leaked.

contact@eclipticdynamics.co.uk

OIS MITIGATES THREATS TO YOU, YOUR DATA AND YOUR INFRASTRUTURE

Ransomware
Malicious code that encrypts users' files and then demands a ransom for the decryption key has become rampant over the past few years. This form of malware is delivered by a compromised webpage or a downloaded file/email attachment. The necessary code, payload deployment advice and ransom collection guidance are freely available on the dark web. Visiting high risk sites/forums severely increases your chances of encountering ransomware.
No user data is stored on the OIS system and OIS has no access to your trusted network - any data you wish to store from your online investigations is stored in a completely separate system accessed via two-factor authentication.

Zero day threats
The most difficult threat to protect against is the vulnerability that has not yet been discovered. The OIS environment is protected by the leading Artificial Intelligence threat detection software that operates in real-time to catch any potential consequences from a zero-day exploit. We also employ a combination of firewall, anti-virus, intrusion detection, application sandboxing and system log file monitoring to protect sensitive online investigations..

Application location leakage
Device locating GPS is used by many applications and websites. This information is potentially available to malicious browser code regardless of VPN connection. OIS provides internet access from a physical server located away from your network eliminating any geo locating information threat.

"Side-channel" tracking
Even when all internet traffic is encrypted by a VPN, an ISP or a compromised web site can potentially learn information relating to a user and begin to build trackable patterns, such as access times, battery levels, screen display sizes/resolutions, volume and features of data, and keystroke patterns.

Browser delivered exploits
Visiting high risk websites presents the threat of activating malicious scripts - these scripts can do anything from using your machine to mine cryptocurrency without your knowledge to delivering persistent ransomware and trojans. These threats are exponentially increased if you use Microsoft Windows, Internet Explorer, Adobe Flash/Reader and Java.

OIS runs in a hardened Linux environment with a significantly reduced attack footprint for browser delivered exploits. Should an exploit run successfully it is OIS that is exposed to the consequences not a device inside your trusted network . OIS instances can be instantly destroyed if a user fears a compromise has occurred. To further mitigate from any persistent threats, the OIS environment is rebuilt completely every day.

Applications And Capability Plugins

OIS is designed to deliver a productive environment for analysts to work in. OIS offers additional applications for users to load into their workspace. We provide seamless integration of these applications into your OIS environment on an individual basis based on your requirements.

Hunchly

The Only Web Capture Tool Designed For Online Investigations. Hunchly automatically collects, documents, and annotates every web page you visit.

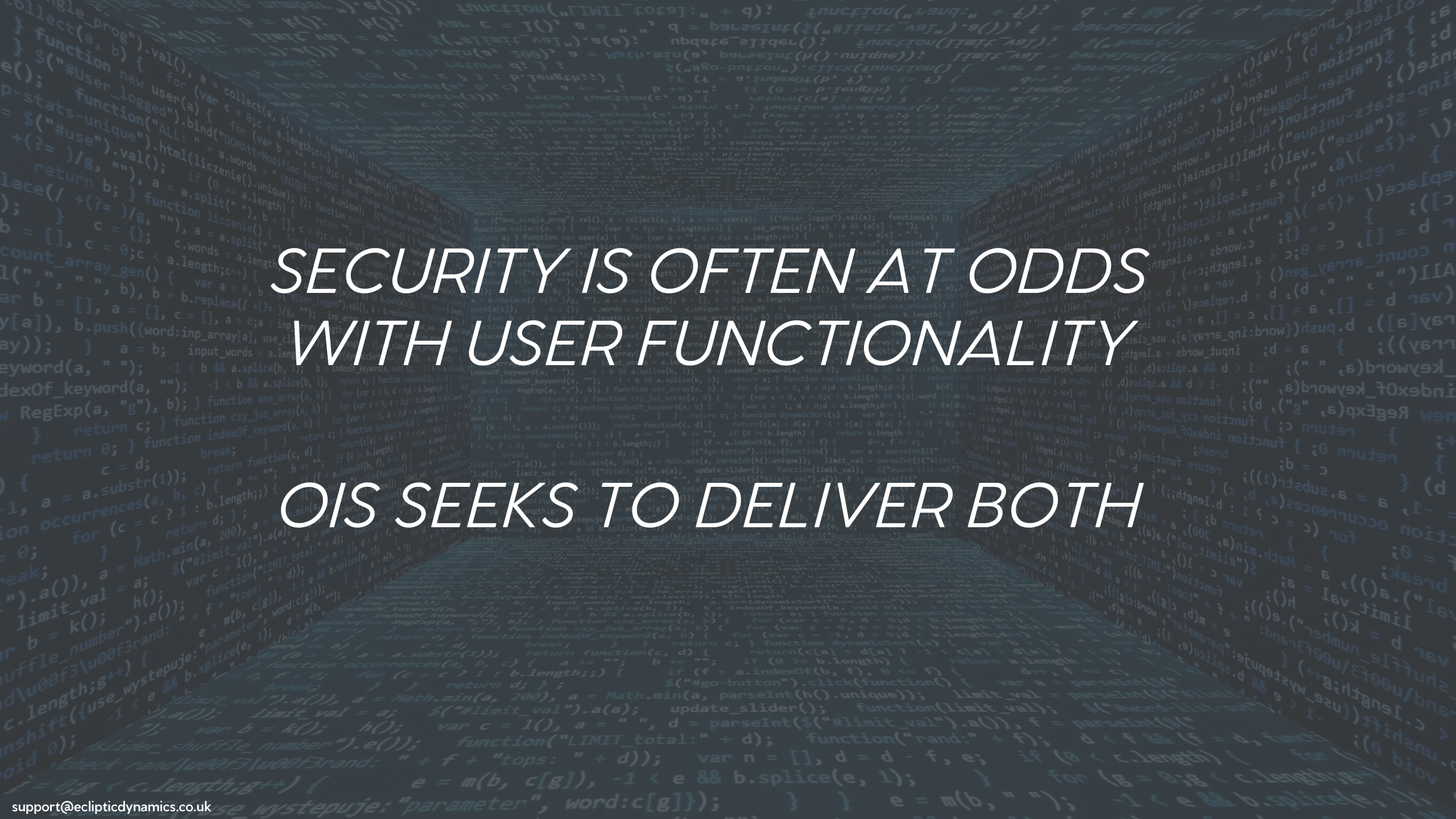
Online research usually starts with the "search engine shotgun approach" — and before you know it, you've got dozens of tabs open and no idea how you got from A to Z – which interrupt your flow by resulting in endless copying and pasting of URLs or take screenshots which slows you down. Hunchly runs quietly in your browser to capture each page as you go — so you never forget to capture a link again.

Dark Search Engine

Finding relevant information on the dark web can be incredibly difficult. Dark Search Engine crawls the dark web and indexes TOR sites for you. It not only allows you to find data but you can also create alerts for new information.

Dark Search Engine integrates into OIS. You can find, view and understand Tor sites in a secure environment.

contact@eclipticdynamics.co.uk


SECURITY IS OFTEN AT ODDS
WITH USER FUNCTIONALITY
OIS SEEKS TO DELIVER BOTH

For any queries please contact:

contact@eclipticdynamics.co.uk