About Darkscope

Darkscope is focused on delivering superior cyber intelligence to clients about nefarious activities being planned against them in the deepweb and darknet. Today's cyberattacks are sophisticated, well researched and planned. They are more complex, better delivered and are more attuned to the market than ever. They will continue to develop at a faster rate and be delivered more professionally than ever before. Being unaware of these risk puts an organisation at heightened risk. Not knowing, or not caring, is not a valid option anymore.

Darkscope delivers new tools that help our clients to be prepared for any attack before it is delivered, by looking in the places the attacks are created. Darkscope has a range of solutions that deliver improved cybersecurity for our clients. These include Cyber Risk Assessment™, Cyber Watchtower™, Domainwatch™ and eScamwatch™.

Cyber Risk Assessment

The Darkscope Cyber Risk Assessment is a comprehensive assessment of an organisation that considers all cyber-related risk vectors inside and outside of the organisation. The output is an actionable comprehensive report which can be added to an Enterprise Risk Management (ERM) plan or can stand alone. It delivers much more than any maturity model assessment as it considers cyber risk factors external to the organisation.

Cyber Risk Score

A Darkscope Cyber Risk Score is an organisational digital risk profile. It details the danger of a cyberattack – phishing, ransomware, denial of service, data or intellectual property theft.

The Darkscope Cyber Risk Score investigates more than the IT in an organisation and will deliver far more than any maturity model assessment can, as it can identify real and present threats. Looking outside the organisation and interrogating its footprint on the internet, in social media and the hidden parts of the internet, a.k.a deepweb and darknet, the Cyber Risk Score provides a meaningful actionable result.

Cyber Watchtower

Using our networks in the deepweb and darknet and our state of the art artificial deep neural networks, Cyber Watchtower provides strategic threat intelligence ahead of any attack, phishing or hacking attempt to an organisation.

EScamwatch

Pretending to be Apple, DHL, or Microsoft in an email is a common form of phishing or email scamming. Darkscope monitors thousands of email addresses similar to our client's email addresses to detect fraud, phishing or other malicious activities in the name of our client organisations.

DARKSCOPE

THE CYBER WATCHTOWER

DomainWatch™

Domainwatch monitors the internet for new domain registrations and sub-domain builds, to find potential scam sites that are the landing pages for phishing, smishing^ and spoofing attacks.
Spear-phishing attacks use fake sites of known organisations to attempt to scam passwords or credit card details from their targets. Many of these sites replicate the site of the organisation that they are spoofing and are difficult to differentiate from the original for most people. When they spoof the site of an organisation, there is a risk of stolen private information, credentials, passwords or credit card information. This can lead to a cybersecurity breach.

State of the Cyber War

Cybercrime in 2017 was valued by CSIS at US$600 billion. It is now the most lucrative criminal activity. Major players in cybercrime include criminal organisations out of Eastern Europe, Africa, China and Korea, and what are called "nation-state" actors from the same regions. The primary motivation for cybercrime is money. Through the theft of personal information (bank and credit card details, medical records, identity) password and login details, intellectual property, and customer or other databases, cybercriminals sell or use this information for profit.

State-sponsored cybercrime targets similar data for different reasons. Those with agendas to promote can also be cybercriminals in their social and political activism – Anonymous attacking a legitimate business for a social cause is cybercrime.

Cybercrime has become more professional than the "Nigerian Prince" scam that we all know. Preparation for an attack on an organisation can take weeks or months before launching. To prepare and perform these activities cybercriminals need a place that is out-of-sight of their target- somewhere in the internet.

Traditional cyber defences, such as firewalls, AV, UTM, DDoS mitigation, DLP, IPL, IDS, proxies, sandboxing, etc., are all passive – they can do nothing until an attempt to breach security happens. Unfortunately, these tools are not particularly good at protecting the organisations that use them. According to Verizon*: 76% of breaches were financially motivated; 50% were carried out by organised criminal groups. Mandiant^ tells us that global median time hackers are on a network before being discovered is 101 days. This blows out to 175 days in EMEA and 498 days in APAC. To help prevent an attack we should know more about where they come from – the internet.

The Internet

The visible, or surface, internet is a tiny part of the whole internet. Depending on whose numbers are used, 96-99% of the internet is hidden from search engines. This hidden part is called the deepweb. In the deepweb there are legitimate sites and activity (46-47%). These include law, intelligence and other databases, gaming, email services, storage services, private and public cloud. To access a site in the deepweb you simply need a password.

Inside the deepweb there are also illicit sites – those that are set up to promote crime, drug sales, hacking, fraud, exploitation and even political hacktivism and extremism. The illicit part of the deepweb is 50-52% of the internet. Within the deepweb is the darknet, where the worst activities happen. The difference between the deepweb and the darknet is in how someone engages. Passwords get you in to the deepweb but to enter the darknet you must know where to go, and how to get there.

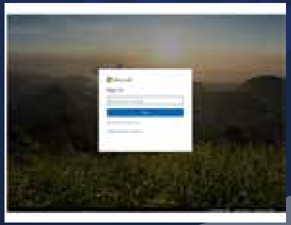
Information about an organisation in the deepweb and darknet cannot be found using search engines but may represent a risk to the organisation. It may be exfiltrated data, or the preparation for a planned hack, phishing or other attack. The data may be held, or for sale. Whatever reason it exists, it represents a security risk to the organisation.

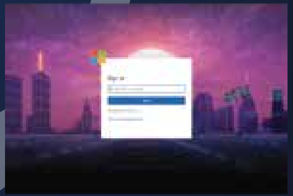
A Cyber Risk Score helps an organisation by exposing the potential risks which cannot be seen or differentiated from normal internet behaviours. With this information the organisation can prepare for and prevent a cyberattack against them.

Darkscope DomainWatch

Bogus domains are the landing pages for many scams. By constantly monitoring for new domain registrations, subdomain changes, domain spoofing, and doppelganger sites, Domainwatch can identify potential scam sites. Using Artificial Intelligence (AI), crawlers, and search engines to find these sites. Many of these fail Domainwatch scrutiny because of three common mistakes: typo's, spelling and grammar.
Spear-phishing attackers create fake sites of known organisations to attempt to scam passwords, credit card details and other personal information from their targets. These domains try to accurately replicate the site they are spoofing, and they work because most people find them difficult to differentiate from the original with the human eye.
Finding replicant or duplicated domains is not hard to do, when they have the same digital footprints. Finding domains that have the same information and look similar, but are digitally different, is a more complex process. It requires the ability to look and see as the human eye would. These two example pages carry the same information but are digitally different – one is real, and one is fake.

Using our unique Deep Artificial Neural Networks (DANN), Domainwatch compares the pages as a human would do.





The DANN alerts us where the page is too similar to the original. More importantly, our AI is trained to find the differences as well as the similarities and to compare pages like a human would do.
Domainwatch is different from competing services which can only find doppelganger or replicated sites. Being able to 'see as humans do', it can find these fake domains and alert the real domain owners allowing them to act to protect their customers from potential scams and protect their intellectual property, brand and reputation