CORVID

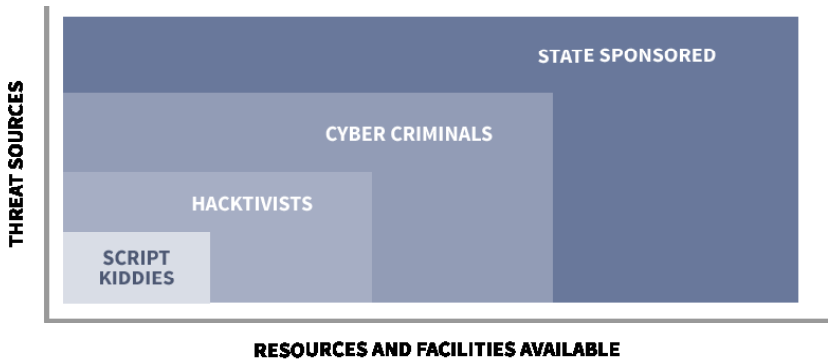
CORVID COMPROMISE ASSESSMENTS

Industry experts may warn that cyber breaches are inevitable but, with a CORVID Compromise Assessment, the loss of data and the reputational damage is not.

Attackers are well aware of how antivirus and firewalls work and design their attacks to evade detection. Fight back with a CORVID Compromise Assessment. Our cyber security specialists – supported by our own up-to-the-minute, constantly evolving intelligence – will complete a forensic-level inspection of your hosts and internet traffic to determine if an attacker has gained a foothold, providing analysis and stopping them in their tracks.

The threat landscape never stands still...

State sponsored attacks are becoming more widespread, no longer focusing solely on governments and the largest companies. In parallel, cyber-criminals are becoming more sophisticated, demonstrating techniques that routinely evade traditional defences.



The threat landscape is constantly evolving and spans a variety of threat actors. One thing is certain - none should be underestimated

A few years ago we believed we were protected if antivirus was installed, if passwords were updated and if users did not open suspicious files and links. As the decade comes to an end however, we are told that 230,000 new malware samples are produced every day[1].

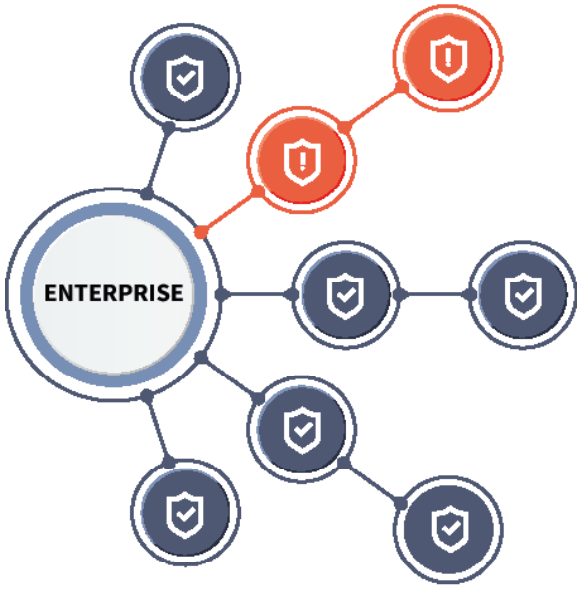
As it can take months for antivirus providers to encounter a new malware sample and update their detection signatures, attackers remain one step ahead. More worryingly, we routinely see attackers spoofing email accounts, imitating admin users and using encrypted communications to undertake their activities, meaning organisations are unable to detect and analyse breaches.

[1] https://thebestvpn.com/cyber-security-statistics-2018/

Key Business Benefits

- Remediate active breaches and understand impact through in-depth threat hunting.
- Prevent recurrence by understanding how attackers got in and making relevant improvements.
- Identify and remove sophisticated malware not detected by other defences.
- Flag security flaws and past data leakage through identification of legacy compromise.
- Ensure systems are free from compromise before joining them together as part of a supply chain or acquisition.
- Prove the effectiveness of your security measures to customers and suppliers.
- Ensure operational activities are not impacted - no system downtime or need to reconfigure your systems.

And sadly it is not only *your* data that is at risk. Many businesses also rely on complex supply chains. Threat actors are increasingly targeting an organisation through focusing on the least secure elements within its supply chain.
As such, not only does an organisation's cyber security measures affect itself, but they also have an impact on its customers and suppliers and, therefore, also its business.

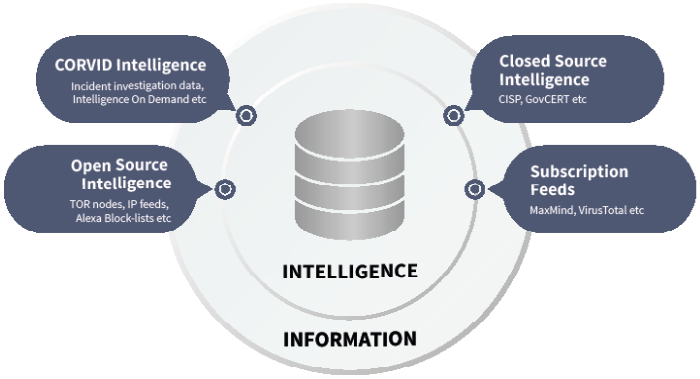


The threat landscape never stands still…

…And neither do we

With a CORVID Compromise Assessment, metadata from your systems will be examined by a team of highly skilled analysts hunting for the tell-tale signs of sophisticated security breaches designed to evade antivirus and intrusion detection.

Before the assessment begins, our analysts will discuss the nature of your infrastructure, likely risks and ask about incident history. This will enable the right assessment to be designed for your organisation. The assessment, typically run over a four-week period, will capture computer metadata which describes the software installed on the computers and servers, as well as networking information, used to identify rogue processes.



CORVID's success is based on innovations in Intelligence on Demand, a vast in-house library of detection techniques and signatures, a unique metadata-generation application and analysts with experience of investigating the most advanced attacks.

The assessment focuses on two key areas:

Endpoints: the endpoint assessment is completed via a frictionless, low-interaction CORVID agent which generates performance metadata. This data is inspected by our analysts to detect:

- Unknown malware such as droppers, trojans, worms and RATs.
- Persistent backdoors which allow attackers to maintain a foothold inside your network.
- Potentially unwanted programs which can increase your attack surface.
- Shadow software, installed without approval, and not covered by company security protocols.
- Malicious executables (through process and file analysis).
- Fileless malware.
- Hijacked processes and malware using advanced-masquerading techniques.
- Lateral movement which allows attackers to spread across your systems.

Internet DNS resolutions: through analysis of DNS lookups, our analysts identify:

- Access to known dangerous sites.
- Beaconing processes, signalling infection.
- Suspicious process behaviour.

At the end of the assessment you will receive a detailed report, highlighting areas that were investigated and explaining the results to give you confidence and reassurance regarding the state of your IT.

With so many providers, why should you select CORVID for your Compromise Assessment?

Our customers choose CORVID because we offer government-grade solutions for managed cyber defence. We have proven experience of defeating attacks from state sponsored sources and criminal gangs, and our analysts routinely investigate targeted and untargeted campaigns.

> *"We use the CORVID Compromise Assessment as part of our acquisition strategy. The assessment gives us peace of mind that the computer systems of the target company are safe and not already housing attackers. The report has become a key factor in determining whether the acquisition presents undue risk to our existing business."*
>
> COO – FINANCIAL SERVICES COMPANY

With CORVID you receive:

- A lightweight, frictionless agent that gathers all the information it needs- there is no need to gather audit logs or change your settings.
- Complete discretion guaranteed – no one will ever know what the findings are and you will not appear as a case study for marketing purposes.
- Highly experienced security analysts with backgrounds in the intelligence and defence communities, supported by machine learning and heuristics.
- Up-to-the-minute intelligence and Intelligence on Demand as a result of our proprietary technology and intelligence.
- On-going communication throughout the assessment.

About CORVID

CORVID was developed by Ultra Electronics, a FTSE 250 company, to safeguard its military, aerospace and critical infrastructure data as well as that of its customers and supply chain.

Ultra's pedigree enabled it to identify that traditional cyber-defences were insufficient to combat the evolving complexity of threats – as a result the CORVID initiative was started to provide a better and more comprehensive solution to the cyber problem. At the request of suppliers and business partners, it was decided to make CORVID available as a commercial solution to all organisations.

Completing a Compromise Assessment of your network will help identify existing compromises and potential risks, allowing you to remediate issues and strengthen security. As a result, you will be better equipped to protect your data and that of your customers and suppliers, enhancing your reputation and complying with legal and regulatory obligations.

Get in touch

To find out more and discover how a CORVID Compromise Assessment can help your business please get in touch.

CALL US
+44 1242 651251

EMAIL US
contact@corvid.co.uk

VISIT US
www.corvid.co.uk

Arle Court, Hatherley Lane, Cheltenham, Gloucestershire, England, GL51 6PN