 CORVID

CORVID COMPROMISE ASSESSMENT

Gain confidence as a one-off service or part of your annual security audit.

Cyber criminals are well-versed in how anti-virus programmes and firewalls operate, and design their attacks to evade detection. You need to be confident that your systems are free from compromise, to ensure the security of your operations, finances and reputation.
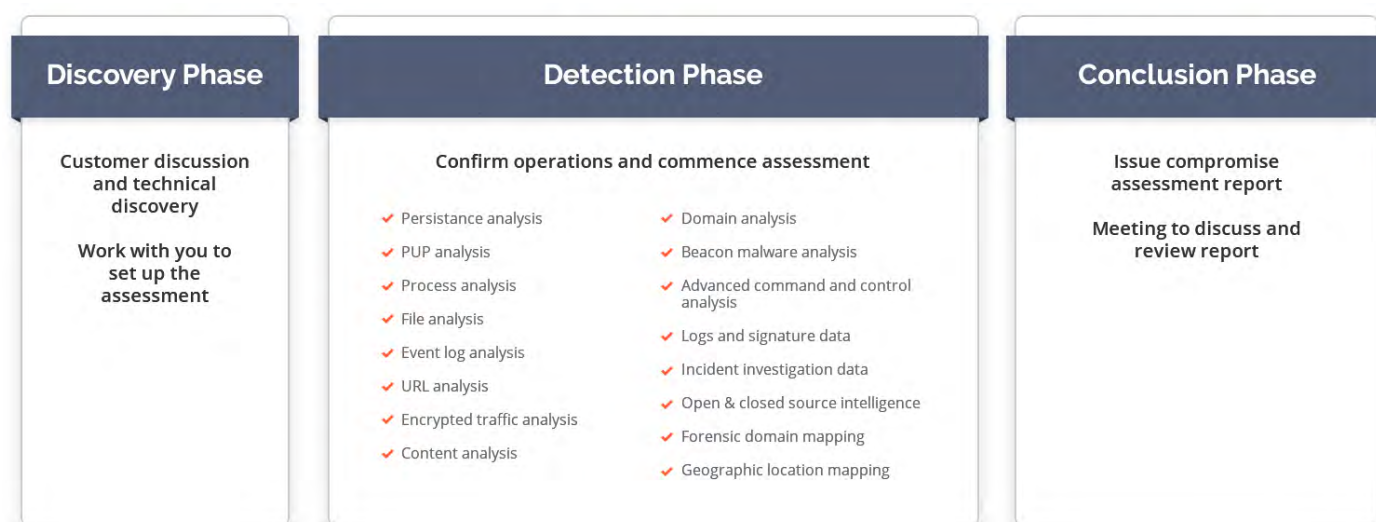
What is a CORVID Compromise Assessment?

A CORVID Compromise Assessment is a forensic-level inspection of your IT estate to determine whether you are, or have been, compromised. If active attacks are identified, our analysts will provide all the details and support needed for full system recovery, with minimal disruption to users. Each bespoke assessment is tailored to reflect your level of concern.

How does it work?

Typically run over four weeks, your Compromise Assessment takes into consideration the nature of your infrastructure, likely risks and any incident history, to enable us to design the right assessment for your needs. Our team of highly skilled analysts examine metadata from your systems, hunting for signs of malicious activity which have evaded your existing security defences.

We'll update you on a weekly basis to inform you of our progress and any routine findings. If we identify something that appears to be actively malicious, a CORVID analyst will contact you immediately to advise you of your options, to isolate the incident and enable swift remediation.

Discovery Phase	Detection Phase	Conclusion Phase
Customer discussion and technical discovery Work with you to set up the assessment	Confirm operations and commence assessment ✔ Persistance analysis ✔ Domain analysis ✔ PUP analysis ✔ Beacon malware analysis ✔ Process analysis ✔ Advanced command and control analysis ✔ File analysis ✔ Logs and signature data ✔ Event log analysis ✔ Incident investigation data ✔ URL analysis ✔ Open & closed source intelligence ✔ Encrypted traffic analysis ✔ Forensic domain mapping ✔ Content analysis ✔ Geographic location mapping	Issue compromise assessment report Meeting to discuss and review report

Endpoint assessment

Our frictionless agent gathers performance metadata, which is inspected by our analysts to detect:
- Unknown malware, such as droppers, trojans and worms
- Persistent backdoors that allow attackers to maintain a foothold in your network
- Potentially unwanted programmes (PUPs) which increase your attack surface
- Shadow software installed without approval, which isn't covered by your security protocols

- Malicious executables
- Fileless malware
- Hijacked processes and malware using advanced masquerading techniques
- Lateral movement by attackers across your network

Once your Compromise Assessment is complete, we'll provide you with a detailed report covering areas of analysis, our findings, and any remediation advice – comprehensive insight into the health of your IT estate.

Considering an acquisition or merger?

No matter how secure your systems are, linking with a weak or poorly protected system gives attackers an easy route into your IT estate. Commission a one-off CORVID Compromise Assessment for the system you're linking with, for peace of mind that any existing vulnerabilities or breaches are identified and fixed before they can cause damage to your systems.

Key business benefits

✔ **Identify if you've been compromised** – we'll carry out a comprehensive inspection of your hosts and internet traffic to determine if you are, or have been, compromised. Our in-depth threat hunting articulates how the breach happened, and provides answers to help you understand the impact to your business

✔ **Ensure no weak links** – cyber criminals target the weakest link in a supply chain. Carrying out a CORVID Compromise Assessment before an acquisition or merger gives you peace of mind that their systems are free from compromise before linking with your own.

✔ **Tailored to your security concerns** – using proprietary tech we've developed in-house, alongside the latest threat intelligence, we provide a bespoke, flexible service that addresses your business' security concerns.

✔ **Demonstrate compliance** – we'll help you meet strict compliance requirements, to strengthen your information security risk methodology. Our clear report details any data breaches, as well as your overall cyber health, which can provide reassurance to your customers and suppliers.

✔ **Remediate active breaches** – if we identify an active breach, our team will halt the adversary in its tracks and eradicate all malicious activity. If malware is found that hasn't been detected by other defences, we'll remove that too.

✔ **No user disruption** – the Compromise Assessment is non-intrusive, so your users won't be aware it's taking place. Our agent operates in low priority, ensuring user activity is unaffected and daily operations are not interfered with, blocked or denied.

About CORVID

We're an experienced team of cyber security experts, developers and analysts who are passionate about delivering innovative, robust and extensive cyber defence solutions and services to help protect businesses against cyber threats.

Find out more

Get in touch to discover how a CORVID Compromise Assessment can help your business.

CALL US
+44 1242 651251

EMAIL US
contact@corvid.co.uk

VISIT US
www.corvid.co.uk

FIND US
in 🐦 ▶

CORVID

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