

Compromise Assessment

What is a Compromise Assessment?

Whether in response to a suspected breach, as part of M&A due diligence, or as part of a regular security health check, compromise assessments uncover breaches, gauge their severity, and provide strategies to stop them. By focusing on evidence of past or ongoing malicious activity such as unauthorised access, malware, or data exfiltration, compromise assessments are a key tool in ensuring critical data is secure.

OccamSec's Process

Our compromise assessment team operate as part of our active defence group. They conduct threat hunts, incident response, purple team exercise and compromise assessments. Utilising the latest indicators of compromise (IOC's) combined with experience across sectors, they execute the process below to determine if an environment has been infiltrated, how it occurred, and how to remedy the situation.



Figure 1 : Compromise Assessment Process

The assessments goal is to uncover malicious behaviour, isolate it, and remove it from the environment. The path the attacker took is also uncovered, enabling customer security tooling to be re-configured in order to prevent similar breaches in the future. Our work in red teaming and penetration testing gives us a unique knowledge of how attacks happen and what adversaries look for in target environments.

At the conclusion of the assessment the deployed technology can either be removed, or the project can evolve into an ongoing threat hunt to provide further protection from skilled threat actors.

Brands that Trust us



Why Conduct a Compromise Assessment

For various reasons, security controls do not prevent all attacks from succeeding. Skilled adversaries can bypass monitoring systems, evade endpoint solutions, and exfiltrate data undetected—something OccamSec's assessment team does regularly. Attackers can dwell in a network undetected for months. Compromise assessments can answer a range of related questions. Some examples include:

- Is our recent acquisition safe to connect to our internal network?
- Are there are remnants of the security incident still in our network?
- Does the organization we just invested in still have the intellectual property we bought it for?
- Do we have a breach in progress that is going to impact our regulatory compliance?
- We have an IOT environment in a specific region that we need to confirm has not been compromised.

In the specific case of M&A compromise assessments are sometimes conducted as part of the due diligence process. The potential for this depends on the specifics of the deal and in some cases clients have engaged us to perform these activities only for us to encounter considerable road-blocks, which has nearly always been an indicator that an incident has already occurred.

Where Does it Fit?

Compromise assessments are not alternatives to red teaming, penetration testing, incident response, or purple team exercises. A predominantly reactive exercise, the assessment determines if an attack has already happened and assesses its impact.

Given the nature of the activity, a compromise assessment may trigger an organization's incident response process. Therefore, it is vital to have a plan in place for this scenario. Additionally, some level of security tooling must also be in place.

The Cloud?

We are often asked if compromise assessments can (or should) be conducted on cloud-hosted environments. The answer is always yes—the cloud is no different from any other technical environment. While there are nuances in its operation and attack vectors may differ, cloud systems are still vulnerable to security breaches, and adversaries can still wreak havoc in them.

Cloud-specific breaches can include misconfigured storage buckets, insecure APIs, and compromised account credentials. Attackers may exploit these vulnerabilities to access sensitive data, launch denial-of-service attacks, or gain unauthorized control over cloud resources. Additionally, lateral movement within cloud environments, such as through compromised virtual machines or poorly secured cloud functions, can lead to widespread compromise and data exfiltration.

Given these potential risks, compromise assessments are essential for identifying and addressing cloud-specific security issues, ensuring the integrity and security of cloud-hosted environments.

Increase Confidence in Your Environment

A compromise assessment offers peace of mind by identifying and mitigating hidden threats within your systems. Cyber attacks are always evolving, there will always be a new method to bypass security controls and a layered defense, while beneficial, may still have gaps that attackers can slip through. Reducing the potential for this to exist, long term, in your environment, is vital for an organization to confidently conduct its operations.