Compromise Assessment

Get 100% assurance that your environment is free from any ongoing or prior threat actor activity.

In today's world, data breaches and cyber attacks are increasingly common, and often go undetected for long periods of time. A ThreatDefence Compromise Assessment leverages our team's extensive experience responding to advanced attacks, cutting-edge threat intelligence and our proprietary SecOps technology to provide an in-depth analysis of your organization's security posture. Our assessment aims to:

- Detect ongoing or previous intrusions within your network
- Evaluate risk by identifying security architecture weaknesses, vulnerabilities, policy violations, and system security misconfigurations
- Enhance your organization's incident response capabilities.

Leverage our SecOps platform and our experience in incident response and digital forensics to get a thorough, forensic-like review of your environment over an extended period of time. We'll activate our deep visibility toolset and analyze every endpoint, cloud service and network flow to discover any anomalies in your network and ensure that your environment is secure and not compromised. The service will help you to reveal any existing or past intrusions, identify vulnerabilities or weaknesses, detect malicious activity,improper usage, policy violations and security misconfigurations.

Visualize All Your Data

Our team will ensure that all your security data is recorded and analyzed in our platform, providing you with deep visibility across your entire environment.

Conduct Forensic Analysis

We leverage our Machine Learning and AI technology to analyze your entire attack surface, including user behavior, connectivity patterns and software activity.

Action on Recommendations

Get a detailed and actionable report with all documented exposures, weaknesses compromises and associated recommendations.

Identify Unknown Threats

Our process includes manual in-depth analysis by our security analysts and threat hunters, identifying abnormal behavior and defense evasion.

Discover Dormant Malware

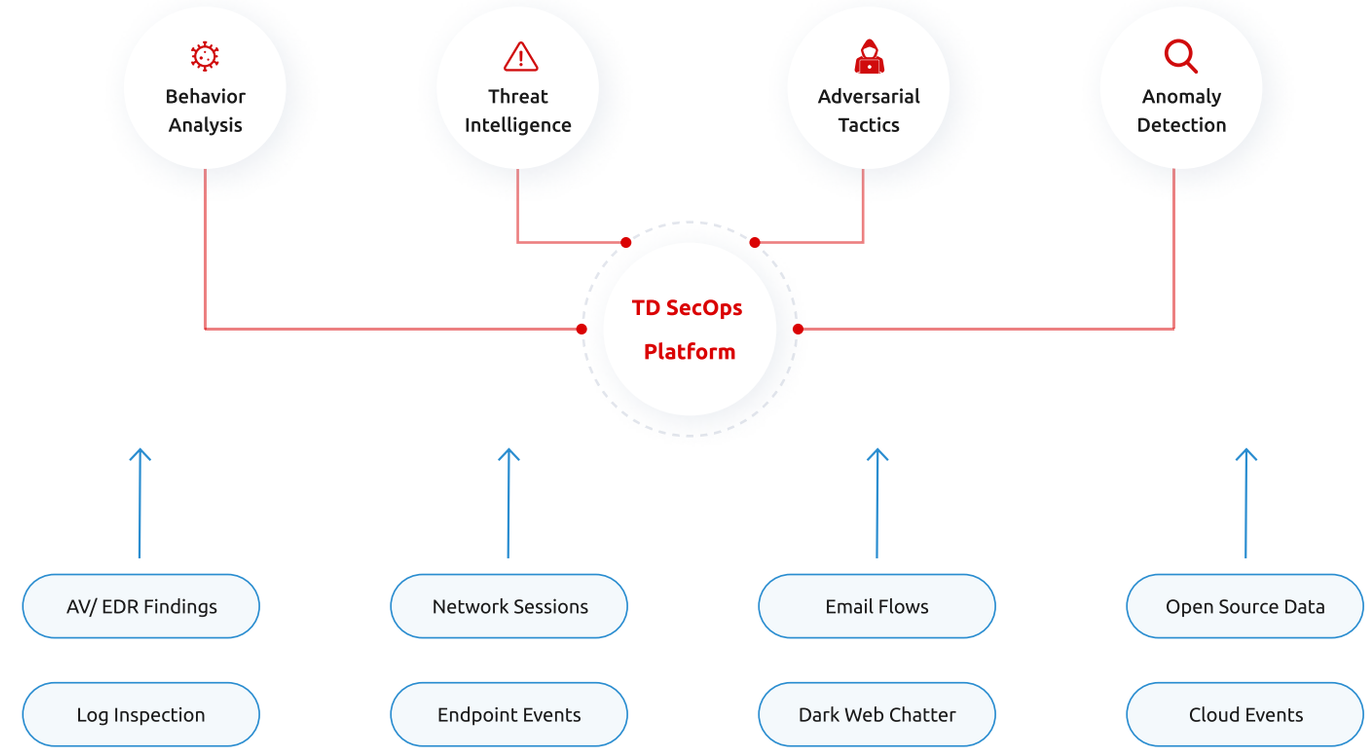
We inspect your environment over an extended period of time to identify any dormant malware or covert threat actors that may have gone undetected.

Our Approach

Our Compromise Assessment combines our state-of-the-art visibility technology with our extensive experience in responding to sophisticated breaches and investigating security incidents. With a focus on deep, forensic analysis that goes beyond the standard scope of common security tools, we integrate all your security data into the assessment process.

This includes data that resides directly within your network and endpoints, as well as external data such as cloud workloads, SaaS applications and Dark Web breaches. We also analyze compromised credentials, external vulnerabilities, and any weaknesses or exposures related to third-party organizations in your supply chain. Our service offers flexible deployment options that can be tailored to meet the specific needs of your organization, including both on-premises and cloud-hosted technology.

- Gain insights into attacker attribution and motivation for targeted organizations
- Identify security architecture and configuration weaknesses, including missing patches or misconfigurations
- Recommend strategic options to better prepare the organization's security team to respond to intrusions.



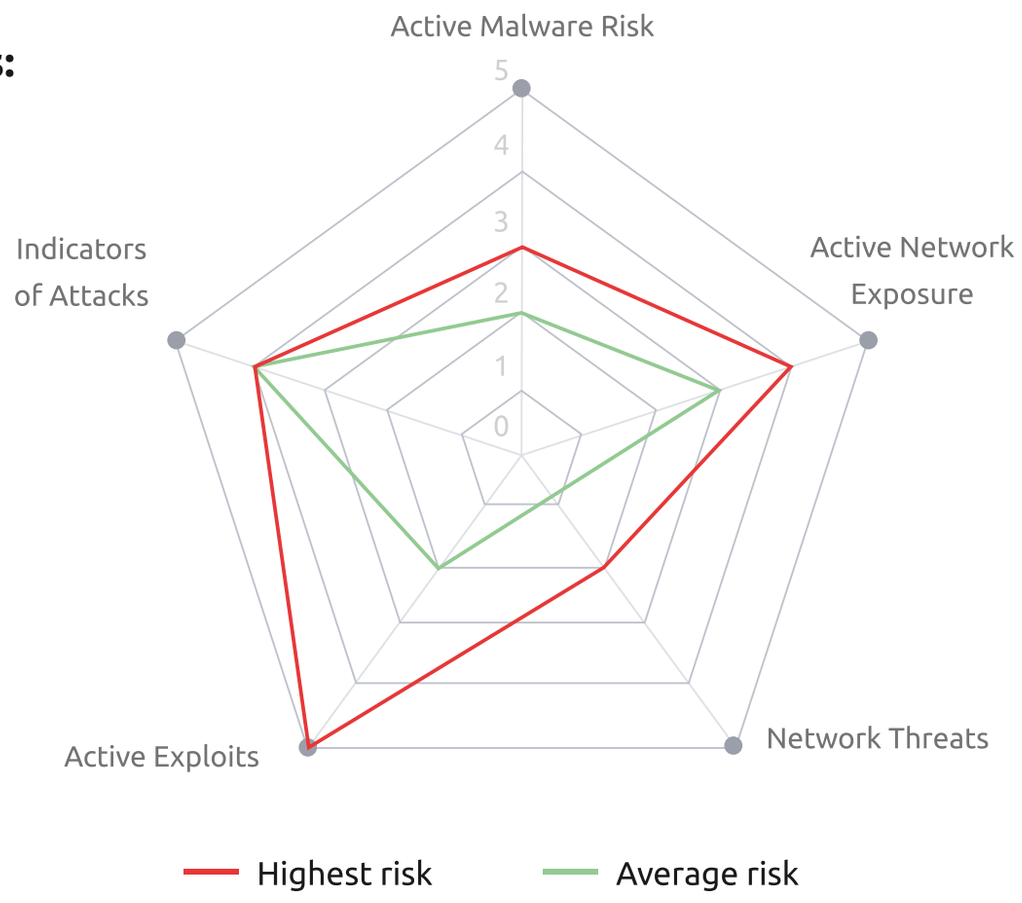
What You Get

You will get a comprehensive review of your environment empowered by our real-time security analytics. We review your infrastructure, systems, networks, applications and cloud systems to quickly determine the presence of current or past attacks. We also provide a view into your organization's systemic risks and exposures, identifying any security program hygiene issues that may exist.

Additionally, our team of experts will then make best practice recommendations to further enhance your organization's ability to effectively respond to future incidents.

Get a detailed report with answers to these questions:

- **Who is targeting you and what are they after?**
- **How effective your security controls?**
- **What can be done to prevent any attacks in the future and increase your cyber resiliency?**



Areas of Concern

Although many organizations still prioritize their protection techniques to detect threats based on a 'point in time' analysis of malicious behavior, intruders rarely execute their entire mission in a few minutes or hours. In fact, the most sophisticated intruders often persist for months or years at a time. Time series analysis is the key factor in detecting compromises, as many persistent threat actors adopt great operational security techniques. Targeting an extended window of time to expose numerous attacker actions, from initial unauthorized access to ultimate mission accomplishment, allows us to detect and contain the most sophisticated adversaries.

- **Identification of malware, unauthorized access, data exfiltration, and other violations**
- **Machine learning analysis of user and machine behavior**
- **Deep analysis of your security data**
- **Detailed report with your security risks and exposures**
- **Security weaknesses, vulnerabilities, system and application misconfigurations**
- **Reports of attacker activities and detailed timelines**
- **Best practice recommendations**
- **Evidence of ongoing or past compromises**

Endpoint Analysis

Our endpoint analysis employs endpoint agents to monitor and detect potential attacker activity, such as malware usage and other malicious techniques. We cover a broad range of operating systems, including Windows, macOS, and Linux, supporting both on-premises and cloud-based deployment options.

Cloud Analysis

Our cloud sensors collect security data from all your cloud environments, whether they are private or public. We not only analyze your cloud systems for any signs of compromise, but also identify any misconfigurations, vulnerabilities, and exposures that could lead to potential security breaches.

Network Analysis

Our network sensors are placed in strategic locations within your enterprise to monitor and detect any signs of compromise. This includes detecting communication with malware command and control servers, unauthorized remote access attempts, data exfiltration, and malicious reconnaissance.

Log Analysis

Our network sensors are strategically placed throughout your enterprise to detect any signs of compromise, such as communication with malware command and control servers, unauthorized remote access attempts, data exfiltration and malicious reconnaissance.

ABOUT THREATDEFENCE

ThreatDefence provides innovative Security Operations and cyber defense solutions to MSPs and Enterprises. Our SecOps Platform is designed to assist businesses of all sizes in implementing world-class detection and response, utilizing all available data sources, whether it be within their network, on the Dark Web, or concealed deep within their supply chain. We value open ecosystems and seamlessly integrate with any and all threat intelligence feeds and log sources, delivering immediate actionable security insights.

For more information, visit
www.threatdefence.com

Phone:
1300 122 434

Email
team@threatdefence.com

Address:
Level 11, 88 Pitt St, Sydney,
NSW 2000