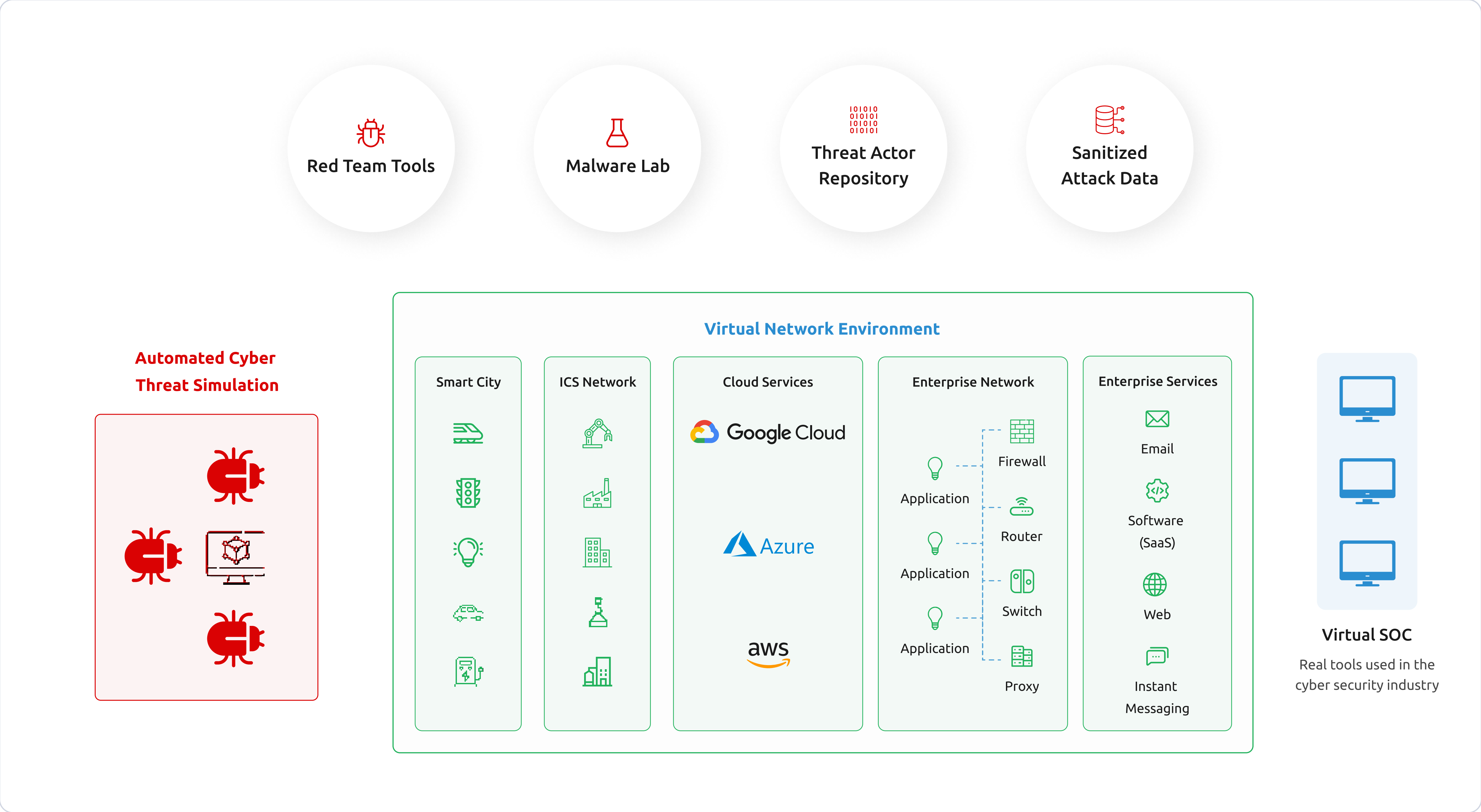
Cyber Security Training and Attack Simulations

Get your team ready for the next cyber event.

The cybersecurity landscape is constantly evolving and growing more complex, with new threats and attack techniques emerging on a daily basis. Unfortunately, many security operations teams are not adequately prepared to handle the intricacies of modern cybersecurity incidents. Threat actors evolve quickly and use increasingly sophisticated tools, achieving their objectives in just hours and causing serious harm before the threat can be contained. Even when an intrusion is detected, security operations teams often lack the experience to act decisively, struggling to counter the tactics of experienced and sophisticated attackers.

Although many cyber security training programs offer some level of simulation exercises, these simulations are typically conducted in simplified training environments that do not replicate the complexity of real systems, such as complex enterprises, multi-cloud environments or industrial networks.

That's where ThreatDefence comes in. We offer a comprehensive cyber range and cyber attack simulation solution that enables organizations to develop their cyber skills using real data and real adversarial attacks recorded during actual cyber incidents. Our solution provides a hands-on, real-world training experience that empowers SecOps teams to respond quickly and effectively to real-life cyber threats.



Datasheet

threatdefence_

Develop Practical Cyber Security Skills

Cybercriminals are constantly devising new ways to penetrate organizational defenses, and the shortage of skilled cybersecurity professionals has made it even more difficult to keep sensitive data secure.

To address this challenge, it is essential to invest in real-world cyber security training that incorporates real data and simulations of actual attacks. This type of training provides cybersecurity professionals with hands-on experience that replicates real-world scenarios, helping them to identify and respond to cyber threats more effectively. It also allows them to develop the skills and strategies needed to protect sensitive data from being compromised.

By using data from real-world adversary attacks in training, professionals can analyze attack patterns, identify vulnerabilities, and develop appropriate defense mechanisms. This type of training can help organizations to stay one step ahead of cybercriminals, and to protect their data and assets from being compromised.

Our SecOps platform supports complex cyber security scenarios, simulating large enterprise and industrial networks. The platform facilitates teamwork and collaboration, organizing trainees into groups dedicated to achieving specific missions and objectives. Our value proposition is a practical and sustainable Security Operations toolset that can be used for various educational and training applications. We focus on practical cyber security skills that can be immediately applied in real-world situations.

Comprehensive Cyber Range

At ThreatDefence, we prioritize the value of practical, real-world cyber security training that can be applied directly to the environment that trainees work in. We provide a virtual cyber range solution that allows organizations to create replicas of their real systems, cloud environments, and networks. This approach ensures that trainees are training on scenarios that are relevant to their job or desired career path and can be immediately applied to their day-to-day work.

Our training scenarios are intentionally designed to be complex and open-ended, and require critical thinking and creative problem-solving skills to address realistic cyber threats. The simulations are organized based on the MITRE ATT&CK framework, which provides a common language for discussing and understanding the various phases of a cyber attack. Our solution goes beyond just training on theoretical concepts; we emulate real adversaries like APT29, running their tools, techniques, and tactics on your cyber range. By modeling adversarial behavior and objectives, such as data exfiltration, espionage, or ransomware deployment, trainees are able to develop a comprehensive understanding of real-world threats and how to defend against them.

Create replicas of your infrastructure

Simulate enterprise networks and services, public cloud environment, and critical infrastructure.

Run practical exercises

Organize trainees in teams and run simulations focused various Red Team or Blue Team skills.

Model adversary behavior

Execute complex, multi-staged scenarios employing tools, tactics and techniques from advanced threat groups.

Simulate zero day attacks

Prepare your team to detect and response to major cyber events, including zero day attacks.

Our cyber security simulations allow organizations to simulate any kind of attack scenario, including zero-day or supply chain attacks, when one of your critical suppliers or software modules is compromised. These simulations put trainees into real cyber crisis scenarios, adding group collaboration and time pressure, further enhancing the effectiveness of the training. The training scenarios can last multiple days, providing trainees with a thorough understanding of how to handle a complex cyber security incident from start to finish.

Collaborative SecOps Workspace

Integrating cyber security training into your working processes is a key way to ensure that your team is ready to handle real-world cyber threats. This approach not only helps trainees to develop their skills in a more practical way, but also allows them to understand how to work collaboratively with other members of their team. Our cyber range can be used in conjunction with your production SecOps tools - by shadowing SOC analysts, trainees can learn from their actions and see how their training can be applied in practical situations. This approach allows trainees to learn from experienced professionals and observe how they handle complex cyber incidents. Additionally, trainees can test their skills in practical situations, allowing them to apply what they have learned in a real-world context.

ThreatDefence enables cross-skilled cyber security training with both offense and defense-focused simulations. Blue Team training involves simulating attacks on your systems and networks, allowing trainees to develop and test their defense capabilities in a controlled environment. Red Team training, on the other hand, involves simulating attacks on your systems and networks by a team of experts who act as attackers, giving trainees the opportunity to see how attackers operate and learn how to detect and respond to real-world attacks.

Blue Team

Get hands-on experience as a SOC analyst using real-world tools and analyzing real data:

- Data visualization and analysis
- Threat hunting
- Digital forensics
- Incident response
- Reverse engineering
- Sanboxes
- Machine learning lab

Red Team

A complete red team toolset with real attack data, real-world adversary profiles and behaviors:

- Model adversary behavior
- Simulate real attacks with real data
- Categorise threats
- Run penetration testing scenarios
- Scan for vulnerabilities
- Malware lab
- Up-to-date repository of real threat actors

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