CYB3R OPERATIONS

Accelerating Your Ability to Identify, Assess, and Respond to Third Party Risks

Corporate Deck

TLP:AMBER

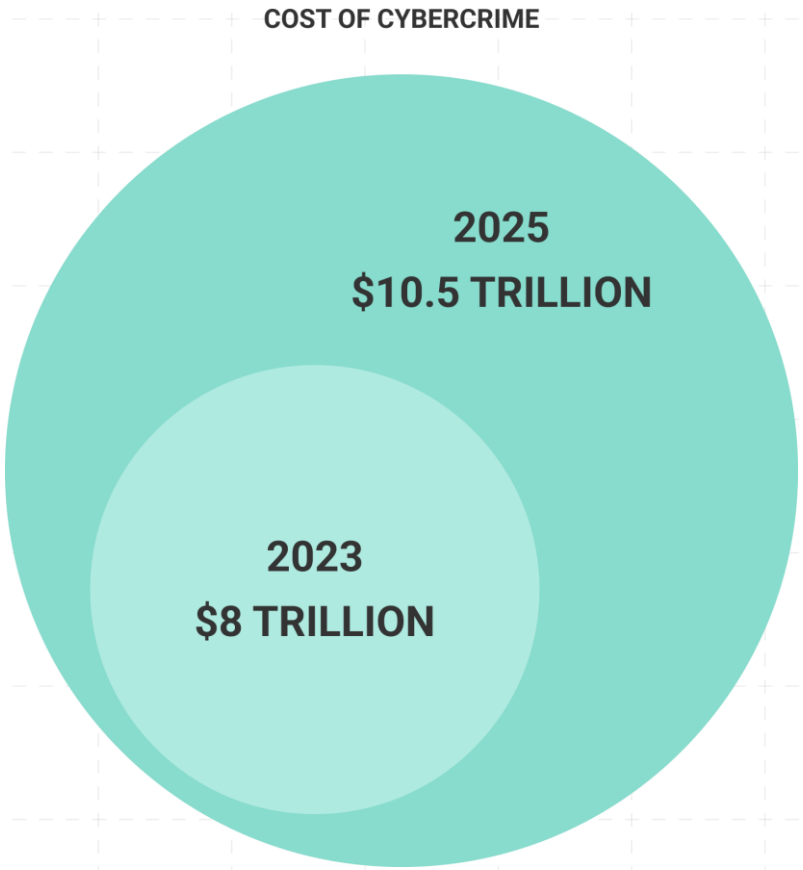
CYB3R OPERATIONS

Challenges combating third party risk

- **Lack of Third-Party Visibility:** security teams are responsible for knowing which third parties operate around or within their environment. Often, this data is siloed and difficult to access.

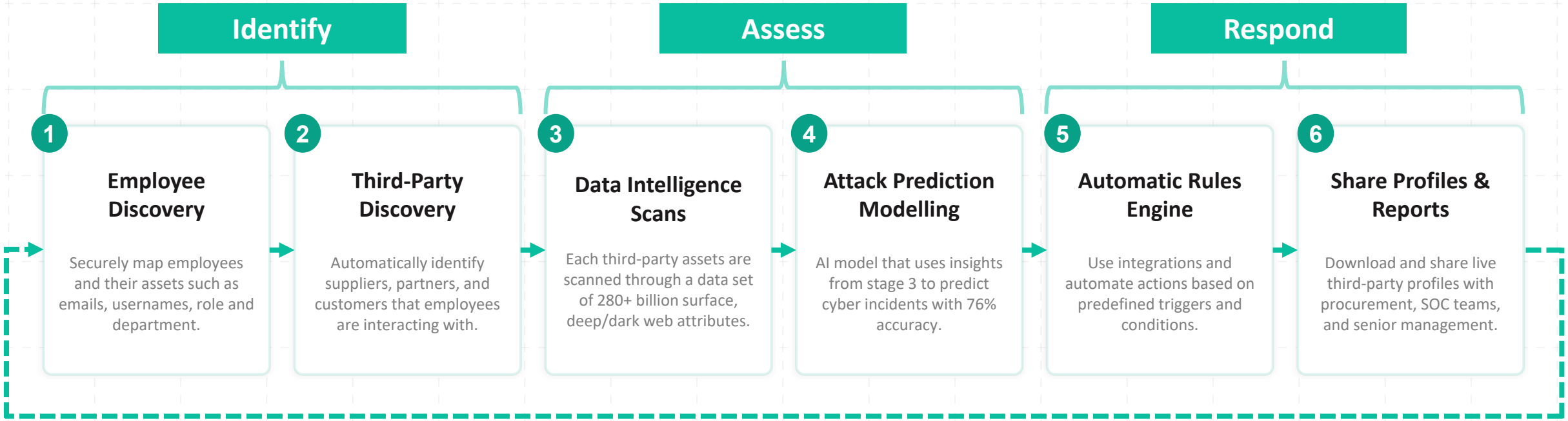
- **Inability to Assess or Predict Risks:** Without third party visibility, businesses struggle to evaluate or foresee risks posed by external organisations, which can lead to severe business impacts such as reputational damage, financial fraud, or ransomware attacks.

- **Automation Challenges:** Even if security teams could predict risks, they face significant challenges in automating responses to mitigate these risks, complicating their ability to efficiently manage and neutralise potential threats.



CYB3R OPERATIONS

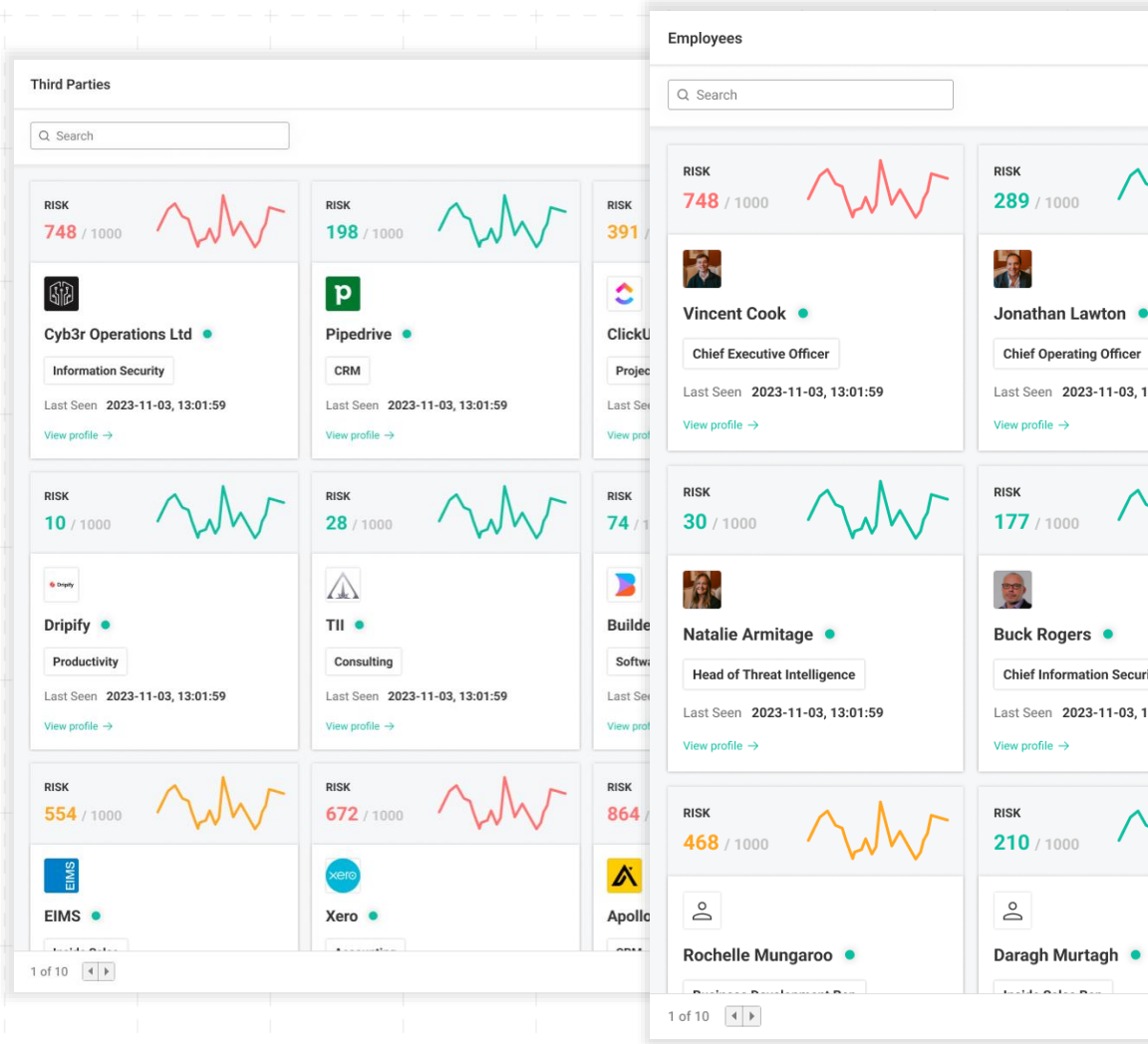
Constant End-to-end threat prediction and mitigation



CYB3R OPERATIONS

Automatic discovery capabilities

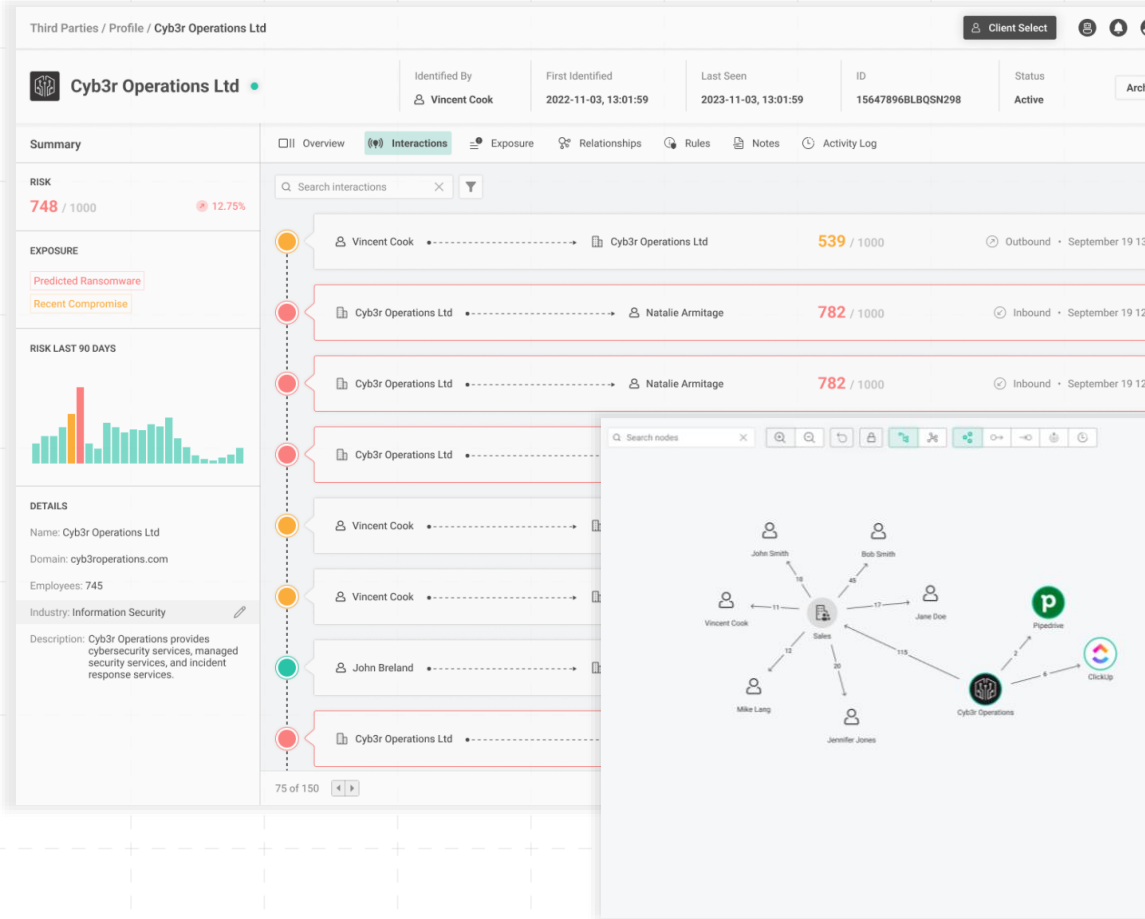
- **Third Party Discovery:** Identify suppliers, partners, and customers within your organisation's environment with just one click.
- **Employee Discovery:** Identify employees, their role, and department within your organisation with just one click.
- **Unique Risk Profiling:** Utilise advanced AI to create detailed real-time risk profiles for all discovered employees and third parties.
- **No Existing Integrations:** Our solution does not require integrations into any existing ERP, Procurement, HR, or TPRM tools.
- **Onboarding Speed:** Significantly accelerate onboarding by up to 70x and boost data visibility by 30x compared to outdated solutions.
- **Real-Time Updates:** Gain continuous monitoring and real-time updates on the status of all discovered entities.



CYB3R OPERATIONS

Effortlessly investigate & mitigate immediate risks

- **User Interactions:** Analyse employee interactions between third parties to detect abnormal or risky behaviours.
- **Investigation Graph:** Visually identify threats using a relationship mapping graph and comprehensive entity exploration options.
- **Auditing:** Utilise note-taking functions and detailed audit logs for each third party to maintain comprehensive records and oversight.
- **Risk & Compliance:** Align with compliance frameworks such as NIST to demonstrate effective third-party risk management processes.
- **Shadow Third-Party:** Identify and uncover unauthorised solutions, SaaS applications, and tools that the security team, procurement, and leadership may not be aware of.
- **Insider Threat:** Detect and mitigate risks posed by users collaborating with threat actors and/or competitors to compromise the business.



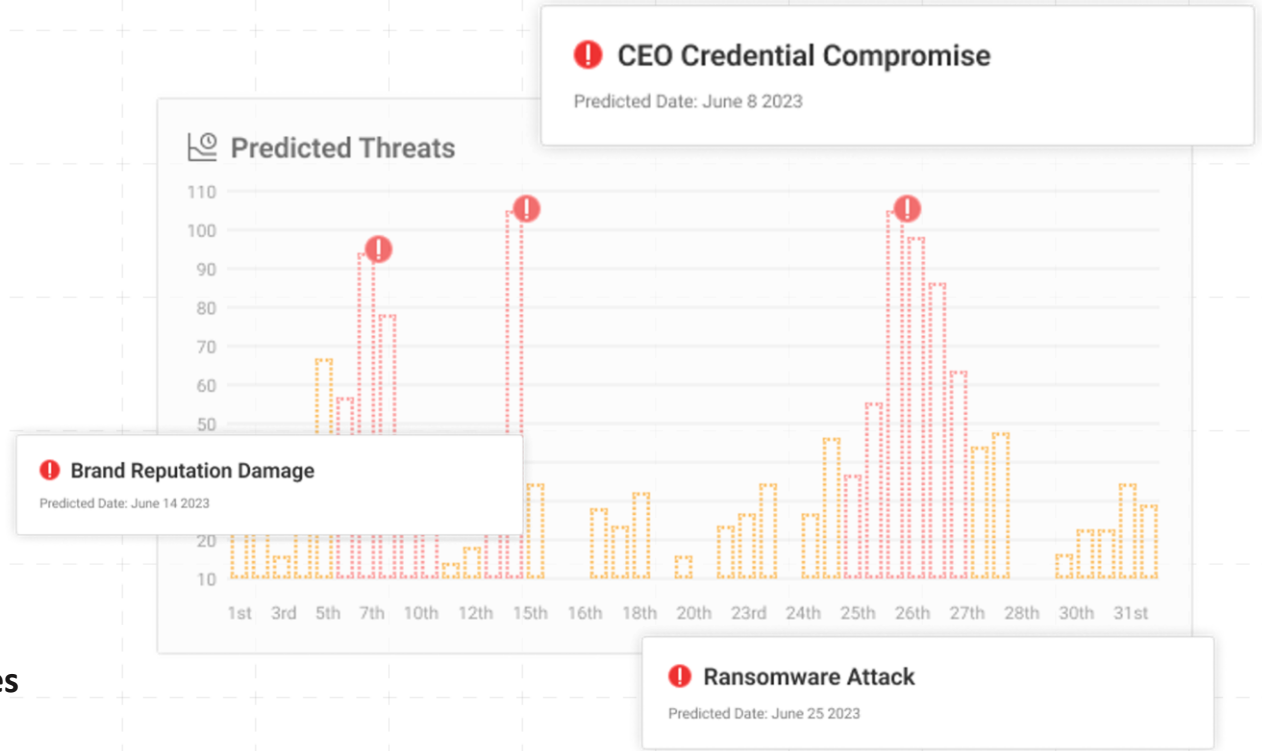
CYB3R OPERATIONS

Comprehensive threat prediction and risk management

Our proprietary platform uses a surface, deep, and dark web data set of over **280 billion attributes to build an employee and third-party predictive risk framework**. This can predict the successful occurrence of a cyber incidents against an organisation to a **76% accuracy rate.**

Prediction risk is calculated on exposure factors across 14 surface, deep, and dark web segments:

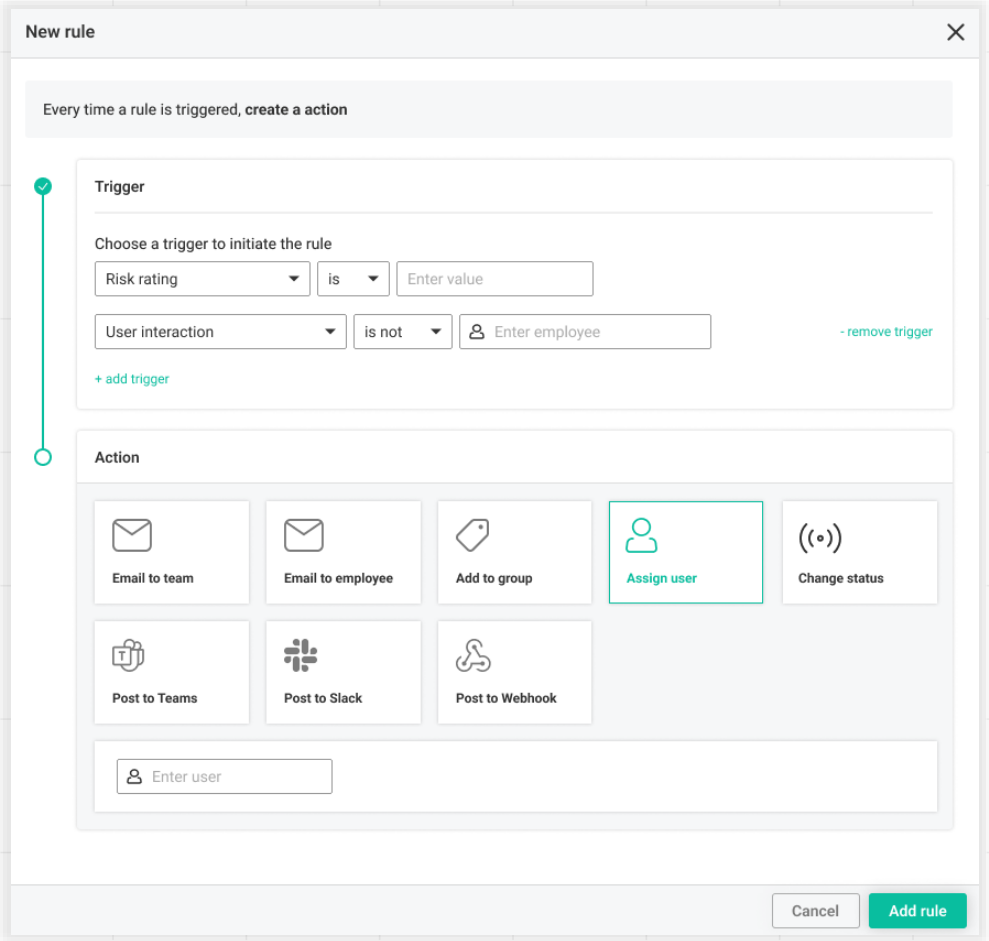
- # Information Stealers
- # Public Leaks
- # Private Leaks
- # Paste Sites
- # Dark Nets
- # Dark Forums
- # Black Markets
- # Chatrooms
- # Ransomware Sites
- # Industry News
- # Sanctions
- # Social Nets
- # Infrastructure Vulnerabilities
- # Community Intelligence



CYB3R OPERATIONS

Integrations & customisable responses

- **Fully Configurable:** Design predefined triggers and conditions that are completely customisable to meet your specific policies.
- **Global Rules:** Apply rules globally across all entities discovered or tailor them individually to minimise noise and enhance precision.
- **Workflow Integrations:** Integrate seamlessly with Slack, Microsoft Teams, SIEM systems, APIs, webhooks, and custom applications for streamlined and efficient incident response.
- **Trigger Behaviours:** Analyse the frequency of triggers to identify trends and patterns in high-risk businesses.
- **Continuous Alerting:** Focus on automated threat detection and ensures seamless, ongoing alerting with minimal analyst intervention.



CYB3R OPERATIONS

Download & share actionable reports

- **Executive Reporting:** Provide executives with high-level intelligence reports that offer comprehensive insights into security posture, highlight potential risks, and recommend strategic actions for mitigating threats.

- **Resource Management:** Informed decision-making and proactive risk management allow for the efficient allocation of resources, ensuring that the most critical threats are addressed promptly and effectively.

- **Technical Reporting:** Provide detailed, actionable insights for security teams, enabling them to understand the technical aspects of identified threats, vulnerabilities, and mitigation strategies.

- **Compliance Reporting:** Generate concise reports to ensure adherence to regulations and standards, such as NIST.

- **Third Party Responsibilities:** Provide reports to third parties to foster a community of organizations committed to maintaining high standards and compliance, effortlessly.

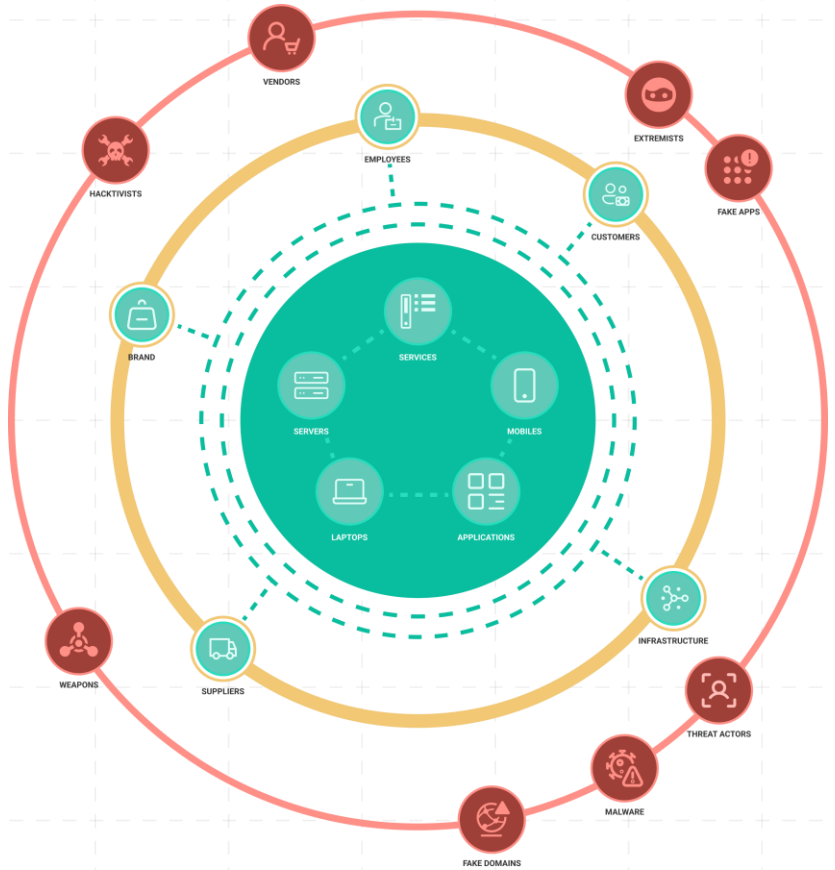
CYB3R OPERATIONS

Enhancing cyber defence through proactive actions

Deploying Dedicated Security Awareness Training: Automatically deliver targeted security awareness training to employees who are most susceptible to phishing attacks. This fosters a robust cybersecurity culture within the organisation, as employees are continuously tested and develop a 'security first' mindset.

Adjusting SIEM and Firewall Rules: Dynamically adjust rules on Security Information and Event Management (SIEM) tools or firewalls to manage network traffic effectively within the organisation’s digital environment. This includes blocking specific IP addresses or restricting access to high-risk websites, enhancing overall security.

Automatically Quarantining Communications: Automatically quarantine inbound or outbound communication from third parties to employees. This eliminates the risk of employees clicking on malicious links or attachments, significantly reducing the threat of malware.



CYB3R OPERATIONS

Learn more about us, contact the team

CONTACT INFORMATION

For more information, an in-depth demo, or technical details please contact us using the following information:

cyb3roperations.com

team@cyb3roperations.com

UK OFFICE

167-169 Great Portland Street
5th Floor
London
W1W 5PF

REQUEST DEMO

CONTACT SALES