Cye Brochure

Cyber **Expert Services**

Expert-Led Assessments and Incident Response Services

Cye combines AI, data science, and human expertise to help organizations understand their exposure, validate defenses, reduce risk, and respond effectively to cyber incidents.

By integrating assessment findings into Cye's Exposure Management Platform, organizations can continuously track progress, prioritize remediation efforts, and demonstrate measurable risk reduction over time.

Outcomes You Can Expect

- Reduce risk and organizational exposure
- Make decisions based on business impact
- Validate defenses and strengthen resilience
- 24/7 IR and accelerated recovery

Organizational **Assessments**

Gain evidence-based clarity of your organization's exploitable attack paths, and build a security roadmap for sustainable resilience.

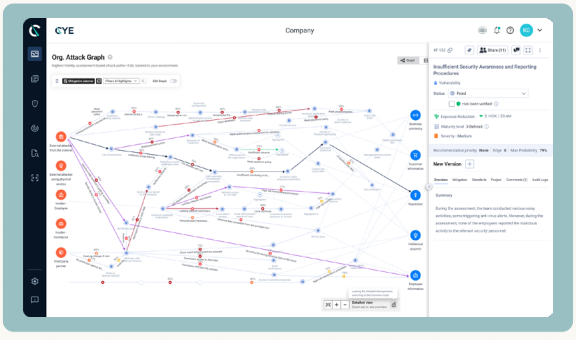
Maturity Assessment

Measure your cybersecurity maturity against the NIST Cybersecurity Framework and industry benchmarks. Understand where you stand, identify gaps, and demonstrate progress over time.

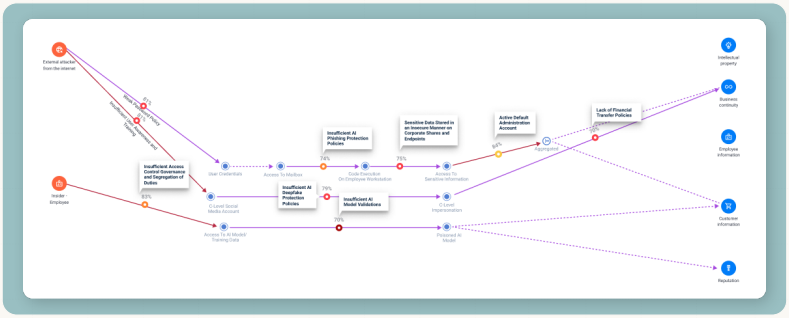
Risk Assessment

See your organizational exposure and security posture from an attacker's perspective. The assessment uncovers potential vulnerabilities that attackers can exploit to penetrate and move laterally within the environment. This includes a thorough evaluation of existing mitigation measures to prevent cross-domain lateral movement, or attackers gaining control of critical business assets.

These insights enable leaders to design and continuously track effective mitigation plans with associated timelines, team ownership, and resource planning on Cye's platform.



AI Security



Organizational AI Security Assessment

Ensure AI is adopted securely across the organization. Cye evaluates AI governance, onboarding processes, security controls, and technical implementations to identify gaps in how AI tools are introduced, managed, monitored, and protected.

LLM Penetration Testing

Identify vulnerabilities before attackers do. Adversarial testing of LLM-powered applications uncovers risks such as prompt injection, data leakage, insecure output handling, unauthorized tool execution, excessive permissions, and model manipulation, with prioritized recommendations for remediation.

External Assessment

External security assessments evaluate organization's external posture from an attacker's perspective. Reconnaissance gathers publicly exposed information—IP ranges, leaked vulnerabilities, key assets, as well as scans of internet-facing services to reveal most likely attackers' breach tactics.

OT Environment Maturity Assessment

Assess operational technology environments through safe, passive analysis that identifies security gaps without disrupting production. This includes reviews of configurations and policies, team interviews to assess maturity against NIST 800-82 criteria, and physically reviews of OT assets e.g. PLCs, HMIs, control rooms to uncover technical, procedural, and physical weaknesses.

M&A Security Assessments

A suite of cybersecurity assessments designed to evaluate risks across the M&A lifecycle, including organizational defenses, product vulnerabilities, threat exposure, and post-integration weaknesses. Assessments' insights are reflected with a thorough due diligence report that includes findings and a recommended action plan to enable evidence-based M&A negotiations and drive a post-M&A security roadmap.

Validation **Services**

Red team, purple team, and penetration testing engagements validate whether your controls, detections, and response capabilities can withstand real-world attack techniques.

Technical Assessments

Targeted assessments across cloud, data, application, DevSecOps, infrastructure, and identity to uncover weaknesses and strengthen defenses. The assessments across different attack surfaces share Cye's unique methodology, results-driven execution and clear reporting.

Strategic & Advisory **Engagements**

Mitigation Workshop

Building on the findings presented on the exposure management platform, Cye works directly with customers' technical teams to identify root causes and refine short- and long-term plans around their existing tools, budget, and operational realities—producing a defensible roadmap that reduces the most risk for the least cost.

CISO Advisory

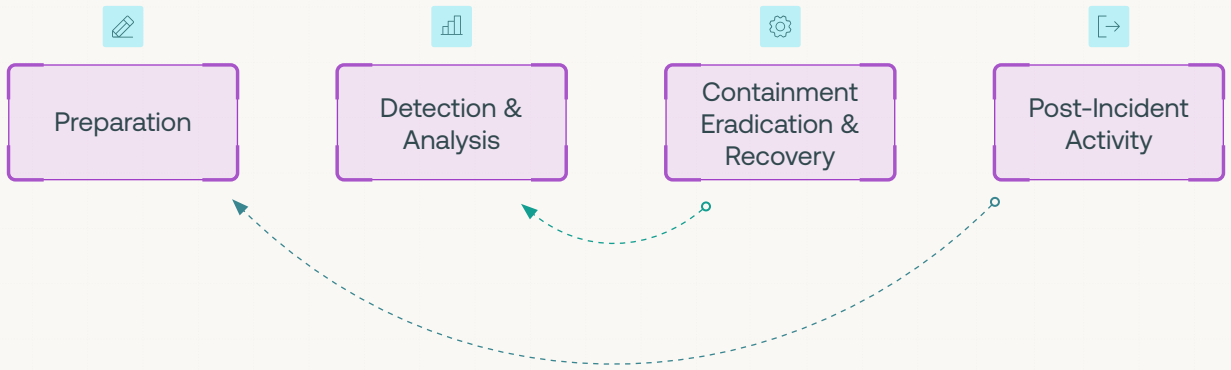
Access experienced security leadership for architecture reviews, risk prioritization, cloud initiatives, and long-term security strategy.

> *The baseline assessment sharpened our focus in terms of cybersecurity. It made us aware of potential cyber threats. What was helpful and valuable was Cye's ability to contextualize cybersecurity.*

Oscar Lindberg
Chief Information Officer
AutoStore

Emergency & Operations

Prepare for incidents before they happen and respond effectively when they do: Receive 24/7 support for successful containment, remediation, and recovery from a breach, and minimize operational impact to your business.



Threat Hunting

Proactively identify hidden adversaries, suspicious activity, and indicators of compromise across your environment.

Cyber Threat Intelligence Program

Gain actionable intelligence on the threat actors, tactics, and campaigns most relevant to your organization.

Incident Response & Digital Forensics

Rapidly contain incidents, establish root cause, minimize business impact, and strengthen defenses against future attacks.

Incident Response SLA & Engagement Readiness

Ensure immediate access to expert responders through predefined service levels, onboarding, and readiness planning.

Crisis Readiness Program

Develop playbooks, define responsibilities, and prepare teams to act decisively during a cyber crisis that reduces its impact on the organization's business continuity.

Executive Crisis Management Tabletop

Pressure-test executive decision-making, communication, and coordination through realistic, scenario-based exercises. This evaluates existing Business Continuity Plans (BCPs) and adjusts them as needed.

Cye's staff is knowledgeable and responsive. Their teams communicate clearly to help us reduce our risks and resolve technical issues quickly.

Sundar Sankarnarayanan
Vice President Of Engineering

JEEVES

Engage with a Cye expert to review your current security posture, discuss your priorities, and determine the right assessment or response service for your organization.

Engage Us

About Cye

Cye combines an AI-native exposure management platform with world-class cyber expertise to help organizations know the financial impact of their cyber exposure, prioritize risk mitigation and automate remediation. Cye's 500+ customers gain the clarity to make smart defensible decisions that reduce their risk exploitability with speed, and improve their resilience to the hyper dynamic threat landscape.

Visit us at cyesec.com.