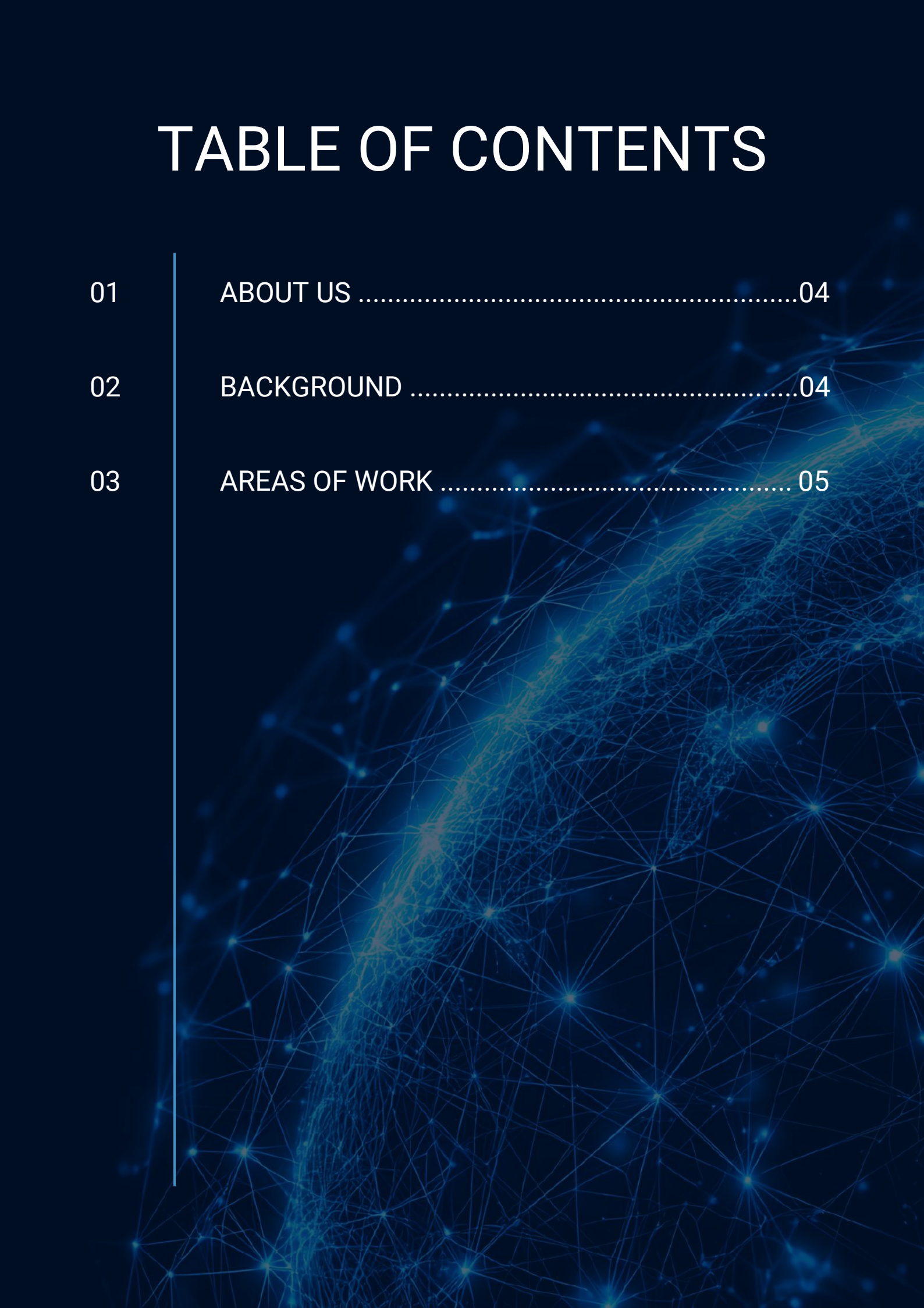
ATHENIAN TECH

ATHENIAN TECH

We Help You Protect Your Business

OUR SERVICES

TABLE OF CONTENTS



AREAS OF WORK

- AI Advisory & Responsible AI Governance
- Cybersecurity Strategy & vCISO as Services
- Data Privacy, Regulatory Compliance
- Digital Risk Monitoring & External Attack Surface
- Enhanced Risk and GDPR Management
- Security Posture Hardening
- Geopolitical Risk Advisory
- Incident Response & Breach Management
- Penetration Testing
- Policy and Compliance Design (DPDPA, GDPR)
- Ransomware & Cyber Resilience Programs
- Ready-to-use policy and Cybersecurity toolkit
- Security Awareness, Training & Tabletop Exercises
- Third-Party & Supply Chain Risk Management
- AI-Driven Threat Intelligence
- Proactive Threat Intelligence
- Website and Mobile Application Security Testing

ABOUT US

Athenian Tech is a Digital Risk Management company providing Artificial Intelligence, Machine learning-powered technology solutions against advanced digital and cyber threats. Our eminent clients include Amazon, BAE Systems, Meta, Microsoft and UNODC.

Athenian Tech leverages Artificial Intelligence, Machine learning-powered technology solutions to protect Digital Identity for businesses. Athenian Tech offers 360-degree protection against advanced digital and cyber threats.

Athenian Tech focuses on protecting businesses and business leaders from identity thefts, frauds, social engineering attacks, APTs, Ransomware attacks, and Crypto-jacking emerging threat vectors from the Dark, Deep and Surface Web.

BACKGROUND

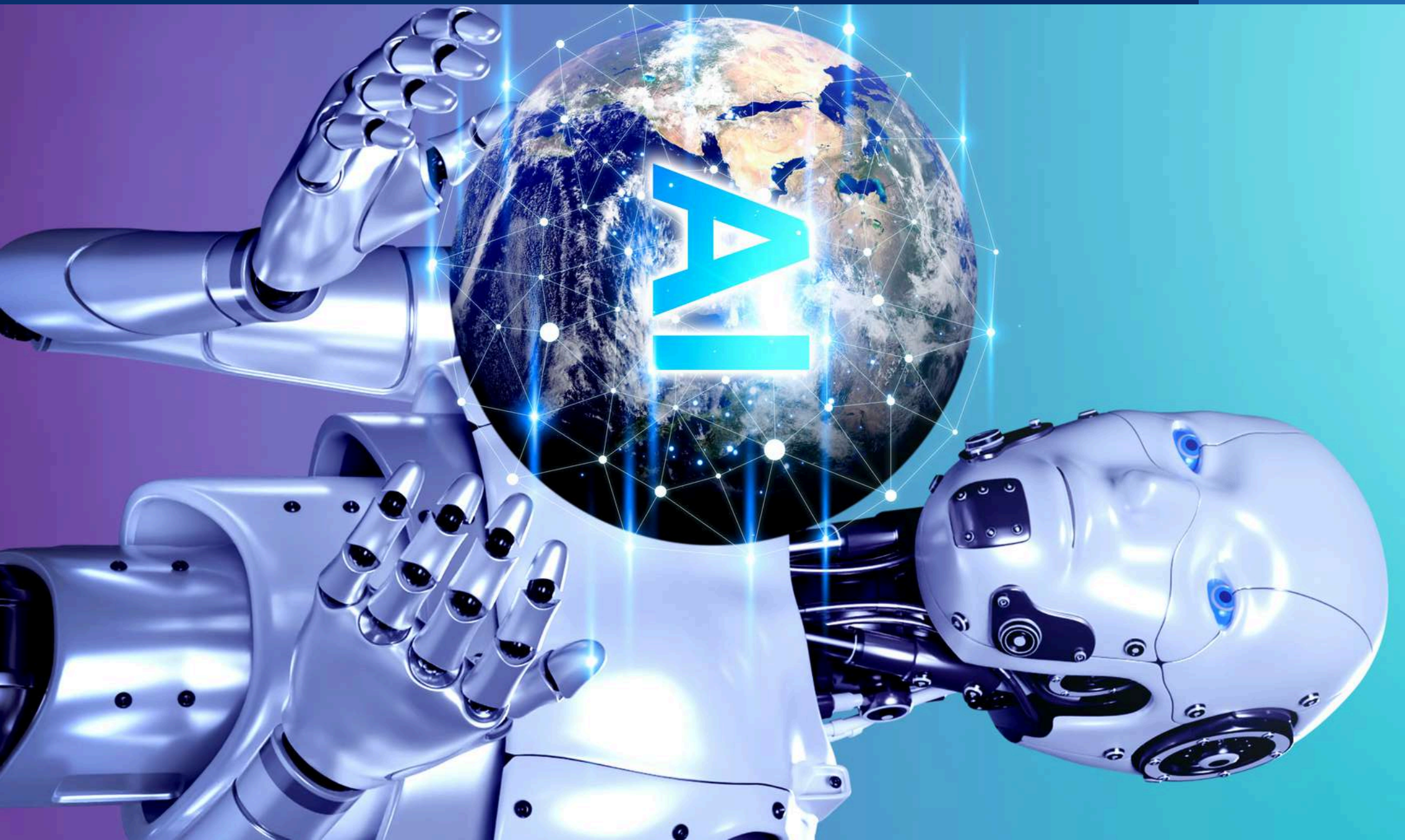
Athenian Tech was founded to address the growing complexity of digital risk and cyber threats faced by modern organisations. At its core, the company combines advanced artificial intelligence and machine learning technologies to deliver continuous, 360-degree digital risk monitoring and threat intelligence, extending beyond traditional perimeter defences to include deep and dark web exposure.

The organisation’s platforms are designed to detect, analyse, and prioritise emerging threats such as identity theft, social engineering, ransomware, advanced persistent threats, and reputation abuse. By correlating data from diverse sources and applying AI-driven analytics, Athenian Tech enables proactive identification of risk vectors that pose strategic, operational, and security challenges to enterprises.

Athenian Tech works with businesses to strengthen their cyber resilience, improve threat awareness, and reduce digital exposure. Its approach integrates technology capability with expert advisory support, empowering organisations to anticipate risks, inform decision-making, and maintain trust in complex digital ecosystems.

AREAS OF WORK

AI ADVISORY & RESPONSIBLE AI GOVERNANCE



Strengthening Responsible Innovation, Accountability, and Trust in AI Systems

With the increasing integration of Artificial Intelligence (AI) across governance, industry, and public services, the need for proper oversight and governance of AI has become imperative. Although AI offers opportunities to improve efficiency, decision-making, and innovation, its improper use could pose risks.

AI Advisory & Responsible AI Governance primarily advises organisations, governments, and institutions on implementing AI systems that are ethical, secure, and in the public interest. A proper governance framework is required because it helps balance innovation with safeguards.

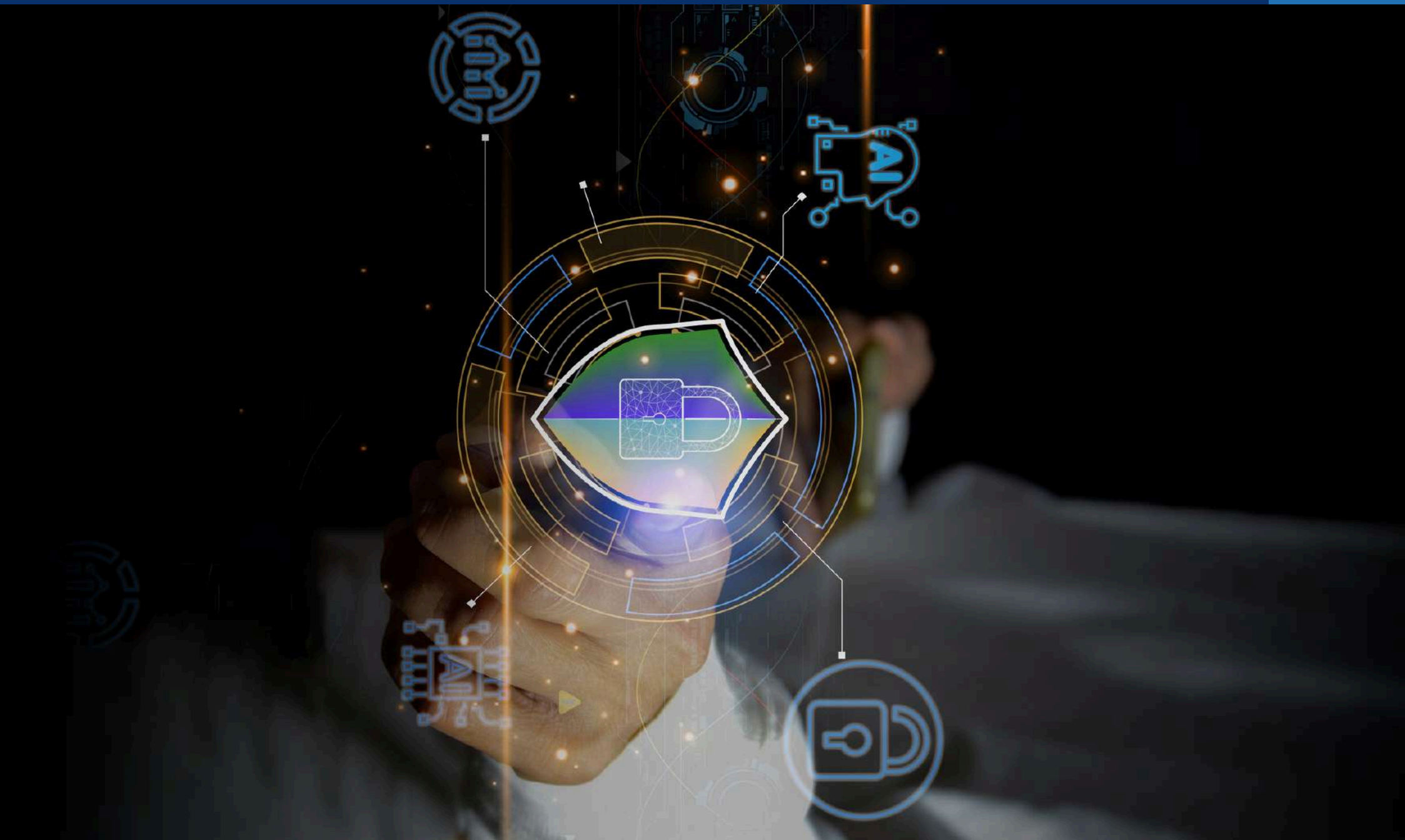
This field enables the development of governance structures that consider the entire lifecycle of AI, from data collection to AI model deployment. This is done with a focus on transparency, risk mitigation, and ensuring that AI systems are auditable and fair.

Through discussions, policy engagement, and advisory initiatives led by experts, this work seeks to bring together government officials, regulators, legal experts, technologists, and industry leaders to facilitate informed discussions on the responsible adoption of AI. The aim is to enable future-ready models of governance that promote innovation while ensuring public trust and accountability.

Key Focus Areas Include the Following:

- **Ethical & Responsible AI** - Promoting fairness, transparency, and accountability in AI systems.
- **AI Governance Frameworks** - Supporting lifecycle-based oversight and policy design.
- **Risk & Impact Assessments** - Identifying bias, misuse, and unintended consequences.
- **Explainability & Transparency** - Strengthening trust through interpretable AI systems.
- **AI Security & Compliance** - Aligning AI use with regulatory, legal, and societal expectations.

CYBERSECURITY STRATEGY & vCISO AS SERVICES



Strengthening Organisational Resilience, Governance, and Cyber Preparedness

With the growing role of digital systems in governance, economics, and essential services, cybersecurity has evolved from a technical matter to a leadership issue. The sophistication of cyber threats, from data breaches and ransomware attacks to state-sponsored attacks, has forced organisations to develop long-term cybersecurity strategies that are risk and compliance-driven.

Cybersecurity Strategy & vCISO as a Service is all about improving the governance, leadership, and decision-making processes within the overall cyber ecosystem of an organisation. This service offering is related to helping organisations evaluate their existing security situation, determine the systemic risks, and develop a comprehensive cybersecurity roadmap.

The vCISO service offers the benefit of having high-level cybersecurity leadership without necessarily requiring a full-time executive position. The vCISO acts as a strategic advisor and helps in governance structures, policy development, risk management, and regulatory compliance. The vCISO service is especially useful for organisations that have complex compliance issues, are undergoing rapid digital transformation, or lack resources.

Structured engagement, advisory, and stakeholder discussions are used to bring together the executive leadership, CISOs, legal, and technical teams to improve the cyber resilience of institutions. The aim is to help organisations prepare and manage cyber risk proactively and develop sustainable security programmes that are aligned with long-term organisational strategies.

Key Focus Areas Include the Following:

- **Cybersecurity Strategy & Roadmaps** – Aligning security with organisational objectives.
- **vCISO Advisory Services** – Executive-level guidance on governance and risk.
- **Risk & Maturity Assessments** – Evaluating cyber posture and capability gaps.
- **Security Governance & Policies** – Strengthening oversight and accountability.
- **Incident Preparedness & Response** – Improving readiness and decision-making.
- **Regulatory & Compliance Alignment** – Supporting adherence to cyber laws and standards.

DATA PRIVACY AND REGULATORY COMPLIANCE

Strengthening Data Protection, Accountability, and Regulatory Trust

As data-driven technologies continue to shape digital governance, commerce, and public services, protecting personal and sensitive information has become a core organisational responsibility. Expanding data collection, cross-border processing, and increasing regulatory scrutiny have heightened expectations around how data is handled, safeguarded, and governed.

Data Privacy and Regulatory Compliance focuses on supporting organisations in understanding and operationalising data protection requirements through structured governance and compliance frameworks. This area of work emphasises accountability, transparency, and lawful data processing across the data lifecycle, ensuring that privacy principles are embedded into systems, processes, and organisational decision-making.

Through advisory engagements, policy discussions, and expert-led sessions, this work brings together regulators, legal experts, compliance leaders, CISOs, and business stakeholders. The objective is to enable organisations to reduce regulatory risk, demonstrate responsible data stewardship, and build sustainable trust with users, partners, and supervisory authorities.

The objective is to support organisations in building resilient, compliant, and future-ready data governance practices that protect individual rights, enhance institutional credibility, and sustain trust in the digital ecosystem.

Key Focus Areas Include the Following:

- **Data Protection Governance** – Establishing accountability and oversight structures.
- **Regulatory Compliance Frameworks** – Aligning with applicable data protection laws.
- **Privacy-by-Design & Default** – Embedding privacy across systems and processes.
- **Consent & Data Management** – Strengthening lawful and transparent data handling.
- **Data Security & Breach Preparedness** – Reducing risk and improving response readiness.
- **Trust & Transparency** – Reinforcing confidence among users and regulators.

DIGITAL RISK MONITORING & EXTERNAL ATTACK SURFACE

Strengthening Visibility, Early Warning, and Resilience Across the Digital Perimeter

As organisations expand their digital presence across cloud platforms, internet-facing applications, and third-party services, their exposure to external cyber risks continues to grow. Unmanaged assets, misconfigurations, and publicly exposed systems often become primary entry points for cyber attacks, making continuous visibility into the external attack surface a critical organisational requirement.

Digital Risk Monitoring & External Attack Surface focuses on enabling organisations to identify, understand, and manage risks originating from their internet-facing assets. This area of work emphasises continuous monitoring of external exposure, including domains, IPs, cloud resources, and third-party dependencies, ensuring that potential weaknesses are identified before they can be exploited.

Through ongoing monitoring, risk assessments, and expert-led analysis, this work supports security teams, risk leaders, and decision-makers in strengthening situational awareness and prioritising remediation efforts. The objective is to reduce exposure, improve early warning capabilities, and enhance organisational resilience against externally driven cyber threats.

The objective is to support organisations in proactively managing digital exposure, minimising attack opportunities, and strengthening cyber preparedness across the extended digital ecosystem.

Key Focus Areas Include the Following:

- **External Attack Surface Discovery** – Identifying internet-facing assets and exposures.
- **Digital Risk Monitoring** – Continuous tracking of threats, vulnerabilities, and indicators.
- **Shadow IT & Third-Party Exposure** – Managing unmanaged and external dependencies.
- **Vulnerability & Misconfiguration Insights** – Highlighting externally exploitable weaknesses.
- **Brand & Domain Abuse Monitoring** – Detecting impersonation, phishing, and misuse.

ENHANCED RISK AND GDPR MANAGEMENT

Strengthening Risk Governance, Data Protection, and Regulatory Accountability

As regulatory scrutiny around data protection continues to intensify, organisations are required to demonstrate not only compliance with GDPR obligations but also effective management of privacy and data-related risks. Increasing volumes of personal data, complex processing activities, and reliance on third parties have elevated the importance of adopting structured, risk-based approaches to data protection.

Enhanced Risk and GDPR Management focuses on supporting organisations in systematically identifying, assessing, and mitigating data protection risks across the data lifecycle. This area of work emphasises integrating GDPR requirements into enterprise risk management and governance frameworks, ensuring that privacy risks are evaluated consistently and addressed through proportionate controls and safeguards.

Through advisory engagements, structured risk assessments, and expert-led discussions, this work brings together data protection officers, legal teams, CISOs, risk leaders, and business stakeholders. The objective is to strengthen compliance readiness, improve accountability, and ensure that regulatory requirements are translated into practical and sustainable operational measures.

The objective is to support organisations in reducing regulatory exposure, strengthening data protection governance, and building trust with regulators, partners, and data subjects.

Key Focus Areas Include the Following:

- **GDPR Risk Assessments** – Identifying and prioritising data protection risks.
- **Data Protection Governance** – Strengthening accountability and oversight structures.
- **Privacy Impact & Risk Management** – Supporting DPIAs and risk mitigation measures.
- **Compliance Monitoring & Reporting** – Ensuring continuous regulatory alignment.
- **Incident & Breach Preparedness** – Improving readiness and response mechanisms.
- **Regulatory Engagement & Assurance** – Supporting audits and supervisory interactions.

SECURITY POSTURE HARDENING

Strengthening Baseline Security Controls and Reducing Systemic Risk

As organisations expand their digital infrastructure and adopt increasingly interconnected systems, weaknesses in baseline security controls can significantly increase exposure to cyber threats. Many security incidents arise from preventable issues such as misconfigurations, excessive access privileges, and delayed remediation, underscoring the importance of strengthening foundational security posture.

Security Posture Hardening focuses on enhancing the effectiveness of core security controls across systems, networks, applications, and user environments. This area of work emphasises a structured, risk-based approach to identifying control gaps, prioritising remediation efforts, and strengthening defence-in-depth across the organisation.

Through targeted assessments, expert-led advisory engagements, and stakeholder collaboration, this work supports security and IT teams in aligning technical improvements with governance and risk management objectives. The objective is to reduce attack surface, improve control consistency, and establish a resilient security baseline that supports long-term cyber maturity.

The objective is to support organisations in minimising preventable security weaknesses, improving resilience, and strengthening overall cybersecurity readiness.

Key Focus Areas Include the Following:

- **Baseline Security Assessments** – Identifying control gaps and misconfigurations.
- **System & Network Hardening** – Strengthening configurations and access controls.
- **Identity & Privileged Access Management** – Reducing account-related risks.
- **Patch & Vulnerability Management** – Improving remediation effectiveness.
- **Security Monitoring & Logging** – Enhancing visibility and detection.
- **Continuous Improvement & Validation** – Sustaining posture hardening efforts.

GEOPOLITICAL RISK ADVISORY

Strengthening Strategic Foresight, Resilience, and Informed Decision-Making

In an increasingly interconnected global environment, geopolitical developments have a direct and growing influence on business operations, investment decisions, regulatory environments, and supply chains. Shifts in political stability, international relations, trade policies, sanctions, and regional conflicts can rapidly alter risk landscapes, making proactive geopolitical risk assessment essential for organisations operating across borders.

Geopolitical Risk Advisory focuses on supporting organisations in understanding, anticipating, and responding to geopolitical dynamics that may impact strategic objectives and operational continuity. This area of work emphasises structured analysis of regional developments, political trends, and regulatory shifts to help organisations identify potential exposures and assess their implications.

Through expert-led briefings, strategic advisories, and stakeholder discussions, this work brings together policy specialists, risk professionals, and senior decision-makers. The objective is to enable organisations to incorporate geopolitical awareness into governance and planning processes, strengthen resilience to external shocks, and make informed decisions in an uncertain global landscape.

The objective is to support organisations in navigating geopolitical complexity, reducing strategic blind spots, and strengthening long-term operational and investment resilience.

Key Focus Areas Include the Following:

- **Geopolitical Risk Assessment** – Identifying regional and global risk drivers.
- **Political & Regulatory Analysis** – Monitoring policy shifts and governance changes.
- **Cross-Border Risk Exposure** – Evaluating impacts on operations and investments.
- **Strategic Foresight & Scenario Planning** – Preparing for geopolitical uncertainty.
- **Supply Chain & Market Disruptions** – Assessing resilience and dependencies.
- **Advisory Briefings & Insights** – Supporting leadership decision-making.

INCIDENT RESPONSE & BREACH MANAGEMENT

Strengthening Preparedness, Coordination, and Effective Crisis Response

As cyber incidents and data breaches continue to increase in frequency and impact, organisations face growing pressure to respond swiftly, decisively, and in compliance with regulatory expectations. Delayed detection or uncoordinated response efforts can significantly amplify operational disruption, legal exposure, and reputational damage, underscoring the need for structured incident response and breach management capabilities.

Incident Response & Breach Management focuses on enabling organisations to prepare for, manage, and recover from cyber incidents through clearly defined response frameworks. This area of work emphasises establishing roles, escalation paths, and decision-making processes that ensure effective coordination across technical, legal, communications, and leadership teams during high-pressure situations.

Through advisory engagements, response planning exercises, and expert-led discussions, this work brings together CISOs, incident response teams, legal counsel, compliance leaders, and senior management. The objective is to strengthen response readiness, improve regulatory alignment, and ensure that incidents are handled efficiently, transparently, and with minimal impact.

The objective is to support organisations in minimising damage, maintaining stakeholder trust, and recovering effectively from cyber incidents and data breaches.

Key Focus Areas Include the Following:

- **Incident Response Frameworks** – Defining roles, processes, and escalation paths.
- **Breach Detection & Analysis** – Improving identification and assessment of incidents.
- **Crisis Management & Coordination** – Aligning technical, legal, and leadership actions.
- **Regulatory Notification & Compliance** – Managing reporting obligations and timelines.
- **Communication & Stakeholder Management** – Supporting accurate and timely disclosures.
- **Post-Incident Review & Improvement** – Strengthening resilience through lessons learned.

PENETRATION TESTING

Strengthening Security Assurance Through Proactive Vulnerability Assessment

As organisations continue to expand digital systems and applications, vulnerabilities within networks, platforms, and software remain a primary pathway for cyber attacks. Automated scans alone are often insufficient to uncover complex weaknesses or validate how security controls perform under real-world conditions, making penetration testing a critical component of cybersecurity assurance.

Penetration Testing focuses on evaluating the security posture of systems, applications, and infrastructure by simulating realistic attack scenarios in a controlled and ethical manner. This area of work emphasises identifying exploitable vulnerabilities, configuration weaknesses, and logic flaws that attackers could leverage, while assessing their potential business and operational impact.

Through structured testing engagements, expert analysis, and post-assessment discussions, this work brings together security teams, technology owners, and risk stakeholders. The objective is to provide clear, actionable insights that support prioritised remediation, strengthen defensive controls, and validate the effectiveness of existing security measures.

The objective is to support organisations in proactively reducing their attack surface, validating security investments, and strengthening overall cyber resilience in an evolving threat landscape.

Key Focus Areas Include the Following:

- **Network & Infrastructure Testing** – Assessing internal and external network security.
- **Application Security Testing** – Identifying vulnerabilities in web and mobile applications.
- **Cloud & API Security Testing** – Evaluating modern and distributed environments.
- **Attack Simulation & Exploitation** – Understanding real-world attack paths.
- **Risk-Based Reporting** – Prioritising findings by impact and likelihood.
- **Remediation Guidance & Validation** – Supporting effective vulnerability closure.

POLICY AND COMPLIANCE DESIGN (DPDPA, GDPR)

Strengthening Regulatory Alignment, Accountability, and Policy Readiness

As data protection regulations continue to evolve across jurisdictions, organisations face increasing pressure to translate legal requirements into clear, enforceable internal policies. Frameworks such as the Digital Personal Data Protection Act (DPDPA) and the General Data Protection Regulation (GDPR) impose stringent obligations around accountability, transparency, and lawful data processing, making structured policy design a critical governance requirement.

Policy and Compliance Design (DPDPA, GDPR) focuses on supporting organisations in developing comprehensive policy frameworks that align regulatory expectations with organisational context and risk profiles. This area of work emphasises clarity, consistency, and accountability—ensuring that policies provide practical guidance to stakeholders and support compliant decision-making across the data lifecycle.

Through advisory engagements, policy workshops, and expert-led discussions, this work brings together legal experts, data protection officers, compliance leaders, CISOs, and business stakeholders. The objective is to ensure that regulatory requirements are interpreted accurately, operationalised effectively, and embedded into organisational processes rather than treated as standalone documentation.

The objective is to support organisations in building robust, auditable, and future-ready policy frameworks that reduce compliance risk and strengthen regulatory confidence.

Key Focus Areas Include the Following:

- **Regulatory Mapping & Interpretation** – Translating DPDPA and GDPR obligations.
- **Data Protection Policy Frameworks** – Developing clear and enforceable policies.
- **Roles & Accountability Structures** – Defining ownership and governance mechanisms.
- **Compliance Integration** – Aligning policies with operational processes.
- **Audit & Assessment Readiness** – Supporting regulatory reviews and evaluations.
- **Continuous Policy Review** – Adapting frameworks to regulatory and business change.

RANSOMWARE & CYBER RESILIENCE PROGRAMS

Strengthening Organisational Resilience Against Ransomware and Disruptive Cyber Threats

Ransomware attacks have emerged as one of the most significant cyber risks facing organisations, with the potential to cause widespread operational disruption, data loss, and reputational damage. As attack methods become more targeted and persistent, organisations must adopt resilience-focused strategies that address not only prevention, but also preparedness, response, and recovery.

Ransomware & Cyber Resilience Programs focus on supporting organisations in building structured capabilities to withstand and recover from ransomware incidents and other high-impact cyber disruptions. This area of work emphasises proactive risk assessment, resilience planning, and the integration of technical, operational, and governance measures to limit the impact of attacks on critical functions.

Through advisory engagements, resilience assessments, and expert-led discussions, this work brings together cybersecurity leaders, IT teams, risk managers, and senior decision-makers. The objective is to strengthen organisational readiness, improve recovery capability, and ensure continuity of operations during and after disruptive cyber events.

The objective is to support organisations in minimising downtime, protecting critical assets, and strengthening long-term cyber resilience.

Key Focus Areas Include the Following:

- **Ransomware Risk Assessment** – Identifying exposure and critical dependencies.
- **Cyber Resilience Frameworks** – Integrating prevention, response, and recovery.
- **Backup & Recovery Strategies** – Ensuring data integrity and restoration readiness.
- **Incident Preparedness & Response** – Strengthening detection and coordination.
- **Business Continuity & Crisis Management** – Maintaining operations during disruption.
- **Post-Incident Recovery & Improvement** – Enhancing resilience through lessons learned.

READY-TO-USE POLICY AND CYBERSECURITY TOOLKIT

Enabling Rapid Adoption of Structured Cybersecurity and Policy Controls

As organisations face increasing regulatory, operational, and cyber risk pressures, the ability to quickly establish effective security and governance controls has become essential. Many institutions struggle not due to a lack of intent, but due to the time, expertise, and resources required to design comprehensive policies and cybersecurity frameworks from the ground up.

Ready-to-use Policy and Cybersecurity Toolkit focuses on supporting organisations with pre-developed, adaptable resources that enable immediate implementation of governance, compliance, and security best practices. This area of work emphasises practicality and consistency, providing structured templates and frameworks that align with regulatory expectations while remaining flexible to organisational context and risk profiles.

Through guided adoption, advisory support, and expert-led sessions, this work brings together security teams, compliance leaders, and operational stakeholders. The objective is to accelerate security maturity, reduce implementation timelines, and ensure that policies and controls are embedded into everyday operations rather than treated as static documentation.

The objective is to support organisations in strengthening cybersecurity posture and governance readiness efficiently through clear, actionable, and standardised resources.

Key Focus Areas Include the Following:

- **Policy & Procedure Templates** – Ready-to-adapt governance and compliance documents.
- **Cybersecurity Control Frameworks** – Structured security baselines and controls.
- **Regulatory Alignment** – Supporting compliance with data protection and cyber laws.
- **Implementation Guidance** – Enabling effective adoption and operationalisation.
- **Audit & Documentation Readiness** – Supporting assessments and reviews.
- **Continuous Improvement Support** – Updating toolkits to address evolving risks.

SECURITY AWARENESS, TRAINING & TABLETOP EXERCISES

Strengthening Human Readiness, Organisational Awareness, and Response Capability

As cyber threats continue to evolve, human behaviour remains a critical factor in both preventing and responding to security incidents. Phishing attacks, social engineering, and procedural errors continue to be among the most common causes of breaches, highlighting the need for sustained security awareness and preparedness across all levels of an organisation.

Security Awareness, Training & Tabletop Exercises focus on building informed, vigilant, and prepared teams capable of recognising threats and responding effectively under pressure. This area of work emphasises continuous, role-based training and practical learning approaches that reinforce secure behaviours while ensuring clarity around responsibilities during cyber incidents.

Through structured training programmes, facilitated tabletop exercises, and expert-led simulations, this work brings together employees, technical teams, and senior leadership. The objective is to strengthen organisational readiness, improve coordination during incidents, and ensure that response plans are understood, tested, and effective before real-world events occur.

The objective is to support organisations in reducing human-related risk, strengthening incident preparedness, and improving collective response capability.

Key Focus Areas Include the Following:

- **Security Awareness Programmes** – Building cyber-conscious organisational culture.
- **Role-Based Training** – Tailoring learning to functions and responsibilities.
- **Phishing & Social Engineering Readiness** – Reducing human-driven attack success.
- **Tabletop & Simulation Exercises** – Testing response plans and coordination.
- **Leadership & Crisis Decision-Making** – Strengthening executive preparedness.
- **Continuous Learning & Improvement** – Reinforcing awareness through regular updates.

THIRD-PARTY & SUPPLY CHAIN RISK MANAGEMENT

Third-Party & Supply Chain Risk Management

As organisations increasingly depend on external vendors, service providers, and technology partners, third-party and supply chain risks have become a significant source of cyber, operational, and regulatory exposure. Security incidents originating from vendors can quickly propagate across interconnected systems, impacting data protection, service availability, and organisational reputation.

Third-Party & Supply Chain Risk Management focuses on supporting organisations in identifying, assessing, and managing risks arising from external relationships throughout the vendor lifecycle. This area of work emphasises structured governance, consistent risk assessment, and clear accountability to ensure that third-party risks are understood and managed in alignment with organisational risk tolerance.

Through advisory engagements, risk assessments, and expert-led discussions, this work brings together procurement teams, CISOs, risk leaders, legal experts, and business stakeholders. The objective is to improve visibility into supply chain dependencies, prioritise high-risk vendors, and embed third-party risk considerations into procurement, contracting, and ongoing oversight processes.

The objective is to support organisations in reducing systemic exposure, strengthening resilience across extended ecosystems, and maintaining trust with customers, partners, and regulators.

Key Focus Areas Include the Following:

- **Third-Party Risk Frameworks** – Establishing structured governance and oversight.
- **Vendor Security Assessments** – Evaluating cybersecurity and data protection practices.
- **Supply Chain Visibility** – Identifying dependencies and concentration risks.
- **Contractual & Policy Controls** – Strengthening security and compliance obligations.
- **Continuous Monitoring** – Tracking risk posture across vendor relationships.
- **Regulatory & Audit Readiness** – Supporting compliance and assurance requirements.

AI-DRIVEN THREAT INTELLIGENCE

Strengthening Threat Visibility, Prediction, and Informed Security Decision-Making

As cyber threats continue to grow in volume and sophistication, organisations face increasing challenges in identifying which risks require immediate attention. Traditional threat intelligence approaches, often reliant on static indicators and manual analysis, can struggle to keep pace with rapidly evolving attacker techniques and large volumes of security data.

AI-Driven Threat Intelligence focuses on enhancing an organisation's ability to detect, analyse, and prioritise threats using advanced analytics and automation. This area of work emphasises the use of artificial intelligence to correlate diverse data sources, identify hidden patterns, and surface actionable insights that support faster and more informed security decisions.

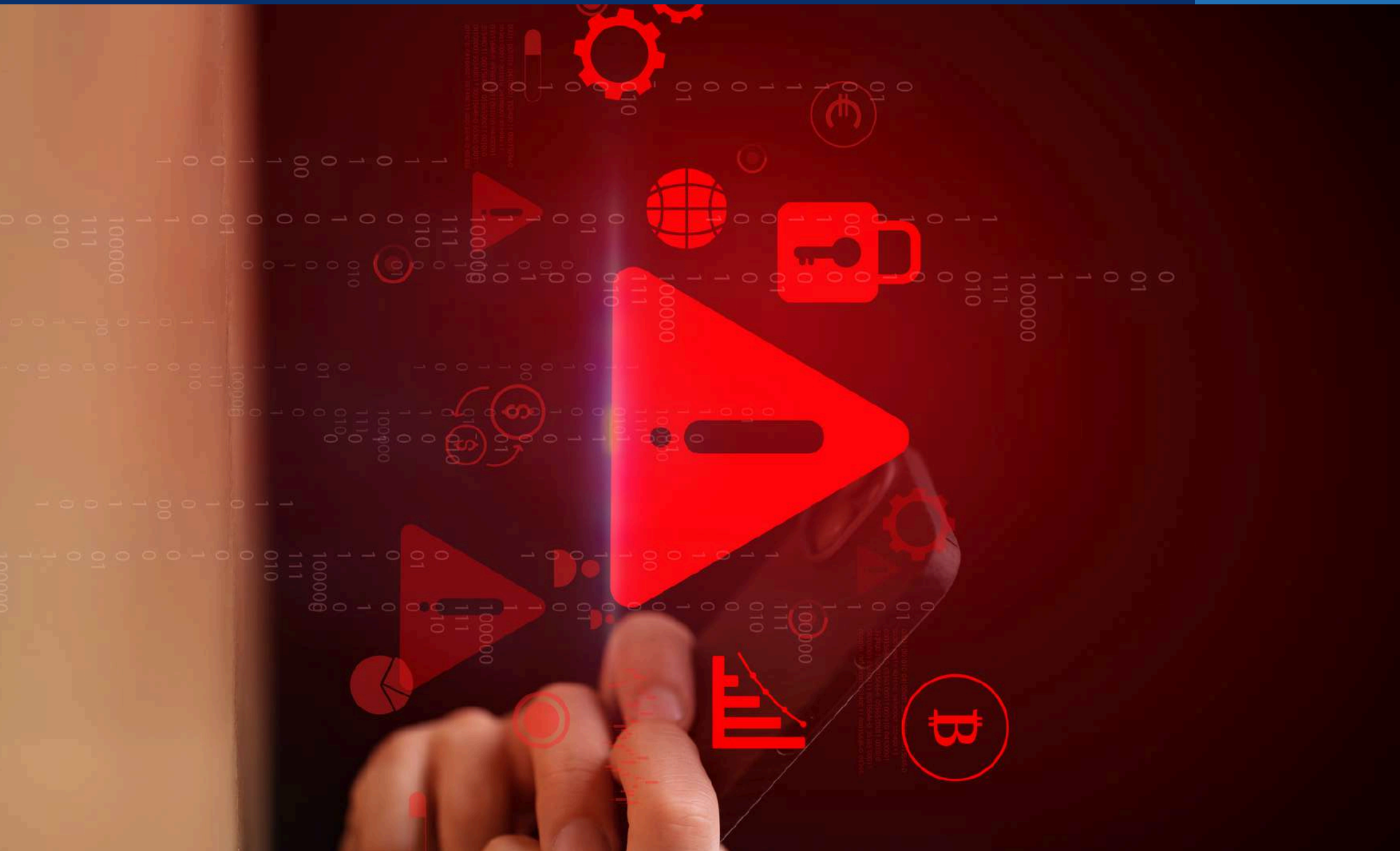
Through advisory engagements, capability assessments, and expert-led discussions, this work brings together security leaders, analysts, and risk stakeholders. The objective is to integrate AI-driven intelligence into existing security operations, improve early warning capabilities, and enable organisations to move from reactive defence toward proactive threat management.

The objective is to support organisations in improving threat awareness, reducing response time, and strengthening overall cyber resilience through intelligence-led security strategies.

Key Focus Areas Include the Following:

- **AI-Enabled Threat Analysis** – Identifying patterns and emerging attack techniques.
- **Threat Actor & Campaign Insights** – Understanding behaviours and motivations.
- **Early Warning & Predictive Indicators** – Enhancing proactive risk detection.
- **Intelligence Integration** – Aligning insights with security operations and response.
- **Noise Reduction & Prioritisation** – Improving analyst efficiency and focus.
- **Strategic Threat Intelligence** – Supporting long-term security planning.

PROACTIVE THREAT INTELLIGENCE



Strengthening Anticipation, Early Detection, and Strategic Risk Awareness

As cyber threats continue to evolve in sophistication, scale, and intent, organisations must move beyond reactive security approaches toward proactive identification of emerging risks. Reliance on post-incident indicators or static threat feeds can leave critical gaps in awareness, increasing the likelihood of successful attacks and prolonged exposure.

Proactive Threat Intelligence focuses on enabling organisations to anticipate threats before they materialise into incidents. This area of work emphasises continuous monitoring of the threat landscape, analysis of emerging attack techniques, and assessment of threat actor behaviour to identify early indicators of potential compromise.

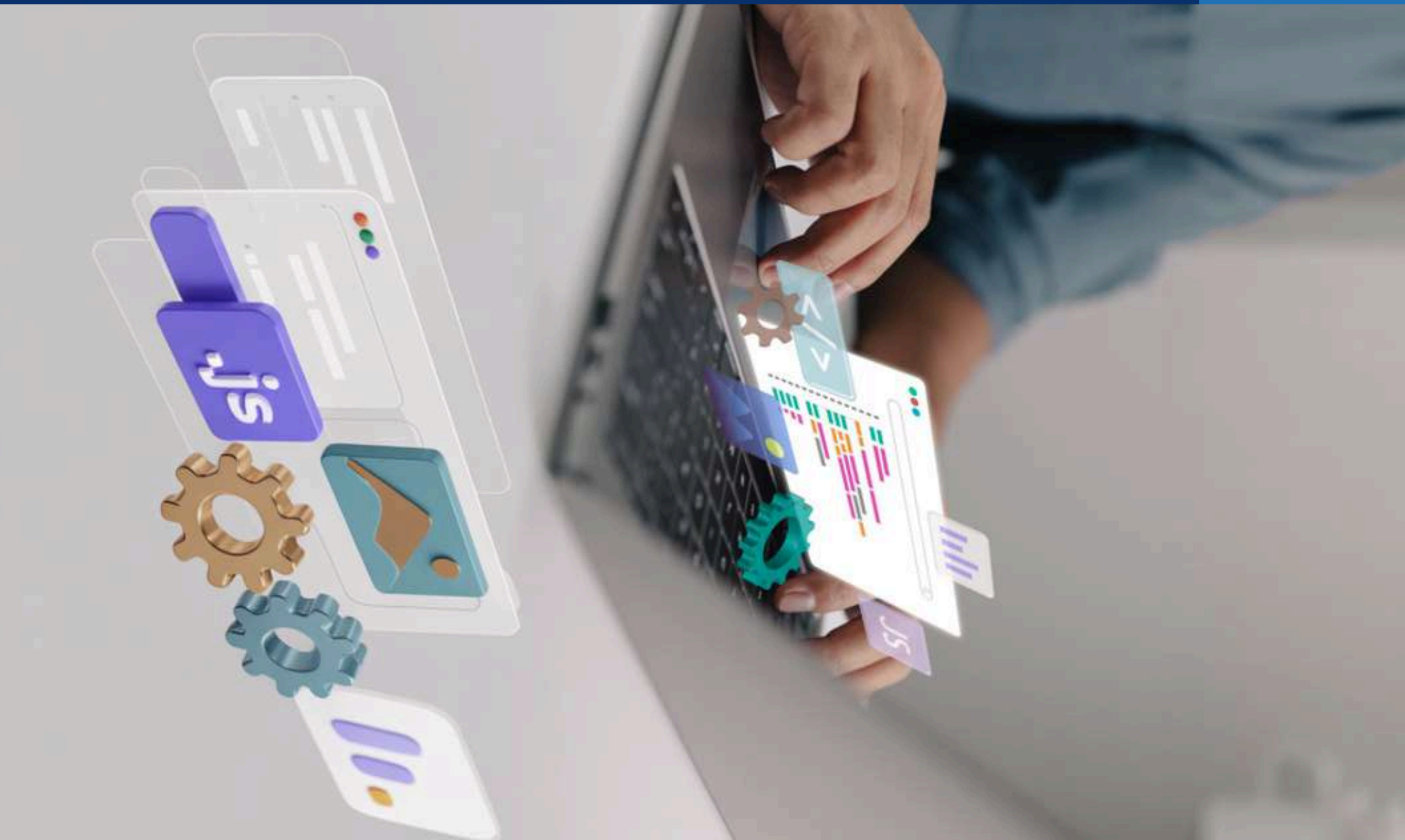
Through intelligence briefings, advisory engagements, and expert-led discussions, this work brings together security leaders, analysts, and risk stakeholders. The objective is to embed forward-looking intelligence into security operations and governance frameworks, supporting timely preventive actions and informed strategic decision-making.

The objective is to support organisations in reducing uncertainty, improving preparedness, and strengthening resilience by integrating proactive threat intelligence into cybersecurity planning.

Key Focus Areas Include the Following:

- **Emerging Threat Monitoring** – Tracking evolving attack techniques and trends.
- **Threat Actor Analysis** – Understanding capabilities, intent, and targeting patterns.
- **Early Warning Indicators** – Identifying precursors to potential attacks.
- **Intelligence-to-Action Workflows** – Aligning insights with preventive controls.
- **Strategic Risk Insights** – Supporting leadership-level security planning.
- **Continuous Intelligence Improvement** – Adapting intelligence to changing threats.

WEBSITE AND APPLICATION SECURITY TESTING



Website and Mobile Application Security Testing

As organisations increasingly rely on websites and mobile applications to deliver services, engage users, and support core business functions, application-layer vulnerabilities have become a critical source of cyber risk. Weaknesses in application design, authentication, data handling, or logic can expose sensitive information, disrupt services, and undermine user trust.

Website and Mobile Application Security Testing focuses on identifying and addressing security weaknesses across web and mobile environments through structured, real-world testing. This area of work emphasises assessing applications against realistic attack scenarios to uncover vulnerabilities that automated tools alone may not detect, including flaws in business logic, access controls, and data protection mechanisms.

Through controlled testing engagements, expert analysis, and stakeholder discussions, this work brings together development teams, security professionals, and risk stakeholders. The objective is to provide clear, actionable insights that support prioritised remediation, strengthen secure development practices, and improve overall application security posture.

The objective is to support organisations in reducing application-layer risk, protecting user data, and ensuring that digital platforms remain secure and resilient.

Key Focus Areas Include the Following:

- **Web Application Security Testing** – Identifying vulnerabilities in websites and portals.
- **Mobile Application Security Testing** – Assessing iOS and Android application risks.
- **Authentication & Access Control Testing** – Evaluating identity and session management.
- **Input Validation & Data Protection** – Preventing injection and data leakage issues.
- **Business Logic Testing** – Identifying design and workflow weaknesses.
- **Remediation & Secure Development Guidance** – Supporting effective vulnerability resolution.

ATHENIAN TECH

Contact Us

www.atheniantech.com