HexaBreach

BEYOND LIMITS, BEYOND EXPECTATIONS

CORPORATE CAPABILITIES BROCHURE

Cybersecurity. Digital Forensics. Threat Intelligence. Cyber Resilience.

Advanced security, investigation, intelligence, and resilience services for organizations operating in complex digital environments.

CREST PARTNER | ISO 27001:2022 | GDPR COMPLIANT | TRUSTED. SECURE. RESILIENT.

CONTENTS

What We Deliver

A unified view of HexaBreach capabilities across platforms, managed services, offensive security, security and identity, digital forensics, specialized services, resilience, training, academics, and industry solutions.

COMPANY OVERVIEW

Built for Complex Cyber Challenges

HexaBreach is a cybersecurity, digital forensics, threat intelligence, and cyber resilience company delivering advanced technical services, strategic advisory, managed security capability, and specialist investigation support for organizations operating in high-risk digital environments.

We help enterprises, public-sector institutions, financial organizations, telecommunications providers, legal teams, and critical infrastructure operators anticipate threats, protect critical assets, investigate incidents, recover operations, and strengthen long-term security maturity.

Security Engineering

We design, implement, assess, and optimize security architectures across cloud, identity, endpoint, network, application, data protection, and security operations environments.

Digital Investigations

We preserve, acquire, examine, recover, and interpret digital evidence across endpoints, mobile devices, cloud platforms, networks, storage media, and enterprise systems.

Cyber Resilience

We prepare organizations to withstand disruption, validate recovery capability, reduce downtime, restore operations, and improve maturity after cyber incidents.

Threat Intelligence

We transform external threat activity, adversary behavior, exposure data, and incident findings into actionable intelligence for decision-makers and security teams.

Governance, Risk & Compliance

We support security governance, assurance, audit readiness, risk management, compliance alignment, policy development, and executive security reporting.

Specialized Services

We provide advanced forensic access, technical recovery, digital reconstruction, mobile extraction, and expert support for complex cases where standard tools are not enough.

CYBERSECURITY · DIGITAL FORENSICS · INCIDENT RESPONSE · THREAT INTELLIGENCE · GRC · MDR · CLOUD SECURITY · IDENTITY SECURITY · MOBILE FORENSICS · DATA RECOVERY · CYBER RESILIENCE · TRAINING

WHY HEXABREACH

Trusted Expertise. Proven Methodologies. Measurable Outcomes.

HexaBreach combines advanced cybersecurity expertise, digital investigation capability, threat intelligence, and resilience engineering to help organizations protect critical assets, respond effectively to incidents, and strengthen long-term operational security.

Deep Technical Capability

Hands-on practitioners with experience across security engineering, penetration testing, digital forensics, incident response, cloud security, and cyber resilience.

Evidence-Driven Delivery

Our work is grounded in validated findings, documented procedures, forensic integrity, and decision-ready reporting that supports confident action.

Advanced Specialized Services

From advanced mobile extraction and digital reconstruction to technical investigations, we deliver capabilities beyond conventional consulting engagements.

Outcome-Focused Engagements

We help organizations reduce risk, improve visibility, accelerate response, strengthen resilience, and enhance overall security maturity.

Our Security Lifecycle Approach

Protect
STRENGTHEN DEFENSES

Detect
IDENTIFY THREATS EARLY

Investigate
TURN EVIDENCE INTO INTELLIGENCE

Recover
RESTORE AND STRENGTHEN OPERATIONS

Trusted Expertise

Experienced security, forensic, and resilience professionals.

Proven Methodologies

Structured approaches aligned with industry best practices.

Advanced Capability

Modern tooling and specialist technical expertise.

Measurable Impact

Focused on outcomes that strengthen security posture.

CORE SERVICE PORTFOLIO

Integrated Cyber Capability Across the Full Lifecycle

HexaBreach delivers a comprehensive portfolio of cybersecurity, digital forensics, intelligence, governance, and resilience services designed to help organizations prevent attacks, detect threats, investigate incidents, recover operations, and continuously improve their security posture.

Cybersecurity Services

Enterprise security services designed to assess, strengthen, and continuously improve organizational defense capability.

- Advanced Penetration Testing
- Application Security Audit
- Vulnerability Assessment
- Cloud Security Implementation
- Zero Trust Architecture

Digital Forensics & Incident Response

Forensic-led investigations, incident response, evidence preservation, and recovery support for high-impact security events.

- Incident Response
- Computer Forensics
- Mobile Forensics
- Network Forensics
- Cloud Forensics

Threat Intelligence

Strategic, operational, and tactical intelligence to help organizations understand adversaries, exposures, and emerging risks.

- Cyber Threat Intelligence
- Compromise Assessment
- Insider Threat Assessment
- Dark Web Monitoring
- Threat Actor Profiling

Governance, Risk & Compliance

Practical advisory services for security governance, assurance, risk management, and regulatory alignment.

- Assurance & Audit
- Risk Management
- Compliance & Governance
- SOC Audit
- Cyber Security Due Diligence

Cyber Resilience & Recovery

Resilience engineering services that prepare organizations to withstand, recover from, and improve after disruption.

- Ransomware Recovery
- Disaster Recovery as a Service
- Recovery Readiness Assessment
- Active Directory Recovery
- Multi-Cloud Resilience

Hexabreach Specialized Services

Advanced technical services for complex forensic, operational, and investigative challenges that exceed standard tooling.

- Advanced Mobile Extraction
- Advanced Data Recovery
- Digital Reconstruction
- Technical VAPT
- Specialized Investigations

ASSESS · PROTECT · DETECT · INVESTIGATE · RESPOND · RECOVER · IMPROVE

HEXASHIELD UNIFIED SOC PLATFORM

Visibility. Detection. Automation. Response.

HexaShield is a unified security operations platform designed to centralize visibility, accelerate threat detection, automate response actions, and improve operational efficiency across modern enterprise environments.

Built to support organizations facing increasingly complex cyber threats, HexaShield consolidates telemetry, analytics, investigation workflows, and response orchestration into a single operational ecosystem—enabling security teams to move faster, investigate deeper, and respond with confidence.

Unified SIEM

Centralized collection, normalization, correlation, investigation, and reporting across diverse security data sources.

Native SOAR

Automate repetitive tasks, orchestrate response actions, and reduce analyst workload through intelligent workflows.

Behavioral Analytics & UEBA

Detect anomalous user and entity behavior patterns that may indicate insider threats or compromised accounts.

Asset & Risk Mapping

Correlate assets, identities, vulnerabilities, and threats to provide context-driven risk visibility.

SECURITY OPERATIONS | THREAT DETECTION | INCIDENT RESPONSE | AUTOMATION | THREAT HUNTING

HEXACORE DFIR

Hybrid Digital Forensics & Incident Response

HexaCore DFIR combines expert-led incident response, forensic investigation, evidence management, and scalable analysis infrastructure into a unified digital forensics platform.

Designed for organizations requiring rapid response and deep investigative capability, HexaCore enables secure evidence collection, centralized forensic processing, collaborative investigations, and defensible reporting while maintaining evidential integrity throughout the investigative lifecycle.

Remote Evidence Collection

Secure acquisition of endpoint, server, cloud, and mobile evidence from distributed environments.

Memory Acquisition

Capture volatile evidence to support malware analysis, compromise assessment, and threat reconstruction.

Centralized DFIR Operations

Consolidate investigations, evidence, reporting, and examiner workflows within a single platform.

Investigation Collaboration

Enable analysts, legal teams, and investigators to work from a common evidence framework.

INCIDENT RESPONSE · DIGITAL FORENSICS · EVIDENCE MANAGEMENT · MEMORY ANALYSIS · THREAT INVESTIGATION

HEXANDR

Network Detection & Response

HexaNDR delivers continuous network visibility, behavioral analytics, threat detection, and rapid investigation capabilities across enterprise environments.

By analyzing network communications, traffic patterns, lateral movement, and anomalous behaviors, HexaNDR helps organizations identify sophisticated threats that traditional signature-based controls often miss.

Network Visibility

Monitor communications across on-premises, cloud, hybrid, and remote environments.

Behavioral Detection

Identify unusual activity patterns, suspicious communications, and attacker behavior.

Threat Hunting

Investigate indicators of compromise and uncover hidden attacker activity.

Rapid Investigation

Reconstruct attacker movements, communication paths, and affected assets.

NETWORK SECURITY · THREAT DETECTION · THREAT HUNTING · BEHAVIOR ANALYTICS · NDR

HEXAVISION IR

Video Surveillance as a Service

HexaVision IR provides cloud-managed video surveillance, intelligent monitoring, event investigation, and operational visibility without the complexity of traditional surveillance deployments.

Combining modern IP cameras, secure cloud infrastructure, centralized management, and intelligent analytics, HexaVision IR enables organizations to enhance security, improve situational awareness, and simplify video operations across distributed locations.

Cloud Video Management

Centralized administration and monitoring across multiple locations and facilities.

Remote Monitoring

Access live and recorded footage securely from anywhere through a unified platform.

Intelligent Analytics

Accelerate investigations using event search, motion analytics, and operational insights.

Scalable Deployment

Support single sites, multi-branch organizations, campuses, and distributed operations.

VSAAS · VIDEO SURVEILLANCE · REMOTE MONITORING · CLOUD SECURITY · VIDEO ANALYTICS

SECURITY & IDENTITY

Securing Modern Enterprises Through Identity-Centric Security.

Our services combine modern security frameworks, advanced threat detection, identity security, security orchestration, and Zero Trust principles to help organizations reduce risk, improve visibility, and establish a stronger foundation for cyber resilience.

Cyber Security Mesh Architecture (CSMA)

Design and implement distributed security architectures that improve interoperability, visibility, and policy enforcement across modern environments.

Cyber Threat Intelligence

Deliver strategic, operational, and tactical intelligence to improve threat awareness, decision-making, and proactive defense.

Extended Detection & Response (XDR)

Correlate endpoint, cloud, network, identity, and application telemetry to accelerate threat detection and investigation.

Identity & Access Management (IAM)

Establish secure identity governance, authentication, lifecycle management, and access control processes.

Identity Threat Detection & Response (ITDR)

Detect, investigate, and respond to attacks targeting identities, credentials, authentication systems, and directory services.

Managed Detection & Response (MDR)

Continuous monitoring, threat hunting, incident triage, and response support delivered by HexaBreach analysts.

Privileged Access Management (PAM)

Secure, monitor, and control privileged accounts, administrative access, and elevated credentials.

Privileged Identity Management (PIM)

Govern privileged roles through just-in-time access, approval workflows, and least-privilege enforcement.

Zero Trust Architecture (ZTA)

Design and implement Zero Trust strategies based on continuous verification, least-privilege access, identity-centric controls, micro-segmentation, and adaptive security policies across users, devices, applications, and data.

IDENTITY SECURITY · ZERO TRUST · IAM · PAM · PIM · ITDR · XDR · THREAT INTELLIGENCE · SOAR · MDR

MANAGED DETECTION & RESPONSE

Continuous Threat Monitoring, Detection & Response

HexaBreach MDR delivers continuous security monitoring, threat detection, threat hunting, incident triage, and response support to help organizations rapidly identify and contain cyber threats before they impact business operations.

Combining advanced analytics, security expertise, and proven operational processes, our MDR service extends your security capability with around-the-clock visibility, proactive threat identification, and actionable guidance during security events.

24/7 Security Monitoring

Continuous monitoring across endpoints, identities, cloud services, applications, and network infrastructure.

Threat Hunting

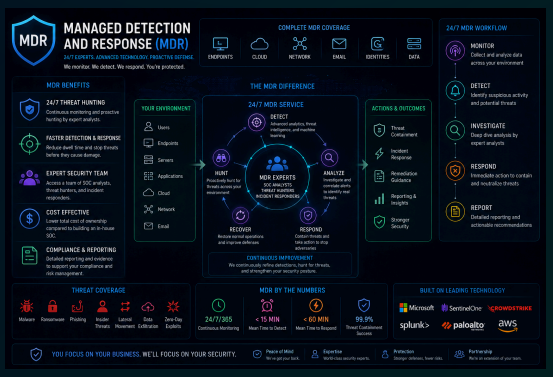
Proactive investigation of suspicious activity, attacker behaviors, and emerging threat techniques.

Detection Engineering

Continuous improvement of detection content, analytics, correlation rules, and response playbooks.

Incident Response Support

Escalation, containment guidance, investigation support, and coordinated response during security incidents.



24/7 MONITORING

THREAT DETECTION

THREAT HUNTING

DETECTION ENGINEERING

INCIDENT RESPONSE

OFFENSIVE SECURITY

Test Like an Adversary. Improve Like an Enterprise.

Advanced Penetration Testing

Real-world attack simulations that identify exploitable weaknesses across systems, networks, applications, and users to assess overall security risk.

Tactical VAPT

Enterprise-focused vulnerability assessment and penetration testing that uses active attack techniques to uncover security gaps beyond automated scanning.

Red-Team Simulation

Adversary emulation exercises that test security controls, detection capabilities, incident response, and organizational resilience.

Application Security Audit

Comprehensive assessment of application architecture, code, configurations, and runtime security to identify and mitigate risks.

Vulnerability Assessment

Identification, validation, and prioritization of known vulnerabilities across infrastructure and applications using automated and manual techniques.

Source Code Review

Detailed analysis of source code to uncover security flaws, insecure coding practices, logic errors, and hidden vulnerabilities.

Breach & Attack Simulation

Continuous testing of security controls through safe attack simulations to validate detection and response effectiveness.

Vulnerability Management

Ongoing vulnerability discovery, prioritization, and remediation across on-premises, cloud, and hybrid environments.

API Penetration Testing

Specialized security testing of APIs to identify authentication, authorization, business logic, and data exposure vulnerabilities.

PENETRATION TESTING | TACTICAL VAPT | RED TEAMING | APPLICATION SECURITY | API SECURITY | CLOUD TESTING | BAS

DIGITAL FORENSICS & INCIDENT RESPONSE

Preserve Evidence. Reconstruct Events. Restore Confidence.

HexaBreach Digital Forensics & Incident Response services help organizations investigate security incidents, determine root causes, preserve critical evidence, contain threats, and restore operations while maintaining forensic integrity throughout the investigative process.

Incident Response

Expert-led containment, investigation, and recovery from ransomware, data breaches, insider threats, and other cyber incidents. We combine threat intelligence, forensic analysis, and response strategy to identify root causes, stop attacker activity, and support secure recovery.

Computer Forensics

Digital investigations and evidence recovery from laptops, desktops, servers, and virtual machines. We preserve and analyze digital artifacts in a forensically sound and legally defensible manner for cyber incidents, fraud, and internal investigations.

Mobile Forensics

Acquisition, analysis, and reporting of digital evidence from smartphones, tablets, and connected devices. We support investigations, litigation, regulatory inquiries, and incident response through forensic examination of Android and iOS systems.

Network Forensics

Analysis of network traffic, logs, and security events to uncover unauthorized access, malicious activity, and data exfiltration. We reconstruct incidents and provide detailed visibility into attacker behavior and timelines.

Cloud Forensics

Investigation of security incidents across AWS, Microsoft Azure, and Google Cloud environments. We analyze cloud logs, configurations, and audit trails to reconstruct events and preserve evidence for compliance and legal requirements.

Compromise Assessment

Intelligence-driven investigations designed to uncover hidden or ongoing breaches. Through threat hunting, forensic analysis, and malware detection, we identify attacker activity, persistence mechanisms, and potential data exposure.

INCIDENT RESPONSE | COMPUTER FORENSICS | MOBILE FORENSICS | NETWORK FORENSICS | CLOUD FORENSICS | COMPROMISE ASSESSMENT

HEXABREACH SPECIALIZED SERVICES (HSS)

When Standard Tools Are Not Enough

HexaBreach Specialized Services provides advanced technical capabilities for complex forensic, recovery, intelligence, and investigative challenges that exceed the scope of conventional tools, methodologies, and operational workflows.

Leveraging specialist expertise, advanced laboratory resources, and proven investigative methodologies, HSS supports law enforcement agencies, legal teams, enterprises, insurers, and security professionals confronting difficult technical and evidential challenges.

Advanced Mobile Access

Extraction and analysis support for locked, encrypted, damaged, unsupported, and high-security mobile devices.

Data Recovery & Reconstruction

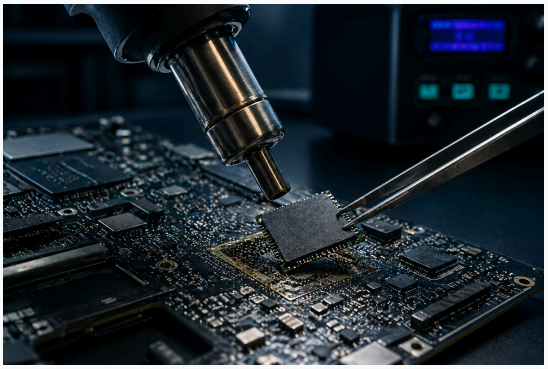
Recover deleted, damaged, fragmented, encrypted, and partially corrupted digital information.

Digital Reconstruction

Rebuild timelines, databases, communications, user activity, and evidential event sequences.

Specialized Investigations

Technical support for sensitive investigations, insider threats, fraud, cybercrime, and complex incidents.



ADVANCED EXTRACTION

DATA RECOVERY

DIGITAL RECONSTRUCTION

CYBERCRIME INVESTIGATION

TECHNICAL INTELLIGENCE

DISASTER RECOVERY & RESILIENCE

Building Recovery Capability Before an Incident.

HexaBreach Disaster Recovery & Resilience services help organizations prepare for cyber incidents, ransomware attacks, infrastructure failures, and operational disruptions by strengthening recovery capability, validating resilience strategies, and ensuring critical business services can be restored quickly and securely.

Cyber Resilience & Ransomware Recovery

Assess resilience against ransomware attacks and establish structured recovery strategies for critical systems, identities, applications, and business operations.

Disaster Recovery as a Service

Design, implement, operate, and continuously improve disaster recovery capabilities for enterprise environments.

Managed Recovery Operations Center

Centralized recovery coordination, monitoring, reporting, and operational management during recovery activities.

Active Directory Recovery & Identity Resilience

Strengthen identity infrastructure resilience and establish rapid recovery procedures for compromised directory services.

Recovery Readiness Assessment & DR Audit

Evaluate recovery maturity, governance structures, documentation, operational readiness, and recovery objectives.

Multi-Cloud Resilience Engineering

Architect resilient recovery capabilities across cloud, hybrid, and multi-cloud environments.

Recovery Security Testing & DR Penetration Testing

Validate recovery environments, failover capabilities, backup security, and disaster recovery controls.

Continuous Recovery Validation Platform

Continuously test, validate, and measure recovery capability through automated recovery assurance and resilience exercises.

Advanced Data Recovery & Digital Reconstruction

Recover critical information from damaged, deleted, encrypted, fragmented, or compromised digital assets.

CYBER RESILIENCE · RANSOMWARE RECOVERY · DISASTER RECOVERY · IDENTITY RECOVERY · CLOUD RESILIENCE · RECOVERY TESTING · RECOVERY VALIDATION · DATA RECOVERY

TRAINING & CERTIFICATION

Developing The People Behind The Defense.

HexaBreach Training & Certification programs equip cybersecurity professionals, investigators, analysts, engineers, and operational teams with practical, real-world skills designed to strengthen organizational capability and improve security outcomes. Delivered through instructor-led training, private cohorts, workshops, simulations, and customized learning pathways, our programs focus on hands-on technical proficiency, operational readiness, and professional development.

Advanced Digital Forensics

Comprehensive training in computer, mobile, cloud, and network forensics, evidence handling, forensic methodologies, and digital investigations.

Incident Response & Crisis Management

Develop the skills required to identify, contain, investigate, coordinate, and recover from cybersecurity incidents and major security events.

Security Operations Center (SOC)

Build expertise in SOC operations, security monitoring, alert triage, threat analysis, operational workflows, and detection engineering.

Threat Hunting & Detection Engineering

Learn proactive threat hunting, attacker behavior analysis, detection development, SIEM analytics, and advanced investigative techniques.

Offensive Security & Penetration Testing

Gain practical knowledge in vulnerability assessments, penetration testing, adversary emulation, and offensive security methodologies.

Cybersecurity Engineering

Training focused on security architecture, Zero Trust, identity security, cloud security, and enterprise defense strategies.

Cloud & Infrastructure Security

Secure modern cloud environments, hybrid infrastructures, workloads, applications, and critical business systems.

Executive & Leadership Programs

Strategic cybersecurity training for executives, managers, board members, and decision-makers responsible for cyber risk governance.

Custom Enterprise Training

Tailored learning programs, private cohorts, workshops, and capability development initiatives aligned to organizational objectives.

DIGITAL FORENSICS · MOBILE ANALYSIS · NETWORK FORENSICS · SOC ENGINEERING · THREAT HUNTING · INCIDENT RESPONSE · SECURITY ARCHITECTURE · PRIVATE COHORTS · LEARNING HUB

HEXABREACH ACADEMICS

Bridging Academia, Research & Industry Capability.

HexaBreach Academics helps universities, colleges, TVETs, research institutions, and training providers build practical cybersecurity, digital forensics, and cyber resilience capability through academic partnerships, lab development, curriculum support, and workforce readiness programs.

Academic Partnerships

Collaborative programs that strengthen institutional cyber and DFIR education.

Cyber & DFIR Labs

Design and deployment of cyber ranges, forensic labs, and simulation environments.

Curriculum Support

Industry-aligned modules for cybersecurity, forensics, threat intelligence, and resilience.

Instructor Enablement

Training and technical support for lecturers, trainers, and program facilitators.

Workforce Readiness

Practical pathways preparing learners for operational cyber and investigation roles.

Research & Innovation

Support for applied research, cyber innovation, and emerging technology initiatives.

ACADEMIC PARTNERSHIPS · CYBER LABS · DFIR LABS · CYBER RANGES · CURRICULUM · WORKFORCE READINESS

INDUSTRY SOLUTIONS

Cybersecurity, Investigation & Resilience For High-Trust Industries.

HexaBreach delivers sector-specific cybersecurity, digital forensics, resilience, intelligence, and recovery services tailored to the operational, regulatory, and security requirements of critical industries.

Government & Public Sector

Cyber investigations, digital evidence support, resilience programs, intelligence services, and critical infrastructure protection.

Financial Services

Fraud investigations, ransomware resilience, regulatory assurance, identity security, and SOC modernization.

Telecommunications

Network visibility, incident response, cyber resilience, and large-scale security monitoring.

Enterprise & Commercial

Managed security, offensive testing, cloud security, identity governance, and resilience engineering.

Legal & Investigations

Digital evidence recovery, litigation support, forensic reporting, expert analysis, and case support services.

Critical Infrastructure

Operational resilience, cyber readiness, incident response, recovery planning, and OT visibility.

Education & Research

Cyber laboratories, digital forensics programs, academic partnerships, workforce development, and cyber ranges.

Healthcare

Protection of sensitive data, ransomware preparedness, identity security, and operational continuity planning.

Insurance & Risk Services

Breach investigations, compromise assessments, cyber claims support, and digital evidence services.

GOVERNMENT · FINANCIAL SERVICES · TELECOMMUNICATIONS · ENTERPRISE · HEALTHCARE · CRITICAL INFRASTRUCTURE · EDUCATION · INSURANCE · LEGAL

ENGAGEMENT MODELS

Flexible Delivery For Different Operational Needs.

HexaBreach engagements are structured to support one-time projects, urgent incidents, continuous operations, long-term advisory, specialized investigations, and strategic transformation programs.

Project-Based Engagements

Defined scope, timeline, deliverables, and outcome-focused execution for assessments, implementations, audits, investigations, and recovery projects.

Incident Response Retainers

Priority access to forensic, incident response, recovery, and crisis support when cyber incidents require immediate expert assistance.

Managed Services

Continuous security monitoring, detection engineering, response support, platform management, resilience validation, and operational improvement.

Specialized Casework

Advanced expert support for complex forensic, recovery, cybercrime, intelligence, mobile extraction, and digital reconstruction matters.

Advisory & Transformation

Strategic support for security architecture, governance, Zero Trust, SOC modernization, resilience programs, and executive cyber strategy.

Training & Capacity Building

Instructor-led training, private cohorts, academic programs, workshops, cyber ranges, and workforce readiness initiatives.

Engagement Lifecycle

DISCOVER · ASSESS · DESIGN · DEPLOY · OPERATE · INVESTIGATE · RECOVER · IMPROVE

Each engagement is tailored to the client’s operating environment, risk profile, regulatory obligations, technical maturity, and desired business outcomes.

HexaBreach

BEYOND LIMITS, BEYOND EXPECTATIONS

ENGAGE HEXABREACH

Secure Today. Strengthen Tomorrow.

From cybersecurity and digital forensics to resilience engineering, threat intelligence, managed services, and specialized investigations, HexaBreach helps organizations navigate complex cyber challenges with confidence.

Website

www.hexabreach.com

Telephone

+254 728 146 497

Email

contact@hexabreach.com

Location

Nairobi, Kenya

HexaBreach

BEYOND LIMITS, BEYOND EXPECTATIONS

CYBERSECURITY | DIGITAL FORENSICS | THREAT INTELLIGENCE

CYBER RESILIENCE ENGINEERING

WEBSITE
www.hexabreach.com

EMAIL
contact@hexabreach.com

PHONE
+254 728 146 497

LOCATION
Nairobi, Kenya