haktrak

POWERED BY PEOPLE. PROTECTED BY SCIENCE.

COMPANY PROFILE

Exhibition Tower
Manama – Kingdom of Bahrain
+973 17673210
+973 35055473
info@haktraknetworks.com
www.haktraknetworks.com

ABOUT COMPANY

HakTrak is a leading cybersecurity company in the Middle East, renowned for its unwavering commitment to innovation, development, and research. The company was founded in 2015 when our co-founder submitted the first patent, establishing the foundation for real-time threat detection powered by machine learning.

Today, HakTrak is a well-established company with offices in the UK and Bahrain, boasting numerous clients and $2M in revenue. Differentiating ourselves from vendors, we take immense pride in creating our innovative solutions in-house.

At HakTrak, we provide top-notch security solutions to businesses of all sizes, utilizing cutting-edge technology and experienced professionals. Our comprehensive services and solutions protect your systems from ever-increasing cyber threats and offer training and awareness programs to help enterprises understand and manage cybersecurity risks. Our expert team has extensive experience in the field of cybersecurity, enabling them to tackle even the most complex security challenges. Our ultimate purpose is to help enterprises protect their critical data and infrastructure from cyberattacks.

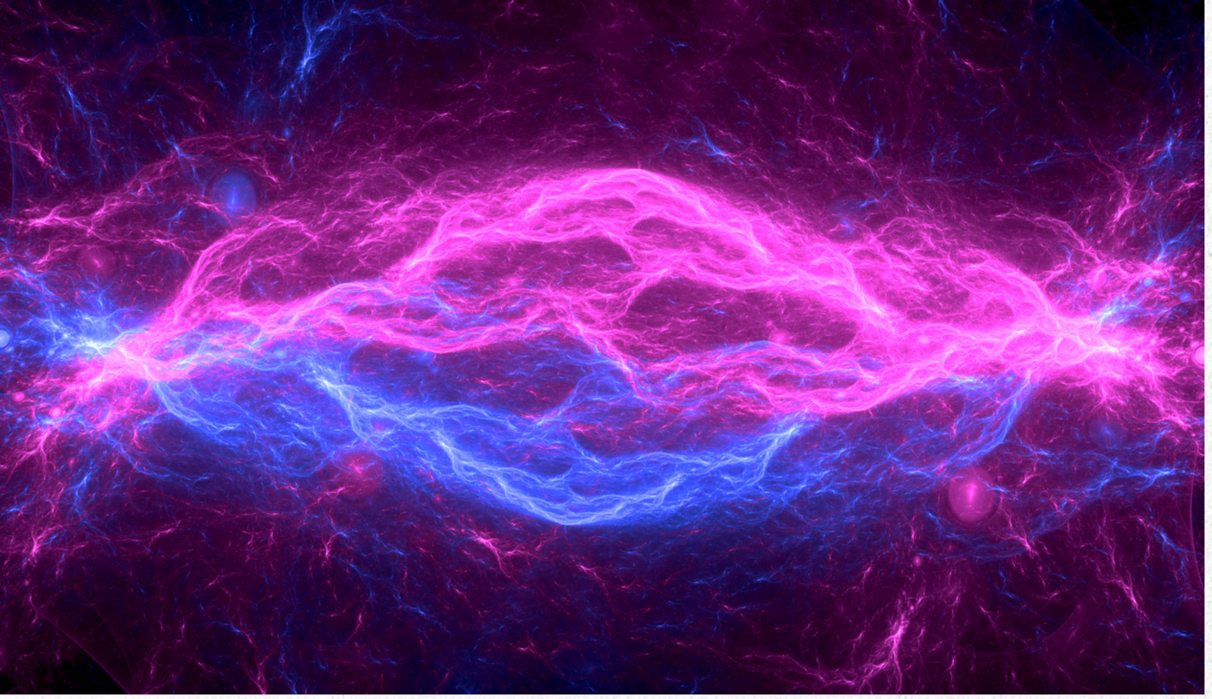
haktrak

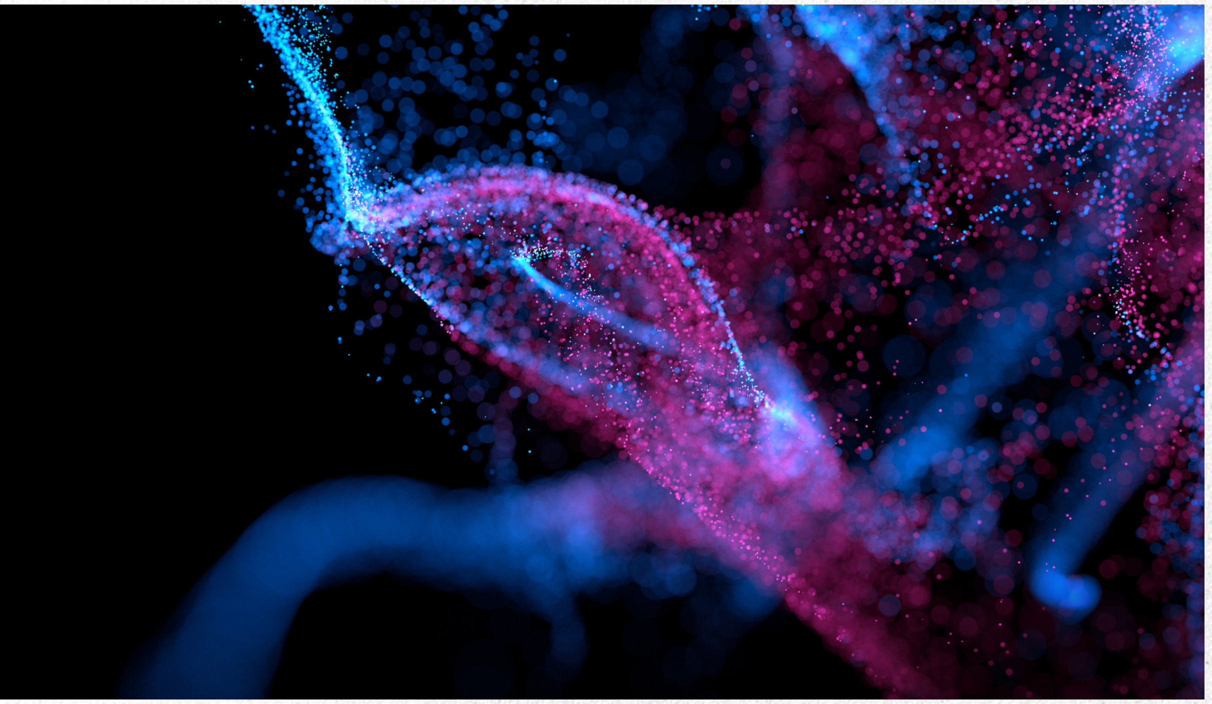
WHY CHOOSE HAKTRAK?

As cyberattacks become increasingly sophisticated and resistant to traditional countermeasures, the importance of security for organizations worldwide continues to grow. Businesses must adapt their security strategies and allocate sufficient resources to detect and respond rapidly to potential breaches.

- **Comprehensive Defense:** Enhance your organization's cybersecurity posture by implementing complete protection against cyber threats through our services and solutions.
- **Innovative Approach:** As a client-centric, cybersecurity-focused, service-oriented, and quality-driven company, HakTrak stands out as a pioneer in the region with its innovative mindset, agile approach, proven best practices, high standards, and disciplined project delivery.
- **Protecting Digital Assets:** Our goal is to help organizations secure their digital assets using HakTrak R&D LAB solutions and services while striving to become global leaders in cybersecurity.

www.haktraknetworks.com





- **Red Team Simulations:** Our Red Team is prepared to test your infrastructure, systems, applications, processes, techniques, and personnel through intelligence-driven adversary simulations that cover the entire lifecycle of a real-world cyberattack.

- **Dedicated MDR and Skilled Security Analysts:** HakTrak provides businesses with a fully staffed operations center that scales with customer growth, ensuring security analysts have the required technology and expertise.

- **Proactive Threat Hunting:** Stay ahead of emerging cyber threats with tailored security solutions to detect and respond to the latest risks.

- **Improved Operational Efficiency:** Enhance your operation's efficiency and resilience with our managed security services, addressing challenges related to skilled resource shortages and ever-growing threats.

- **Cost Savings**: Leverage our cost-effective HakTrak services to reduce the financial burden of maintaining an in-house security team.

- **Regulatory Compliance:** Ensure your organization adheres to industry-specific regulations and standards by implementing our best-in-class cybersecurity solutions.

HAKTRAK SECURITY PLATFORM

haktrak

In the Cloud, On-Premises, or a Hybrid Future-Ready Platform: HakTrak Security Platform is an advanced cyber protection SaaS solution that offers comprehensive visibility, threat hunting, validation, investigation, containment, remediation, and limitless forensic exploration on demand. Our platform boasts unique advantages over traditional network security systems, including an unlimited retention window of full-fidelity network traffic, innovative visualizations, simplicity, and cost savings from an on-demand deployment structure.

Visualized Security: Our platform featured with comprehensive and user-friendly interface offering a complete network view. This intuitive visualization allows for swift identification and effective responses to high-priority threats. By incorporating deep forensics capabilities and practical collaboration tools, our platform empowers security teams to work efficiently and proactively, ensuring a robust defense against evolving cyber threats

Threat Triage and Response: The HakTrak Security Platform employs standard protocols to collect threats from its forensic, response, and predictive capabilities, then delivers the necessary processes to triage, investigate, escalate, and remediate security events swiftly. Incidents are prioritized based on business context, ensuring analysts focus on events posing the most significant risks.

Breach Response: Our platform empowers proactive breach response management. We develop client-specific breach response strategies and store each client's preferred methods in a response process library for swift action during breaches.

Network Threat Detector: Our cutting-edge threat detection system provides a comprehensive, multi-layered detection-in-depth approach to reinforce network security. Our solution identifies potential risks and vulnerabilities across various levels of your network infrastructure by employing advanced analytics, machine learning algorithms, and real-time data processing.

This comprehensive system detects known threats and uncovers emerging and previously unknown attack patterns. Our Network Threat Detector enables early detection of potential security breaches and swift remediation by continuously monitoring network traffic, user behavior, and system logs.

Furthermore, the system is designed to adapt and evolve in response to the ever-changing cyber threat landscape, ensuring your organization remains one step ahead of attackers. With customizable alerts, incident response automation, and seamless integration with your existing security infrastructure, HakTrak's Network Threat Detector offers unparalleled protection for your digital assets.

NGAV, Endpoint Threat Detection, and Response: HakTrak's proprietary endpoint solution unifies Next-Generation Antivirus (NGAV), Endpoint Threat Detection, and Response capabilities into a single, lightweight agent installed across all endpoints. This innovative agent collects comprehensive state information, effectively halting exploits and malware attacks.

By continuously monitoring endpoint activity, HakTrak solution grants insight into endpoints for intrusion analysts, empowering them to identify and remediate potential threats more efficiently. Our system leverages advanced machine learning algorithms and real-time data analysis to detect known and emerging threats, ensuring a robust defense against evolving cybersecurity challenges.

In addition to its powerful threat detection capabilities, HakTrak streamlines incident response through automated workflows, customizable alerts, and seamless integration with existing security infrastructure. Focusing on swift response and proactive threat mitigation, our comprehensive approach to endpoint protection enhances overall network security. It minimizes the risk of data breaches and other cyberattacks, protecting your organization's valuable digital assets.

Forensics, Hunting, and Behavior Analytics: HakTrak's network detector utilizes state-of-the-art forensic techniques and behavior analytics technology, in conjunction with the expertise of our Red Team, to deliver complete visibility, high-performance threat hunting, and superior incident response capabilities.

Our solution incorporates advanced digital forensics methods to examine network traffic, system logs, and user activities in-depth. This comprehensive approach allows for identifying potential security threats and vulnerabilities that may have gone unnoticed by traditional security measures. By conducting thorough forensic investigations, HakTrak's network detector provides valuable insights into your network's security posture, ensuring comprehensive protection against cyberattacks.

Behavior analytics plays a crucial role in our solution, employing machine learning algorithms and real-time data analysis to detect suspicious patterns and anomalies within your network. By continuously monitoring and analyzing network behavior, our platform can proactively identify potential threats and enable swift remediation.

High-performance threat hunting is another crucial component of our solution. Our Red Team actively searches for hidden threats within your network, leveraging forensic evidence and behavior analytics to uncover and neutralize previously undetected risks.

In addition to threat detection, hunting, and forensics, HakTrak's network detector strongly emphasizes superior incident response. Our platform facilitates efficient collaboration among security teams, streamlining the sharing of critical information and enabling them to respond effectively to incidents. With automated workflows, customizable alerts, and seamless integration with your existing security infrastructure, our solution ensures rapid response and remediation of security threats, minimizing the risk of data breaches and other cyberattacks.

IHakTrak Intelligence: Intelligence, in the context of cybersecurity, refers to collecting, analyzing, and disseminating information about potential cyber threats, vulnerabilities, and attack patterns. This information helps organizations understand their risks and protect their networks, systems, and data appropriately.
There are several types of intelligence within the cybersecurity domain:

- **Threat Intelligence:** This type of intelligence focuses on identifying and understanding the tactics, techniques, and procedures (TTPs) used by cybercriminals, as well as their motivations and targets. Threat intelligence helps organizations stay informed about emerging threats and develop proactive risk mitigation strategies.
- **Vulnerability Intelligence**: Vulnerability intelligence involves the identification, analysis, and prioritization of vulnerabilities in software, hardware, and network systems. This information enables organizations to patch or update their plans to reduce the likelihood of a successful cyberattack.
- **Indicators of Compromise (IoC) Intelligence:** IoC intelligence collects and analyzes data points suggesting a security breach or ongoing cyberattack. IoCs include unusual network traffic patterns, suspicious log entries, and malware signatures. Identifying and tracking IoCs help organizations detect and respond to cyber threats more effectively.

- **Open-source Intelligence (OSINT):** OSINT is the collection and analysis of publicly available information from sources such as social media, blogs, forums, and news articles. This type of intelligence can provide valuable insights into threat actors, their TTPs, potential targets, and broader trends in the cybersecurity landscape.
- **Human Intelligence (HUMINT)**: HUMINT is gathered through human interactions, such as interviews, undercover operations, or informants. In cybersecurity, HUMINT can provide insights into cybercriminal organizations' inner workings, motivations, and plans for future attacks.
- **Geopolitical Intelligence/GeoWATCH:** Geopolitical intelligence analyzes political, economic, and social factors influencing cybersecurity. This type of intelligence helps organizations understand the global context in which cyber threats emerge and evolve and the potential impact of geopolitical events on their security posture.
- **Deep and Dark Web Intelligence:** This type of intelligence involves monitoring and analyzing data from the deep and dark web, which are parts of the internet not indexed by traditional search engines. Cybercriminals often use these platforms to conduct illicit activities, such as selling stolen data, sharing hacking tools, or planning cyberattacks. Deep and dark web intelligence can provide insights into emerging threats, attacker TTPs, and potential targets.

- **Third-Party Intelligence:** Third-party intelligence involves collecting and analyzing information about an organization's external partners, suppliers, and vendors. This type of intelligence helps organizations assess the security risks associated with third-party relationships and implement appropriate measures to reduce potential exposure to cyber threats.
- **Identity Intelligence:** Identity intelligence analyzes user behavior, access patterns, and authentication data to detect potential identity-based threats, such as account takeover, insider threats, or unauthorized access. By monitoring and analyzing identity-related data, organizations can identify suspicious activities and take preventive actions to protect sensitive information and systems.

By leveraging these various types of intelligence, organizations can comprehensively understand the threat landscape and proactively defend against cyberattacks. This multi-faceted approach to intelligence ensures that organizations are well-informed and equipped to effectively protect their valuable digital assets.

HakTrak Intelligence, our cutting-edge threat intelligence platform, harnesses the power of over 400 diverse threat intelligence sources and correlates them with over 500 million threat indicators. By combining this vast pool of data with real-time network analysis, our system is designed to detect threats at every stage of an attack's lifecycle, ensuring comprehensive protection for your organization.

Our innovative approach to threat intelligence collection and analysis enables HakTrak Intelligence to identify emerging threats and provide early warnings, allowing your security team to defend against potential attacks proactively and focusing on known and unknown cyber threats; our platform delivers unparalleled insights into the ever-evolving threat landscape.

HakTrak Intelligence's advanced correlation algorithms filter out irrelevant or duplicate information, presenting your security team with actionable intelligence that can inform risk assessments, bolster defenses, prioritize resources effectively, and ensure a more efficient and targeted response to your organization's most critical threats.

In addition to its powerful threat detection capabilities, HakTrak Intelligence supports security teams in incident response and remediation efforts. By providing detailed contextual information about detected threats, our platform enables your team to understand the nature of the attack, its origin, and the potential impact on your organization, facilitating swift and effective decision-making.

By leveraging the power of advanced threat intelligence and real-time network data analysis, HakTrak Intelligence offers unparalleled insight and protection, empowering your organization to stay one step ahead of attackers and protect your valuable digital assets.

HakTrak Security Platform:
A Comprehensive Solution Spanning the Entire Lifecycle

HakTrak Security Platform offers a holistic approach to cybersecurity by addressing the entire lifecycle of an organization's digital assets, working on three dimensions – Internal Security, External Security, and Intelligence-Driven Security. This comprehensive solution ensures that your organization is well-equipped to detect, prevent, and respond to cyber threats at every stage.

● **Internal Security**

● **External Security**

● **Intelligence**

1. Internal Security: Focusing on protecting your organization's internal network, systems, applications, processes, and personnel, our platform delivers advanced threat detection, innovative deception techniques, and robust network security measures. Automated incident response policies and playbooks for various attack scenarios help reduce downtime and potential revenue loss while ensuring the continuity of your business operations.

2. External Security: Our platform addresses external threats by offering solutions for attack surface management, brand protection, domain protection, account takeover protection, executive and VIP protection, digital risk protection, and phishing detection. By proactively identifying and mitigating risks in the external environment, HakTrak ensures the safety of your organization's digital assets, brand reputation, and customer trust.

3. Intelligence-Driven Security: The third dimension of our platform leverages intelligence solutions such as GeoWatch, Dark Web Monitoring, Threat Intelligence, Vulnerability Intelligence, and Third-Party Intelligence. These solutions provide real-time insights, enabling organizations to make informed decisions, anticipate emerging threats, and take proactive measures to protect their assets and infrastructure.

Throughout the entire lifecycle of an organization's digital assets, the HakTrak Security Platform seamlessly integrates with existing security infrastructure while prioritizing remedial tasks based on necessity, ensuring a robust and efficient cybersecurity posture. The platform's continuous monitoring for new vulnerabilities and threats, combined with user behavior analytics and activity regulations, further bolsters your organization's defenses. The Platform offers a comprehensive, three-dimensional approach to cybersecurity that protects your organization against the ever-evolving cyber threat landscape, providing a strong and resilient security posture.

Phishing and Fraud

Phishing attempts are the most prevalent and practical causes of data breaches. HakTrak is committed to ending these cyber threats with our AI-powered technology to detect and prevent phishing, fraud campaigns, and malware-based cyberattacks targeting your employees and clients.

AI-Powered Detection: Our advanced artificial intelligence technology identifies phishing and fraud campaigns in real time, alerting your organization to potential threats before they can cause damage.

Preventative Measures: HakTrak's platform actively works to prevent malicious attacks by detecting and blocking phishing emails and websites, ensuring the safety of your employees and clients.

Deconstructing Infrastructure: Unlike other solutions, HakTrak goes a step further by deconstructing the infrastructure underlying phishing campaigns, effectively dismantling the source of the threat.

Removal of Harmful Sites: Removal of harmful phishing sites from ISPs, web search engines, and social media platforms, minimizing the risk of future attacks.

Data Breach and Compromised Credentials

HakTrak Data Breach Detection scans the surface, deep, and dark web for mentions of your company and executives to identify leaked or stolen data. Our platform detects indications of compromise and provides actionable advice while our intelligence team develops comprehensive insights on breaches and enhanced vulnerabilities.

Dark Web Visibility: Gain valuable insight into the dark web to monitor compromised credentials and potential threats to your organization.
Context-Rich Intelligence: Empower your security teams with improved visibility and context-rich intelligence, enabling them to take real action against compromised credentials.

Identify Credential Compromise: Detect indications of compromise (IOCs) and obtain attacker information, whether from within or outside your organization.

Rapid Breach Detection: Receive automatic alerts when critical data from your organization is disclosed or stolen, ensuring a swift response to potential threats.

Protect Customer Data: Protect PII and customer credentials from breaches and exploitation to maintain customer trust and loyalty.

Physical Security

HakTrak Physical Security Module enhances situational awareness and provides near-real-time alerting for global incidents that pose a physical risk to your organization's people, assets, and business operations. Our Physical Security SOC team continuously detects and analyzes events from multiple digital sources worldwide, quickly distilling them into critical events that could impact your business operations or employees.

Enhanced Situational Awareness: Stay informed about global incidents that may pose a physical threat to your organization's people, assets, and operations.

Continuous Event Detection and Analysis: Our Physical Security SOC team monitors and analyzes events from various digital sources, ensuring you receive timely information about potential threats.

Vetted and Enriched Intelligence: We provide event intelligence that is vetted, enriched, and categorized according to alert rules set within the HakTrak Module.

Customizable Alert Classification: Sort and classify alerts based on essential features of physical threats, such as location, timing, and public impact, allowing your organization to focus on the most relevant events.

INDUSTRIES

haktrak

Government Agencies

HakTrak Solution for Government Agencies: Protecting Critical Information and Infrastructure.

- **Comprehensive Protection**: Defend against cyberattacks, including political impersonation, military frauds, misinformation and disinformation campaigns, and phishing and malware assaults.
- **Multi-Level Security**: Provide cybersecurity solutions for all levels of government, from municipal to federal organizations.
- **Modern Security Solutions**: Address contemporary threats such as account impersonation and takeovers, fraud, email compromise, data leakage, and physical threats.
- **Extended Attack Surface Coverage**: Monitor and protect against cyber risks across social networking sites, deep web, and dark web forums, which have expanded the attack surface.

Oil and Gas

HakTrak Solution for Oil and Gas Industry: Ensuring Secure and Reliable Operations

- **Industrial Control System Protection:** Securing the oil and gas industrial control systems against remote cyberattacks, ensuring the integrity and security of the critical infrastructure.
- **Real-Time Visibility**: Gain real-time visibility into operational data, allowing your organization to swiftly monitor and respond to potential threats.
- **Disciplined Inbound Control:** Implement disciplined inbound control to minimize the risk of unauthorized access and potential damage to your systems.
- **Comprehensive Security Measures:** Address various cyber risks, including ruptures, explosions, fires, releases, and spills, that can impact the safety and stability of your operations.

INDUSTRIES

haktrak

Financial Firms

HakTrak Solution for Financial Firms: Ensuring Secure Financial Transactions and Customer Trust

- **Digital Channel Security:** Safeguard your web portals, social media, and mobile apps from potential cyber threats, ensuring secure interactions between your firm and customers.
- **Proactive Defense:** Identify and address potential risks before they impact your organization or customers, minimizing the chances of successful attacks.
- **Fraud Prevention:** Protect your institution and customers from financial attacks, ensuring the security of sensitive data and transactions.
- **Customer Trust:** Maintain customer trust by demonstrating your commitment to safeguarding their financial information and providing a secure transaction environment.

Healthcare

HakTrak Solution for Healthcare: Protecting Sensitive Data and Ensuring Compliance

- **Data Loss and Breach Prevention:** Prevent vital information leaks and disseminate sensitive data by quickly detecting breaches and taking swift action.
- **Essential Visibility and Control:** Gain real-time visibility beyond traditional network borders to rapidly detect data leaks, corporate risks, and targeted attacks.
- **Scalable, Automated Analysis and Remediation:** Utilize artificial intelligence and automation to reduce time-consuming data collection, analysis, and remediation processes.
- **Compliance Management:** Ensure your healthcare organization adheres to industry-specific regulations and standards, reducing the risk of penalties and reputational damage.

INDUSTRIES

haktrak

Manufacturing Industry

HakTrak Solution for Manufacturing Industry: Safeguarding Valuable Data and Ensuring Uninterrupted Production

- **Managed Digital Identities:** Securely manage digital identities across your organization, ensuring proper access control and reducing the risk of unauthorized access.
- **IoT, IIoT, and ICS Security Protection:** Protect your Internet of Things (IoT), Industrial Internet of Things (IIoT), and Industrial Control Systems (ICS) from potential cyber threats, ensuring the integrity and security of your production processes.
- **Zero Trust Frameworks:** Implement Zero Trust frameworks to minimize the risk of insider threats and maintain strict control over data access within your organization.
- **Advanced Threat Detection and Response:** Utilize cutting-edge technologies to detect and respond to potential cyber threats, minimizing the impact on your manufacturing operations.

E-Commerce

HakTrak Solution for E-Commerce: Ensuring Safe and Reliable Online Transactions

- **Pre-Attack Compliance:** Ensure your E-Commerce platform adheres to industry-specific security standards and regulations, reducing the risk of potential cyberattacks.
- **Penetration Testing:** Identify vulnerabilities in your E-Commerce platform through rigorous penetration testing, enabling you to address potential weaknesses before they can be exploited.
- **Vulnerability Assessment:** Regularly assess your platform's security posture to detect and remediate any vulnerabilities that may emerge over time.
- **Quick Response and Containment:** Implement rapid response and containment measures in the event of a security incident, minimizing the impact on your E-Commerce operations and customers.

MDR

The significance of security for organizations worldwide is continually increasing as cyberattacks become more complex and resistant to standard countermeasures. Businesses must realign their security strategies and allocate adequate resources to detect and respond swiftly to potential breaches.

Key Benefits of Using HakTrak Managed Detection and Response Service

- **Comprehensive Defense:** HakTrak offers one of the most extensive defenses against cybercrime, utilizing our fully managed solution to detect and respond to attacks based on pattern technologies.
- **Innovative Approach:** As a client-centric, cybersecurity-focused, service-oriented, and quality-driven company, HakTrak stands out as a pioneer in the region through its innovative mindset, agile approach, proven best practices, high standards, and project delivery discipline.
- **Protecting Digital Assets:** We aim to help organizations secure their digital assets through a range of HakTrak R&D LAB solutions and services while striving to become global leaders in cybersecurity.
- **Red Team Simulations**: Our Red Team is prepared to test your infrastructure, systems, applications, processes, techniques, and personnel through intelligence-driven adversary simulations covering the entire lifecycle of a real-world cyberattack.
- **Dedicated MDR and Skilled Security Analysts:** HakTrak provides businesses with a fully staffed operations center that scales with customer growth, ensuring security analysts have the required technology and expertise.
- **Enhanced Security:** Strengthen your organization's cybersecurity posture by implementing comprehensive protection against cyber threats.
- **Proactive Threat Hunting:** Stay ahead of emerging cyber threats with tailored security solutions to detect and respond to the latest risks.

- **Improved Operational Efficiency:** Enhance your operation's efficiency and resilience with our managed security services, addressing challenges related to skilled resource shortages and ever-growing threats.
- **Cost Savings**: Leverage our cost-effective MDR service to reduce the financial burden of maintaining an in-house security team.
- **Regulatory Compliance**: Ensure your organization to industry-specific regulations and standards by implementing our best-in-class cybersecurity solutions.

HakTrak Adversary Disruption: Neutralize Threats and Prevent Future Attacks

HakTrak Adversary Disruption offers a sophisticated cybersecurity solution to protect your organization against disruptive cyberattacks and data breaches. This service includes Attack Detection and Threat Hunting, Rapid Incident Response, Defense In Depth, Cybersecurity Risk Rating, and Data Leak Detection. Our security analysts continuously conduct threat intelligence research and hunting operations using cutting-edge technologies to identify and neutralize threats with a personalized adaptive defense system that stays up-to-date with the latest cyber threats.

Attack Detection and Threat Hunting

Our security analysts work 24x7x365 on threat intelligence research and hunting missions, leveraging host and network telemetry and security analytics to detect advanced attacks.

Rapid Incident Response Services

We offer fast support for detecting, identifying, isolating, and nullifying active threats against your organization.

Defense in Depth

HakTrak's Defense in Depth continuously adapts to the latest cyber threats, ensuring the protection of your data, critical infrastructure, and applications. This defense meets the most stringent industry security standards.

Cybersecurity Risk Rating

Our Cybersecurity Risk Rating (CRR) assesses your organization's cybersecurity performance, indicating your susceptibility to attack.

Data Leak Detection

HakTrak's Defense in Depth continuously adapts to the latest cyber threats, ensuring the protection of your data, critical infrastructure, and applications. This defense meets the most stringent industry security standards.

Deep and Dark Web Monitoring

HakTrak Dark Web Monitoring offers an in-depth look into the hidden realms of the deep and dark web, providing valuable insights that help safeguard your organization. By gaining visibility into underground forums and marketplaces, our monitoring service uncovers potential data leaks, stolen credentials, and chatters related to cyberattacks targeting your business.

Our team of skilled security analysts continuously scans and monitors these obscure corners of the internet, identifying any threats that could compromise your organization's security. With real-time alerts, you can stay ahead of cybercriminals and take appropriate action to protect your digital assets.

The Dark Web Monitoring includes

- **Early Detection:** Proactively identify potential threats before they escalate, enabling swift action to mitigate risks.
- **Stolen Credential Monitoring:** Discover if your organization credentials have been compromised, allowing you to take the necessary steps to secure your accounts.
- **Threat Intelligence:** Gain valuable insights into emerging trends and tactics used by cybercriminals, helping you stay informed and prepared for potential threats.
- **Brand Protection:** Monitor for unauthorized use of your brand or intellectual property, preventing potential damage to your reputation and customer trust.
- **Compliance Assurance:** Ensure your organization complies with industry-specific regulations and standards by avoiding potential data breaches and security incidents.

MDR Service Packages: Tailored Solutions to Meet Your Unique Needs

We offer three MDR service packages to suit your organization's specific requirements. Additional add-ons may be available to further enhance your cybersecurity posture depending on the licensed MDR service package.

Improve Operational Efficiency and Resilience

Whether your organization faces challenges related to skilled resource shortages or ever-growing threats or wants to improve its operations, HakTrak Managed Security Services can help. Our MDR service packages are designed to boost operational efficiency and increase resilience, ensuring your business remains protected against evolving cyber threats.

SOLUTIONS

Red Team

HakTrak Red Team Assessment: Strengthen Your Defenses with Real-World Cyberattack Simulations
Defend your digital ecosystem with our comprehensive Red Team Assessment. By simulating real-world cyberattacks, our professional team thoroughly tests your organization's information security, identifies weaknesses, and provides actionable recommendations to fortify your defenses.

Key Features of HakTrak Red Team Assessment

- **Real-World Cyberattack Simulations:** Our experienced Red Team simulates realistic cyberattacks on your organization, targeting your external perimeter and infiltrating your internal environment to uncover vulnerabilities.
- **Adversarial Methods and Open-Source Intelligence:** Utilize advanced techniques and open-source intelligence gathering to identify potential weak points in your information security.
- **Access, Privilege Escalation, and Data Exfiltration:** Follow the required procedures to access your internal systems, escalate privileges, and acquire sensitive data, mimicking the actions of an actual attacker.
- **Comprehensive Reporting:** Receive a thorough report on your security posture at the end of the assessment, detailing identified vulnerabilities and providing actionable recommendations to strengthen your defenses.
- **Mutually Agreed-Upon Objectives:** Work closely with our Red Team to define and achieve specific objectives, ensuring an unrivaled understanding of your security status

Benefits of HakTrak Red Team Assessment

- **Enhanced Cybersecurity:** Gain valuable insights into your organization's cybersecurity posture and identify areas for improvement, strengthening your overall defenses against cyber threats.
- **Proactive Security Testing:** Stay ahead of potential attackers by proactively identifying and addressing vulnerabilities before they can be exploited.
- **Informed Decision-Making:** Use the comprehensive assessment report to make informed decisions about your information security investments, optimizing resource allocation and maximizing ROI.
- **Regulatory Compliance:** Ensure your organization meets industry-specific security regulations and standards by identifying and addressing potential compliance gaps.
- **Increased Stakeholder Confidence:** Build trust with stakeholders, including customers, partners, and regulators, by demonstrating your organization's commitment to cybersecurity.

Cybercrime Investigation

HakTrak Cybercrime and Security Investigation: Uncovering, Analyzing, and Combating Cyber Threats
HakTrak's team of expert cybercrime investigators is dedicated to uncovering, analyzing, and recovering forensic data from the internet. With our state-of-the-art monitoring platforms and methodologies, we detect cyber threats and gather evidence globally, providing comprehensive security investigation services.

Crucial Services of HakTrak Cybercrime and Security Investigation

Unauthorized Access Investigation: Identify and investigate unauthorized access to your organization's systems, networks, and data, determining the extent of the breach and recommending appropriate response measures.

Malware Analysis: Analyze malicious software to understand its origin, functionality, and potential impact on your organization, enabling you to better defend against future threats.

Advanced Persistent Threats (APTs) Investigation: Investigate sophisticated and targeted cyberattacks, identifying the attackers' techniques, tactics, and procedures and recommending strategies to mitigate the risk.

Email Fraud and Phishing Attack Investigation:

- Examine email-based fraud and phishing attacks.
- Determine their source and intent.
- Recommend ways to improve your organization's email security.

Cyber Warfare & Supply Chain Attack Investigation: Investigate cyber warfare and supply chain attacks that target your organization and its partners, assessing the impact and providing recommendations to strengthen your defenses.

DDoS Detection and Response: Detect and respond to Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, minimizing their impact on your organization's operations and infrastructure.

Benefits of HakTrak Cybercrime and Security Investigation

- **Enhanced Cybersecurity:** Strengthen your organization's cybersecurity posture by proactively investigating and responding to cyber threats and incidents.
- **Reduced Risk:** Identify and address potential vulnerabilities and threats before they can be exploited, reducing the risk of cyberattacks and their potential impact on your organization.
- **Improved Compliance**: Ensure your organization meets industry-specific security regulations and standards by identifying and addressing potential compliance gaps.
- **Expert Support:** Benefit from the expertise of our seasoned cybercrime investigators, who utilize industry-standard tools and methodologies to uncover and analyze forensic data.