SINORITY

SINORITY

Company Profile | Product Catalogue

About Sinority

Sinority Co., Ltd. is a startup cyber security company based in Thailand. Our team of experienced professionals is dedicated to providing the highest quality cyber security solutions to businesses of all sizes. We have extensive experience in the industry and pride ourselves on our ability to stay up-to-date with the latest threats and trends.

> ***Secure your business, secure your future.***
>
> ***Sinority - we provide businesses with comprehensive cyber security solutions.***

Sinority Co., Ltd. is based in Bangkok, Thailand, with partners located in Kuala Lumpur, Malaysia and Singapore. Our strategic locations allow us to serve clients across Southeast Asia.

Founded in 2022

Sinority Co., Ltd. is a startup cyber security company in Thailand, with a strong track record of success and a loyal customer base.

Our Mission

At Sinority Co., Ltd., our mission is to empower businesses to protect their valuable data and networks from cyber threats.

Security and Technical Certifications

We have a team of highly skilled cyber security professionals who hold over 80 Security and Technical Certifications.

More than 80 Technical Staff Members

We have a team of over 80 highly skilled technical staff who are dedicated to providing the highest quality cyber security solutions to our clients.

SINORITY

Key Differentiators

"Our services help organizations to establish their Center of Excellence (CoE) in defending cyberattacks and improve their Cybersecurity maturity level"

People

- Security Awareness Training for Technical
- Security Awareness Training for Non-Technical Personnel
- Security Awareness Program

Process

- Cyber Security Maturity Assessment
- Information Security Risk Assessment
- Standard and Compliance Assessment
- Security Roadmap and Advisory

Technology

- Security Technology/Product Implementation
- Incident Response and Digital Forensic Services
- Managed Detection and Response Services

Identify

- Threat Intelligence
- Penetration Testing (Web/Mobile/Network)
- Source Code Review
- Red Teaming
- Compromise Assessment
- Breach and Attack Simulation (BAS)
- Managed CISO Office Services
- Security Configuration Review
- Cybersecurity Maturity/Posture Assessment
- Cybersecurity Risk Assessment
- Integrated Risk Management
- Enterprise Security Strategy & Roadmap
- Security Policy and Framework Development

Detect

- Managed Detection
- Managed Threat Hunting
- External SOC
- Enterprise Vulnerability Management Services

Protect

- Fraud Protection
- Digital Risk Protection (Brand)
- Business Email Protection
- Security Awareness Training (for Tech and non-Tech)
- Security Awareness Program
- Cybersecurity Risk Briefing for board
- DLP Business Consulting

Respond

- Managed Response
- Incident Response
- Incident Response Retainer
- Incident Response Readiness Assessment
- Digital forensics
- Cyber Investigation
- Cyber Drill/Table-top Exercise

Recover

- Business Continuity Management (BCM)
- IT Disaster Recovery Plan (IT DRP)

Attack Surface Management (ASM)

Managed Extended Detection and Response (MXDR)

SINQRITY

Our Technology and Partners

At Sinority Co., Ltd., we understand the importance of collaboration and partnering with industry leaders to provide the highest quality cyber security solutions to our clients. That's why we are proud to have strong partnerships with some of the most respected names in the industry, including Group-IB, Microsoft, Firmus, Cymulate, Archer, and Forcepoint.

GROUP-IB

FIRMUS

Cymulate

FORTINET

snyk

ARCHER

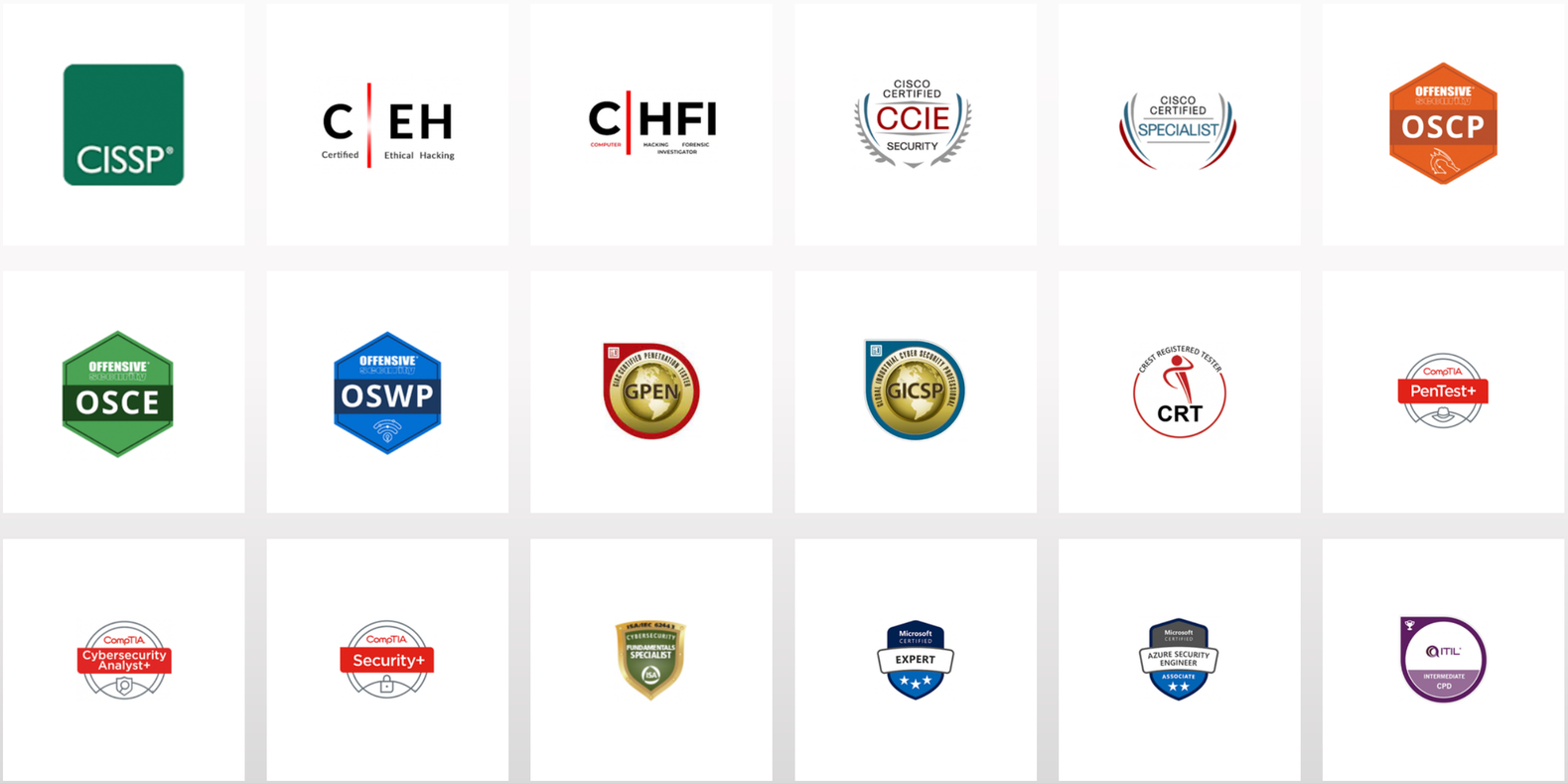
Forcepoint

Microsoft

Our Certificates

Sinority Co., Ltd. takes pride in our team of highly qualified cyber security professionals who hold over 80 technical and security certifications from reputable institutions around the world. Our team members have undergone rigorous training and have demonstrated their expertise in various areas of cyber security, including network security, cloud security, penetration testing, incident response, and more.

These certifications demonstrate our team's dedication to staying up-to-date with the latest trends, technologies, and best practices in the cyber security industry. Our clients can trust that our team members have the knowledge and skills needed to develop and implement effective cyber security solutions that protect their valuable assets.



Attack Surface Management

Discover your external attack surface with risk assessment capabilities which guides you to reduce the chance of getting breaches.

Real-time external asset discovery

Risk assessment with risk scoring

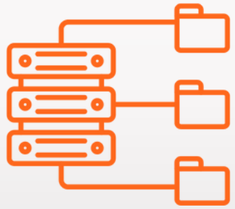
Detect flaws, misconfiguration, vulnerabilities and issues of your external attack surface

Detect leaked credentials and dark web mentions

SINQRITY

Threat Intelligence

In-depth knowledge of threat actor, their motivation and their technique to prevent attack and breaches to your organization.

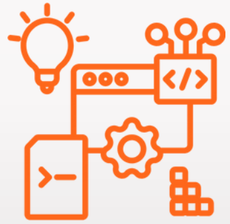


Comprehensive sources (human intelligence, data intelligence, open-source intelligence, malware intelligence, vulnerability intelligence and etc.)

Strategic intelligence and forecasts.

Tailored threat landscape and threat actor attribution.

Dark Web and compromise data detections



Comprehensive Integration

Penetration Testing

Check and verify your Web/Mobile Application and Infrastructure security.

Penetration testing is a critical component of any effective cyber security strategy, and at Sinority Co., Ltd., we understand its importance. Our team of experienced professionals includes certified penetration testers have a deep understanding of the latest testing methodologies and tools.

Web/Mobile Application Penetration Testing follow OWASP

Network and wireless Penetration Testing

Our team of experienced cybersecurity professionals will perform a thorough Penetration Testing to identify potential vulnerabilities and security gaps in your organization's systems and applications. This will allow us to provide recommendations on how to remediate any identified security issues and improve your overall security posture.

Source Code Review

Review your application source code for identifying security and business logic flaws.

Identify and solve security vulnerabilities before going to production.

Identify business logic flaws in your source code.

Combination of manual and automated review.

SINQRITY

Red Teaming

Challenge your cybersecurity team by leveraging threat intelligence insights and test your team's abilities in order to evaluate detection and response capabilities.

Simulate real-world hacker/attacker techniques and scenarios.

Identify weaknesses in your defenses that may not have been identified through traditional security assessments.

Gain insight on people, process and technology against real-world hacker/attacker.

Evaluate your detection and response capabilities.

SINQRITY

Compromise Assessment

Determine whether your systems or networks have already been breached or compromised by cybercriminals. By analyzing the existing network traffic and endpoint data, a compromise assessment can identify potential indicators of compromise (IOCs) and provide insights into the overall security posture of the organization.

At Sinority Co., Ltd., we strongly recommend that our clients undergo a compromise assessment to identify potential security breaches. In today's rapidly evolving cyber threat landscape, it is crucial for organizations to remain vigilant and proactive in protecting their assets.

A compromise assessment can help organizations identify breaches or security incidents that may have gone undetected for a long time. It can provide valuable insights into how an attacker gained entry, what data or systems were targeted, and what steps can be taken to mitigate the impact of the attack.

Confirm if your organization has been breached or hacked.

Detect traces of attack preparation and compromise within your IT infrastructure.

Assess the scale of damage and determine which assets in the network were attacked and how it occurred.

Breach and Attack Simulation (BAS)

Identify different vulnerabilities in security environments by simulating the attack paths and techniques likely to be used by malicious actors.

- Automated test and validate your security control across full cyber kill chain (WAF, Firewall, Endpoint, Email Security, SOC and etc.)
- Lightweight deployment in your environment with unlimited attack simulations.
- Get results faster than traditional security validation

Managed CISO Office Services (MCO)

We provide support and assistance to the Organizational CISO and Team through a set of pre-determined and discussed responsibilities.

- Maintaining the IT Security posture and IT security governance-related activities for your organization
- Provide cybersecurity advisory for your organization

Sinority's MCO services provide a comprehensive, cost-effective solution for organizations that need expert cyber security guidance but do not have the resources to maintain a full-time CISO.

Our MCO services provide access to our experienced CISO professionals, who can provide ongoing guidance and support to help our clients develop and implement effective cyber security strategies. We work closely with our clients to understand their business objectives and risk management goals, and provide customized solutions that meet their unique needs.

SINORITY

Security Configuration Reviews

Sinority provides Security Configuration Reviews by adopting standard/product best practices and (CIS) benchmark.

Our security configuration review services are designed to help our clients identify and address potential security vulnerabilities before they can be exploited by cyber attackers. By working with our experienced professionals, our clients can rest assured that their systems and networks are properly configured and secured.

Identify flaws and gaps using standard/product best practices to optimize and secure your configurations.

Make actionable recommendations on how you could improve your configuration to match with standard/product best practices and CIS baseline.

SINORITY

Cyber Security Maturity / Posture Assessment

Identify your organization security posture and maturity levels and compare against others peer in your business sector.

Identify current security maturity levels by adopting NIST CSF

Compare your current security maturity levels with peer in same industry.

Gain roadmap for your organization to improve security maturity levels

SINQRITY

Cyber Security Risk Assessment

Establish Cybersecurity Risk Assessment methodology and framework for your organizations.

Establish Cybersecurity Risk Assessment methodology and framework for your organization.

Assist you to perform risk assessment along with business impact analysis (BIA).

SINQRITY

Integrated Risk Management

At Sinority Co., Ltd., we offer an integrated risk management solution that provides our clients with a centralized risk management dashboard. Our solution is designed to help our clients streamline their risk management process and make informed decisions based on real-time risk information.

By using our integrated risk management solution, our clients can streamline their risk management process, improve their decision-making, and reduce the risk of cyber attacks and other security incidents. Our experienced professionals use advanced tools and techniques to provide our clients with a comprehensive risk management solution that meets their unique needs.

Our solution allows your business to focus on the risks that are truly important and to assign responsibility of specific risk management activities to individuals.

It breaks down silos between entities, professional functions and disparate risk evaluation tools so that risk can be managed in a holistic, efficient and collaborative manner.

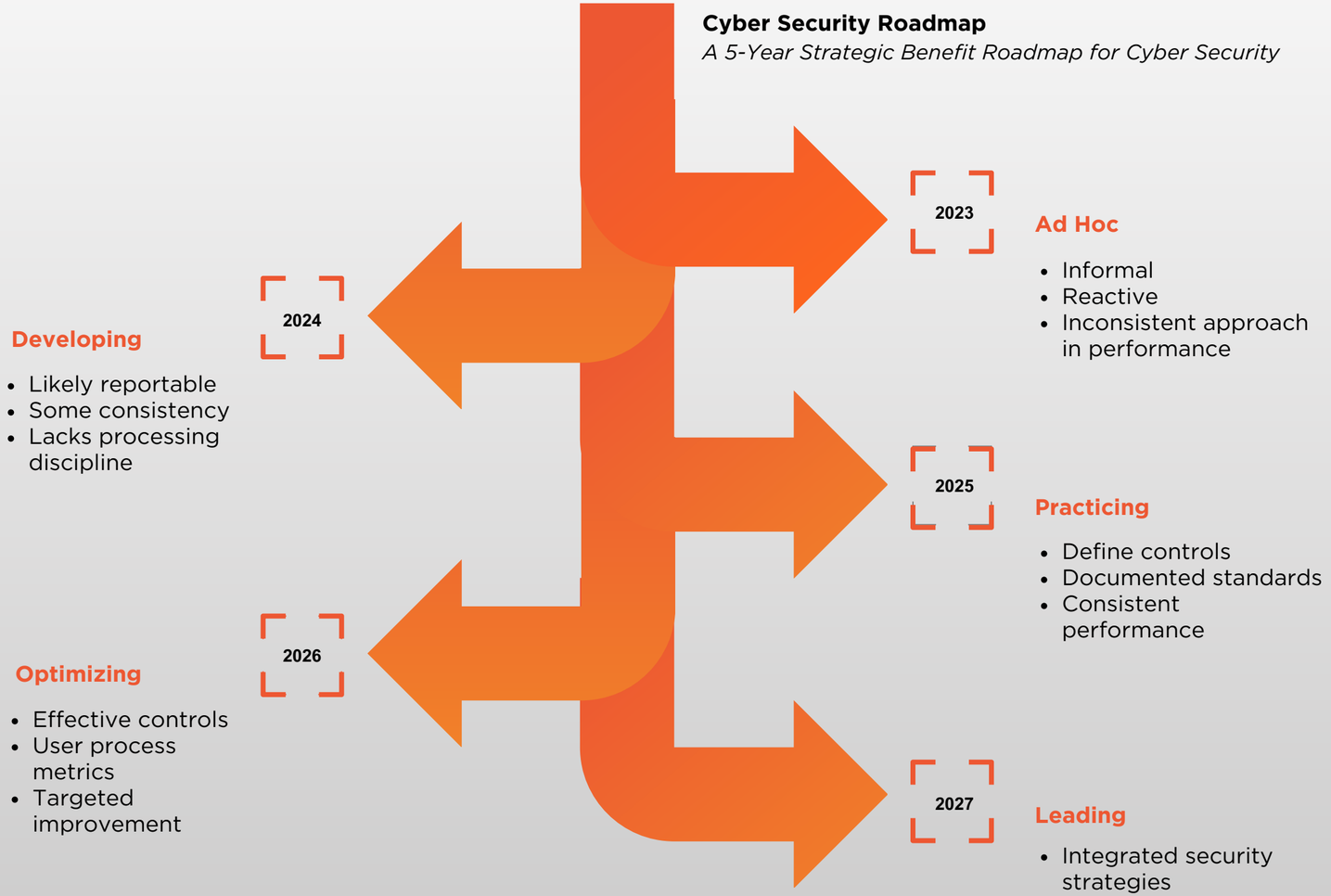
Provides defensible and actionable risk intelligence to risk managers and business decision makers

Enterprise Security Strategy and Roadmap

Defines and prioritizes information assurance and security initiatives that the organization must commence to enhance the protection of information and related technology.

- Assess existing cyber security strategy, plan, or roadmap.
- Develop/update cyber security roadmap.

An effective security planning is essential for any organization's long-term success. That's why we offer a comprehensive five-year enterprise security strategy and roadmap service to help our clients identify their security needs and develop a plan to address them.



Security Policy and Framework Development

Sinority will establish and strengthen your security policy and framework.

Review

Review existing Security Governance and Processes.

Identify

Identify gap of existing security policies, guidelines, procedures and etc.

Develop

Develop/Improve security policies, guidelines and procedures for your organization.

SINORITY

Managed Extended Detection and Response

Identify threats in real time to enable immediate response actions by centralizing, correlation, and analyzing the data generated from various tools deployed in your environment.

Get complete visibility over your security operations, including endpoints, servers, cloud workloads, emails, and networks.

Automate routine tasks to free up resources so SOC personnel can respond to the threats that need to be addressed.

We use advanced threat detection technologies and techniques to identify and analyze potential threats in real-time.

Our MXDR service leverages cutting-edge technologies such as machine learning, behavioral analysis, and threat intelligence to identify threats across your entire network.

In the event of a security incident, our MXDR service provides rapid and effective incident response to minimize the impact of the incident.

SINQRITY

External SOC

Leverage SIEM managed by our external SOC team. SIEM (Security Information and Event Management) is a security management solution that provides real-time monitoring, detection, and response to security threats in cloud environments. It aggregates data from various sources, including logs, alerts, and events, and analyzes that data to detect and respond to potential security threats.

Leverage both cloud-SIEM and on-premises such as Azure sentinel and FortiSIEM

Collect logging and analyze log with our external SOC.

Develop use-cases and playbook specifics for your organization.

Enterprise Vulnerabilities Management Services

Establish vulnerability management lifecycle for your organizations.

Enterprise Vulnerability Management Services (EVMS) is a proactive approach to identifying and mitigating vulnerabilities in an organization's IT systems and infrastructure. EVMS involves a continuous process of identifying, prioritizing, and remedying vulnerabilities to minimize the risk of a security breach.

- Analyze vulnerability scanning report and prioritize remediation actions.
- Suggest mitigations, improvements and additional control.
- Weekly Remediation and Tracking Meeting.
- Monthly executive summary report and analysis.

SINQRITY

Fraud Protection

Eliminate fraud across all digital channels in real time.

Fraud protection refers to measures taken by individuals, organizations, and institutions to prevent and detect fraudulent activities. Fraud can take many forms, such as identity theft, credit card fraud, insurance fraud, and investment fraud, among others.

Fraud protection measures typically include a combination of preventative and detective controls. Preventative controls aim to stop fraud from occurring in the first place, while detective controls are designed to identify fraud after it has occurred.

Protect your business from various types of digital fraud: malware, SIM swap, bad bots, web scraper, account takeover, social engineering fraud, and many more.

Cross-channels correlation to make sure that both your web and mobile channels are protected.

Leverage our Preventive Proxy anti-bot technology to analyze the user sessions, and detect automated tools to respond to malicious bot activity.

Protection from an extensive range of cyber threats targeting specific industries (scam calls, phishing, 3DS protection for banking, account takeover, web scraping, etc.).

SINQRITY

Digital Risk Protection (Brand Protection)

Defend your digital assets with AI-powered brand protection online solutions.

Automated neural-based detection system and all-in-one brand protection platform for business and analysts.

Intuitive and easy-to access dashboards, detailed reports and clear takedown processes.

Actor-centric approach to investigating, researching and predicting scammers' behavior and tool development for improving detection and takedowns.

Incident response: Responding to incidents in a timely and effective manner, including investigation, containment, and remediation.

SINQRITY

Business Email Protection

Block advanced email threats and secure corporate email on-premises and in the cloud from the most sophisticated attacks.

Inspect over 290 different file formats to ensure all attachments are safe. Check all links, including obfuscated and redirected links.

Recursively analyze suspicious URLs, attachments, and objects that can change state over time to discover hidden threats that other solutions miss.

Use a customizable detonation platform for payload detonation.

Anti-phishing protection: Protection against phishing attacks that attempt to trick users into divulging sensitive information, such as passwords or financial information.

SINQRITY

Security Awareness Training

We provide Security Awareness training for both technical and non-technical personnel. Security Awareness training is an essential component of a comprehensive cybersecurity program. It helps employees understand the risks and threats associated with using company technology and provides them with the knowledge and skills needed to identify and respond to potential security threats.

By offering Security Awareness training for both technical and non-technical personnel, Sinority can improve the overall security posture of their organization. This can help reduce the risk of human error-related security incidents, such as phishing attacks or accidental data breaches, and protect sensitive company information.

Interactive cybersecurity awareness training for employees.

Learn about attackers' technology, instruments, and goals, as well as fraud schemes and targeted attacks that involve social engineering and malware.

Customizable course outlines to meet your organizational requirements.

Mobile device security: Educating employees on best practices for securing mobile devices, including setting up passcodes, encrypting data, and avoiding public Wi-Fi.

SINORITY

Cybersecurity Risk Briefing For Management

Security Risk awareness and briefing for Board of Directors (BOD), Senior management and top management. A Cybersecurity Risk Briefing for management is an overview of the current cybersecurity risks facing an organization. It is designed to provide decision-makers with a clear understanding of the potential risks to the organization's data, systems, and operations, as well as the potential impact of those risks.

Focus on business and enterprise risk for top management personal.

Learn about attackers' technology, instruments, and goals, as well as fraud schemes and targeted attacks that involve social engineering and malware.

Address the requirements of your BOD, senior and top management, to acquaint them with current cybersecurity trends and provide them knowledge to decide on measures to best protect your organization.

SINQRITY

Data Loss Prevention (DLP) Consulting

Establish and develop a Data Loss Prevention (DLP) Program that aligns with your business. Data Loss Prevention (DLP) is an important aspect of cybersecurity, and at Sinority, we provide comprehensive DLP services to our clients. DLP involves implementing security controls and policies that prevent sensitive data from being lost, stolen, or accessed by unauthorized individuals.

- DLP policy development: We develop customized DLP policies for our clients based on their unique requirements and industry regulations.
- Data classification: We work with our clients to classify their data based on its sensitivity and importance. This enables us to develop more targeted DLP policies and controls.
- Provide DLP business consultancy to help implement DLP program.
- Assess existing DLP solution implementation or overall program.

By providing comprehensive DLP services, we help our clients protect their sensitive data and comply with industry regulations. Our goal is to help our clients maintain the confidentiality, integrity, and availability of their data, and minimize the risk of data loss or theft.

SINORITY

Incident Response

Quickly stop and investigate hacker attacks, understand how cybercriminals penetrate a company’s network, and prevent them from stealing money and valuable data.

Incident response is the process of detecting, analyzing, and responding to cybersecurity incidents in a timely and effective manner. Our Incident Response services help our clients to minimize the impact of security incidents and ensure business continuity.

- Proper incident response to clearly understand the scope and develop appropriate measures to effectively contain the threat and prevent any additional damage.

- Clear understanding of the incident based on proper digital forensics examination and malware analysis allows you to develop efficient strategy for remediation and recovery.

- Reconstructed attack lifecycle provides you clarity on weaknesses of the affected systems

  Our Incident Response services are designed to help our clients respond quickly and effectively to cybersecurity incidents, minimizing the damage caused by the incident and ensuring business continuity.

SINQRITY

Incident Response Retainer

Pre-negotiated statement of work provided with synergy of proactive and reactive services related to a security incident.

An Incident Response Retainer is a pre-paid agreement that provides access to our Incident Response services in the event of a cybersecurity incident.

By signing up for an Incident Response Retainer, our clients can ensure that they have a dedicated team of cybersecurity professionals available to respond to incidents quickly and effectively. The retainer provides priority access to our incident response services, allowing our clients to respond to cybersecurity incidents in a timely and efficient manner.

Signed SLAs to guarantee timely service and 24/7 emergency response.

Human expertise, rich data sources and unique technologies to stop the attacker and restore infrastructure in time.

Flexible terms of the Retainer and discounted rate for additional consulting services.

A variety of proactive, reactive and educational services for repurposing prepaid hours.

SINQRITY

Incident Response Readiness Assessment

Evaluate your IR team and prepare for quick and effective response. Our team of experienced cybersecurity professionals will perform a thorough assessment of your organization's incident response plan, processes, and procedures. We will evaluate your organization's ability to detect, contain, and respond to a cyber incident in a timely and effective manner.

Integrated assessment of key elements — technology, team, processes & documents.

Leading practices overview leveraged to build and enhance your incident response plan.

Actionable recommendations and roadmap to implement identified improvement opportunities.

Organizations can assess their resource allocation for incident response, ensuring they have the necessary tools to respond to incidents.

SINQRITY

Digital Forensics

Ensure that information for forensic examinations, initiated independently or by law enforcement agencies, is correctly seized and copied.

At Sinority, we provide digital forensics services that help clients investigate and recover from cyber attacks. Our experienced team of digital forensics professionals uses state-of-the-art tools and techniques to uncover evidence, identify the root cause of the incident, and help clients take corrective action. Our digital forensics services include data acquisition, data analysis, evidence preservation, and forensic reporting. We work closely with our clients to ensure that they have a comprehensive understanding of the incident and the steps that need to be taken to prevent future incidents.

Extract the maximum amount of useful information from objects under examination and interpret the collected evidence accurately and comprehensively.

Guarantee the opinions of our forensic specialists will be accepted by courts as adequate evidence for civil, administrative, and criminal proceedings.

All examinations are conducted within the time limits specified when the materials are submitted for analysis.

SINORITY

Cyber Investigation

Conduct cyber security investigations to bring threat actors and cybercrime to justice.

As a cyber security company, Sinority provides cyber investigation services to help clients identify, analyze, and respond to cyber incidents. This may include conducting forensic analysis of digital devices, examining network traffic logs, and reviewing system and application logs to identify the root cause of the incident.

Our team of experienced cyber investigators can work closely with clients to understand the scope of the incident and develop a comprehensive investigation plan that includes collection of evidence, analysis of data, and identification of potential threats and vulnerabilities. We can also provide expert witness testimony and support during legal proceedings related to the cyber incident.

Explore the anatomy of the attack and threat actor's infrastructure, identify the mechanisms and recreate the sequence of events.

Collect all digital evidence in compliance with legal requirements and prepare required documentation for presenting evidence correctly in court.

Provide guidance on how to improve cyber security posture and prevent future incidents through implementation of best practices and recommended security controls.

All examinations are conducted within the time limits specified when the materials are submitted for analysis.

SINORITY

Cyber Drills / Table-Top Exercises

Conduct Cyber drills/Table-top exercises for your organization. These exercises can be tailored to the specific needs and concerns of each client, and can simulate realistic scenarios to test their incident response plans and identify potential gaps in their security posture.

Our team of experienced cyber security professionals can work closely with clients to develop custom scenarios that reflect their unique environment and potential threats. We can then facilitate the exercise and provide feedback on areas that need improvement or refinement.

Familiarize your organization's staff and executives with cyber drill and table-top exercise.

Tailored made scenarios to match with your threat landscape.

Leverages threat intelligence to develop scenarios for your organization.

Improve incident response capabilities, increase resilience to cyber attacks, and enhance overall awareness and preparedness for cyber threats.

SINQRITY

Business Continuity Management (BCM)

Establish a Business Continuity Plan (BCP) for your organization to help prepare for and respond to disruptions to your business operations caused by cyber attacks, natural disasters, or other unexpected events.

Our BCM services are designed to help our clients minimize the impact of disruptions on their operations and ensure they can continue to deliver critical services to their customers even in the face of unexpected events.

We also provide training and awareness programs to help clients build a culture of resilience, ensuring that employees are aware of their roles and responsibilities during a disruption and can respond effectively to minimize the impact on the business.

Assess existing business processes, IT system and Business Impact Analysis (BIA).

Design and develop BCP program in conformance to ISO 22301 or regulatory requirements.

Test, run, evaluate and validate your Business Continuity Plan (BCP).

SINORITY

IT Disaster Recovery Plan (IT DRP)

Establish an IT Disaster Recovery Plan (IT DRP) for your organization. An IT DRP is a crucial element of any organization's business continuity strategy. It outlines the steps to be taken in the event of an IT system failure or disruption, such as a natural disaster, cyber-attack, or hardware malfunction. The plan provides a roadmap for restoring critical business operations and minimizing the impact of the disruption on the organization's productivity and reputation.

Assess existing business processes, IT system and Business Impact Analysis (BIA).

Design and develop IT DRP in conformance to ISO 22301 or regulatory requirements.

Help you test your IT Disaster Recovery Plan (IT DRP).

SINQRITY

SINORITY

Sinority Co., Ltd.

88/14 Thetsaban Songkhro Road
Khwaeng Lat Yao, Khet Chatuchak
Bangkok 10900

Phone: 089 391 5956
Email: sales@sinority.com

sinority.com