Shanghai Guan An Information Technology Co., Ltd.

CONTENTS

Company Profile 01

GUANAN Security Information & Event Management System 03

GUANAN Database Security Audit System 04

GUANAN Distributed Deception System 05

GUANAN Web Application Security System 06

GUANAN Endpoint Detection and Response System 07

GUANAN Vulnerability Scanning System 08

GUANAN Next Generation Firewall System 09

GUANAN Intrusion Prevention System 10

GUANAN Security Services 11

Company Profile

Guan An Info. is a company that provides big data + pan-security products and services. It focuses on the core directions of data security, cyber security, 5G security, AI security, industrial Internet security and public security, and provides comprehensive information security solutions for telecom operators, governments, finance, electric power, public security, health care and other industry users .

The company has established headquarters in Shanghai, Beijing and Shenzhen, as well as multiple laboratories.It is the only certified information security training base in China by United Nations Institute for Training and Research (UNITAR) / Shanghai International Training Center (CIFAL) and a member of the expert group of the UNIDO Shanghai International Intelligent Manufacturing Promotion Center. It is recognized as a Technical Support Unit for Cybersecurity Defense of Major National Events, Little Giant Enterprises of Specialization, Refinement, Differentiation and Innovation certified by MIIT , 5G Start-Up and Shanghai High-tech Enterprises.

Business Direction

Competencies

The core team of Guan An has more than 20 years of professional technical experience in information security and more than 10 years of experience in big data analysis. In domestic and foreign cyber security technology competitions, we' ve won many gold awards.

20+	15+	10+	8+	8+	200+	800+
Experience 20 years+	Service 15 years+	Big Data 10 years+	Data Security 8 years+	Laboratories 8+	Intellectual Property 200+	R&D staff 800+

Key technologies & Qualifications

The company has professional qualifications for product development and services in the field of cyber security and big data, and obtained a number of international and domestic professional system and technology certifications such as ISO9000, ISO20000, ISO27001, ISO14001, ISO45001, CMMI-DEV, CCRC, CNITSEC, CESSCN, CNCERT, and many products have obtained IPv6 Ready Logo international certification.

90+
Trademarks

130+
Software copyright

30+
Product Sales Licenses

80+
Patent for invention

Social Responsibility

Guan An has been continually carrying out technological innovation with the vision of “Assisting China's Big Data +”, focusing on the cyber security personnel training, responding to the national initiative of “The Belt and Road” to promote national cyberspace security construction and international cybersecurity. Exchange and cooperation; actively undertake social responsibilities, promote charity, help target poverty alleviationand spread the positive energy of society.

United Nations Institute for Training and Research (UNITAR)/ Shanghai International Training Center (CIFAL) - Big Data Application and Security Training Base

Cyber Security Skills Competition

Popular Science Comic Growth story of Guanzai

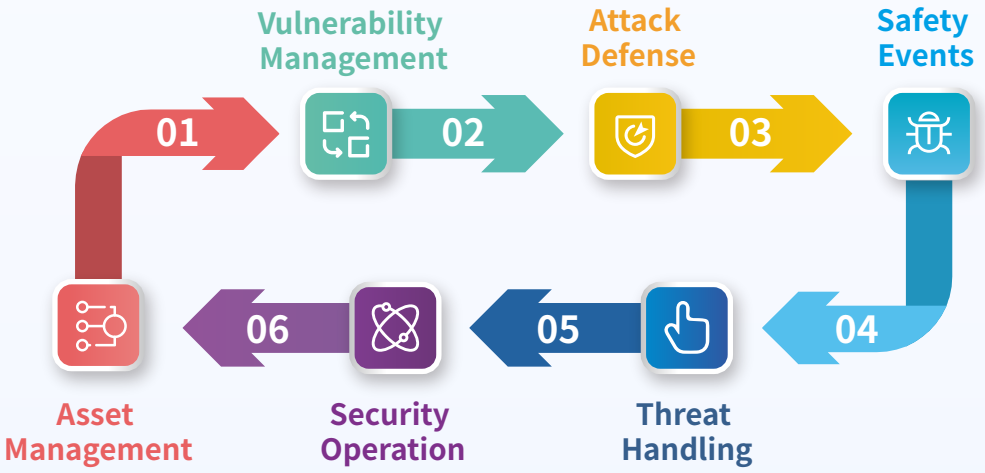
Cyber Security Enters Campus

Social Welfare Activities

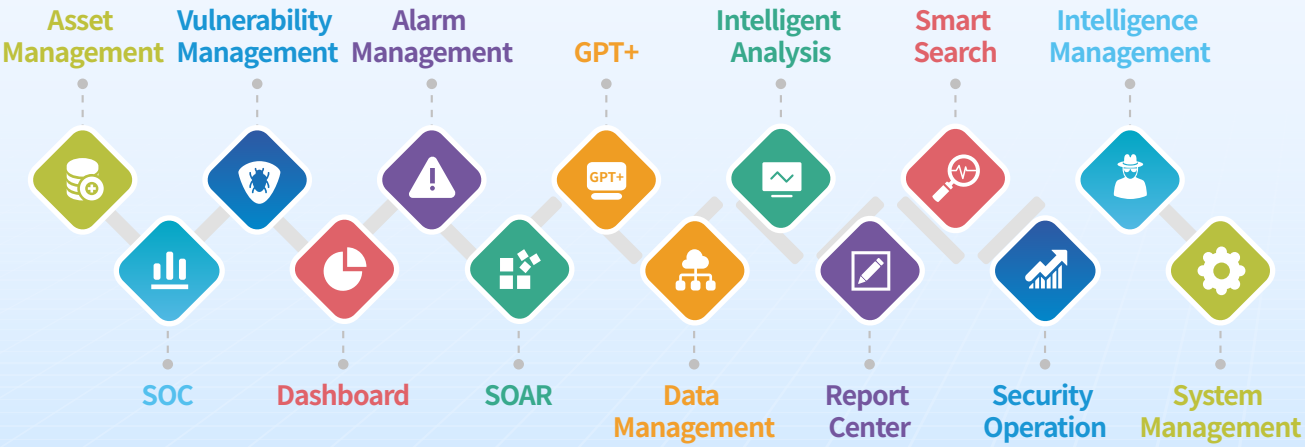
GUANAN Security Information & Event Management System

GUANAN Security Information & Event Management System collects network traffic and log data, and applies data modeling, behavior identification, correlation analysis, artificial intelligence and other methods to analyze a huge amount of heterogeneous security data. It allows SIEM analysis from the perspective of assets, vulnerabilities, alarms and events, and generate large screen display of comprehensive security situation. It helps foster an enterprise network security environment featuring "well-organized data governance, abundant threat analysis scenarios, perfect security warning system, efficient response to security events, and orderly security operation management" The product has been widely used in operators and state-owned enterprises in finance, electricity and other industries.

Perception Chain



Functional Matrix



GUANAN
Database Security Audit System

GUANAN Database Security Audit System is a security audit product which can monitor database activities in real time. The system can help enterprise operation specialists to monitor, analyze and trace database operation behaviors. The system can alarm illegal operations on time and reduce the loss of the database as well. The Database Security Audit System presents database-oriented interface language, intelligent protocol recognition, visual operation status, interactive and drillable risk tracking ability. The system is one new generation of database audit product to perfectly achieve enterprise expectations without implementation, training and maintenance.

Product Value

Comprehensive Business Audit

Covers all database types and enables precise auditing of operational behaviors across diverse environments, ensuring end-to-end visibility into business-related database activities.

Holistic Sensitive Data Protection

Intelligent identification of sensitive data, built-in proprietary strategy for access to sensitive data, reduce the risk of leakage

Real-Time Risk Alerting

Monitors and alerts on risky activities effectively, enabling immediate coordination with security management teams for proactive threat response.

Compliance Assurance

Ensures alignment with regulations, facilitating smooth compliance audits and regulatory adherence for enterprises.

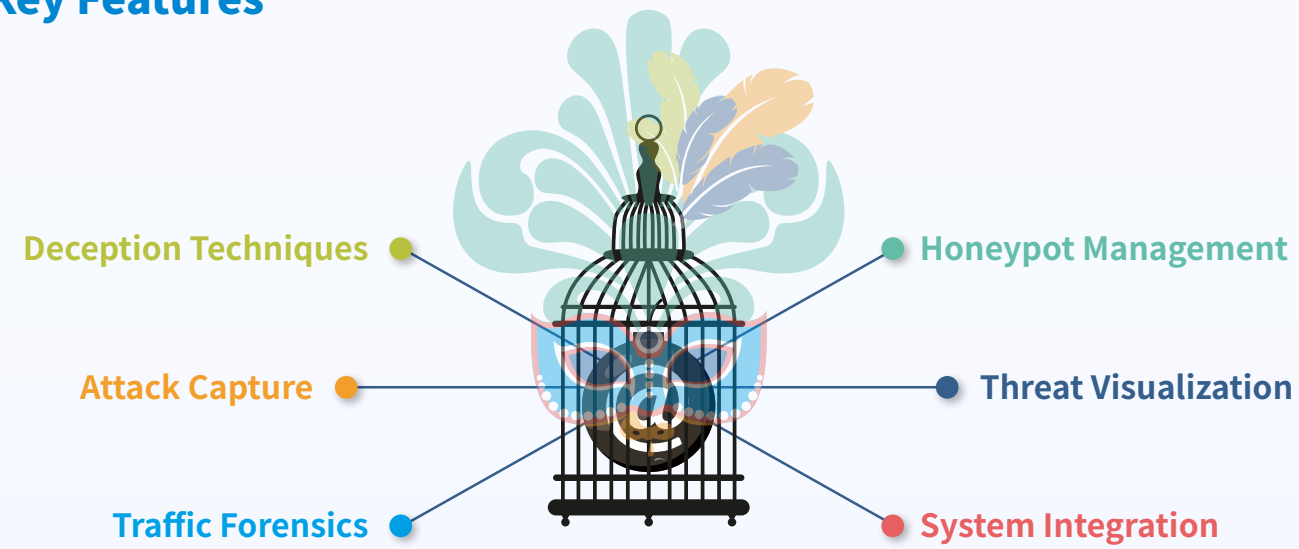
Main advantages

- Big Data-Powered Log Management
- Automated Sensitive Data Identification & Classification
- Clue-Driven Forensic Tracing
- Customizable Multi-Dimen-sional Analytics
- Proactive Rule-Based Protection

GUANAN
Distributed Deception System

As a network security product, GUANAN Distributed Deception System is built with the aim of improving enterprise network security capacity. It relies on deception technologies and empowers customers in threat trapping and perception. By deploying decoys in advance to distract attackers and luring them to visit and attack decoys, it perceives and captures attack behaviors followed by traceability and countermeasures, signaling a breakthrough from the traditional offensive and defensive imbalance.

Key Features



Application Scenarios

Ransomware & Mining Detection

Deploying GUANAN Distributed Deception System on the intranet can detect intranet attack behaviors, including worm propagation, ransomware spread, and mining software dissemination, immediately pinpointing the sources to eliminate security risks.

Intranet Intrusion Detection

Attackers penetrate the intranet using various tactics, leveraging internal programs as jump servers for reconnaissance and attacks. GUANAN Distributed Deception System sets up traps to identify abnormal behaviors, enhancing intranet threat awareness capability and seizing control of security initiatives.

Threat Defense Collaboration

As a crucial intranet security intelligence source, GUANAN Distributed Deception System synchronizes captured events to SOC or other SIEM platforms, coordinating with other security systems to form a cohesive defense mechanism, solidifying intranet security.

GUANAN Web Application Security System

GUANAN Web Application Security System is a new WAAP application that relies on dynamic defense technologies to protect against automated machine behaviors. Instead of passive defense, it pro-actively carries out dynamic obfuscation or encryption of request content, and token authentication. It can hide vulnerabilities & codes, and defend automated attacks without resorting to rules, thresholds or signatures, covering typical defense scenarios including crawlers, tool scanning, vulnerability detection and data traversal. By detecting and discovering attacks and threats, the system serves as the guardian of enterprise application security.

Key Advantages

Application Scenarios

Defense Against Malicious Crawler

Implement proactive defense to validate requests dynamically without relying on predefined patterns, effectively intercept automated web crawlers, and safeguard information from malicious web scraping across social media, e-commerce, public administration, telecoms, mapping services, and self-media platforms.

Defense Against Automated 0-DAY Vulnerability Detection

Leverage data packets to perform dynamic obfuscation and legitimacy checks, fundamentally defend against unknown vulnerabilities, and prevent attackers from exploiting new vulnerabilities for automated probing and attacks.

Defense Against Web Application Attacks

Employ proactive defense and semantic analysis techniques to validate requests dynamically and conduct syntax and lexical analysis, providing comprehensive protection against traditional web application threats like SQL injection and cross-site scripting (XSS).

Defense Against API Data Leakage

Multiple engines protect APIs encompassing API request protocol security, API transmission parameter security, API application security, and API data security. This full-lifecycle coverage eliminates security issues caused by API malicious attacks and sensitive information leakage.

GUANAN Endpoint Detection and Response System

GUANAN Endpoint Detection and Response System supports multiple cloud platforms and server architectures, and is easy to deploy. The product is delivered in the form of software, with simple configuration and operation, and high monitoring accuracy. The product provides enterprise operation and maintenance and security management personnel with the ability to manage a large number of servers security, reducing operation and maintenance costs, and greatly improving the enterprise's security protection capabilities under the background of lower security expertise.

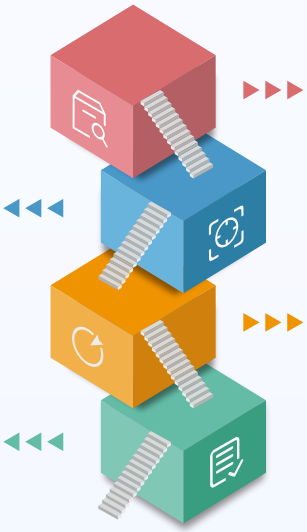
Key Features

Risk Detection

This feature empowers users to accurately identify internal risks, assisting security teams in quickly locating issues and formulating solutions. It provides detailed asset and risk information for in-depth analysis and response, ensuring proactive threat mitigation.

Intrusion Detection

Delivers multi-anchor detection capabilities to real-time and accurately sense intrusion events, identify compromised hosts, and provide actionable response measures—ensuring rapid threat containment and network resilience.



Asset Inventory

Offers precise business-layer asset identification and dynamic awareness. With an A/S architecture, it supports inventory and recognition of over 10 types of hosts and 800+ business applications, enabling comprehensive visibility into IT assets.

Compliance Baseline

Adheres to China's Information Security Level Protection (ISLP) requirements and CIS (Center for Internet Security) Benchmarks, supporting multiple versions of operating systems, web applications, databases, and other business environments to ensure regulatory alignment.

Scenarios

Host Security Protection

Identifies system/application vulnerabilities, EXP/POCs, and emerging threats through Agent-based continuous monitoring and analysis, cross-referencing with a comprehensive vulnerability database for precise and efficient detection.

Advanced Vulnerability Detection

Offers multiple response mechanisms—including auto-blocking, manual isolation, black/white lists, and custom workflows—to empower users to effectively resolve intrusion incidents at their core, ensuring rapid threat containment.

ISLP Compliance Audit

Establishes a security baseline for host systems, conducting tailored compliance checks across different environments. It provides a standardized technical framework to identify non-compliant configurations, enhance security measures, and mitigate risks in alignment with regulatory requirements.

GUANAN Vulnerability Scanning System

As the leading enterprise-level vulnerability management system in China that is comprehensive, accurate and accessible, GUANAN Vulnerability Scanning System helps detect all kinds of vulnerability risks in the network, provides professional and effective security analysis and patching recommendations, reviews patching effect according to the security management process, minimizing the attack surface and losses.

Key Features

Service Discovery

Identifies services running on active network devices and their details, ensuring visibility into operational infrastructure.

Asset Discovery

Detects active assets on the network, enabling comprehensive visibility into connected resources.

Vulnerability Assessment

Scans active assets to identify and assess vulnerabilities, providing insights for risk mitigation and patch prioritization.

Asset Inventory

Scans active assets to determine configurations—including OS, hardware, services, and installed software—for detailed asset management.

Advantages

High-Performance & Stability

Leveraging multicore processing and multithreaded architecture, it handles up to 100,000 transactions/sec. Distributed deployment and parallel processing ensure future-proof scalability for evolving needs.

Massive Storage & Query

Utilizes space-efficient compression to reduce storage costs while enabling sub-second query response for trillions of structured/unstructured data—boosting operational efficiency through rapid data retrieval.

Comprehensive Data Visualization

Intuitive dashboards offer real-time security awareness while an automated reporting system generates tailored industry-standard reports-addressing both holistic security monitoring and operational analytics needs.

Advanced Intelligent Analysis

Harnesses big data and machine learning to integrate, correlate, and predict insights from multi-dimensional, multi-source data-empowering security teams with precise threat detection and investigative support.

Modular Scalability & Compatibility

Built on a dynamic modular architecture, it supports seamless expansion and integrates with mainstream security devices via proprietary protocol parsing. Rich APIs enable easy third-party system integration for customized workflows.

GUANAN Next Generation Firewall System

GUANAN Next Generation Firewall System contains various authentication methods and enables multi-dimensional and elaborate control based on application, content and assets, which can guard against network threats including DoS/DDoS attacks, violence cracking, weak passwords, vulnerability exploitation, viruses, Trojan horses, and ensure authority and security of intranet resource access. It brings cost-effective, efficient and integrated security protection experience to customers in various industries and strongly supports enterprises in building three-dimensional network security protection.

Functional Specifications

Basic Network Functions

- Support transparent, routing, and hybrid modes, and link aggregation;
- Facilitate source NAT, destination NAT, port NAT, and static NAT;
- Enable VLAN and VRF;
- Integrate WLAN and 3G wireless access;
- Provide static routing, policy-based routing, ISP routing, and source interface routing;
- Incorporate dynamic routing protocols OSPF, RIP, and OSPFv3;
- Deploy routing detection function;
- Support IPv6 static routing, router advertisement, and tunnel conversion.

Firewall Capabilities

- Deliver eight-element integration strategy based on users;
- applications, source/destination interfaces, IP addresses, services, and time;
- Facilitate resource management for addresses, services, schedules, applications, and users;
- Allow adjustment of policy priorities;
- Include IPv6 security policies.

Security Protection

- Offer IP-MAC binding, ARP spoofing protection, and ARP Flood attack defense;
- Guard against IPv4 anomaly packet attacks such as Ping of Death, Land-Base, Tear Drop, TCP Flag Winnuke, Smurf, Jolt2.;
- Protect against port scanning and IP scanning;
- Safeguard against SYN Flood, UDP Flood, ICMP Flood, DNS Flood attacks based on interfaces and IPs;
- Defend against IPv6 anomaly packet attacks like Winnuke, Land-Base, TCP Flag, Fraggle, IP Spoof, etc.

VPN Characteristics

- Support various IPSecVPN protocols and deployment methods;
- Provide policy- and route-based IPSecVPN;
- Integrate CA centers and X.509 certificate formats;
- Offer VPN Track;
- Support SSL VPN tunnel mode;
- Incorporate GRE VPN;
- Ensure security protection and bandwidth management under VPN tunnels.

Traffic Management

- Implement multi-tier nested bandwidth management based on channels, interfaces, users, and applications;
- Approve bandwidth priority management;
- Enforce maximum bandwidth limits, minimum bandwidth guarantees, and elastic bandwidth;
- Offer per-IP rate limiting;
- Support exclusion policies.

Intrusion Detection and Prevention

- Automate protocol identification;
- Contain 3,000+ predefined attack signatures;
- Offer automatic and manual updates to the signature database;
- Shield against worms, Trojans, phishing, and more.

User Management

- Support local firewall user authentication;
- Integrate standard Radius, LDAP, and third-party user authentication;
- Provide Portal user authentication;
- Enable online user monitoring and timeout management;
- Facilitate centralized user policy management.

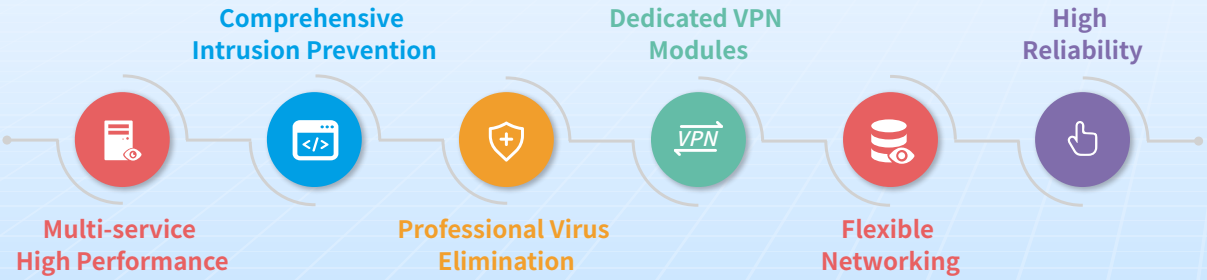
Anti-Virus Protection

- Filter viruses via HTTP, FTP, SMTP, POP3, IMAP protocols;
- Block specific file types from passing through;
- Scan compressed files up to 20 levels deep;
- Support manual and automatic virus database updates;
- Incorporate malicious URL filtering.

Visualization

- Display real-time device health statistics on CPU, memory, and interface traffic;
- Visualize user and application traffic statistics with pie charts, bar graphs, and trend lines;
- Offer real-time ranking of users and applications;
- Provide instant alerts for system events and security risks.

Product Features



GUANAN Intrusion Prevention System

It is new generations of intrusion preventive security products. Facing an increasingly challenging network environment where there are more and more concealed threat means and complex sources affecting wider range, GUANAN Intrusion Preventive System performs thorough analysis and detection of layer 2 to layer 7 of networking from a brand-new user perspective, which can defend against traditional ARP and DDoS attacks block viruses, worms, Trojan horses, overflow attacks and other malicious behaviors hidden in network traffic. The system also supports feature analysis and risk assessment in combination with sandbox, thus comprehensively protecting against known and unknown threats. GUANAN Intrusion Preventive System provides comprehensive security protection from the network layer to the application layer on both users' network and servers, which is in compliance with Multi-Level Protection Scheme (MLPS) 2.0.

Key Features

- Comprehensive Intrusion Prevention
- Proactive Virus Protection
- Advanced Persistent Threat (APT) Defense
- Efficient and Accurate Detection Capabilities
- High-Performance Threat Mitigation

- Virtualized Scalability
- Robust Defense Architecture
- Comprehensive Log Auditing
- User-Friendly Management
- Cutting-Edge Security Expertise and Service

Key Advantages

Proficient Security Protection

Offers full-spectrum defense against intrusions, malware, and DoS/DDoS attacks through integrated prevention mechanisms.

Comprehensive Log Auditing

Generates multi-dimensional statistical reports from diverse log sources, enabling in-depth compliance analysis and incident forensics.

High-Efficiency Precision Detection

Leverages TCP packet reassembly and protocol state analysis to deliver fast, accurate threat identification with minimal false positives.

High Performance & Reliability

Features unified detection technology alongside dual-active failover and VRRP for seamless operation, ensuring low-latency processing and zero single points of failure.

Flexible Networking & Deployment

Supports bypass, routing, and transparent modes alongside virtualized deployment, adapting to hybrid IT environments with ease.

GUANAN Security Services

GUANAN Next Generation Firewall System contains various authentication methods and enables multi-dimensional and elaborate control based on application, content and assets, which can guard against network threats including DoS/DDoS attacks, violence cracking, weak passwords, vulnerability exploitation, viruses, Trojan horses, and ensure authority and security of intranet resource access . It brings cost-effective, efficie nt and integrated security protection experience to customers in various industries and strongly supports enterprises in building three-dimensional network security protection.

Phishing Email Drill Workflow

Plan Development & Scheduling

Set clear timelines and milestones.
Design realistic phishing email templates (subject lines, content, attachments).
Develop an incident response plan for potential risks.

Participant & Role Definition

Define the participant pool (e.g., specific teams/departm ents).
Assign roles: senders (to deploy simulations), targets (recipients), and observers (to monitor outcomes).

Email Creation & Deployment

Craft authentic-looking phishing emails with persuasive themes, malicious links, or fake attachments.
Distribute the emails to the targeted audience via controlled channels.

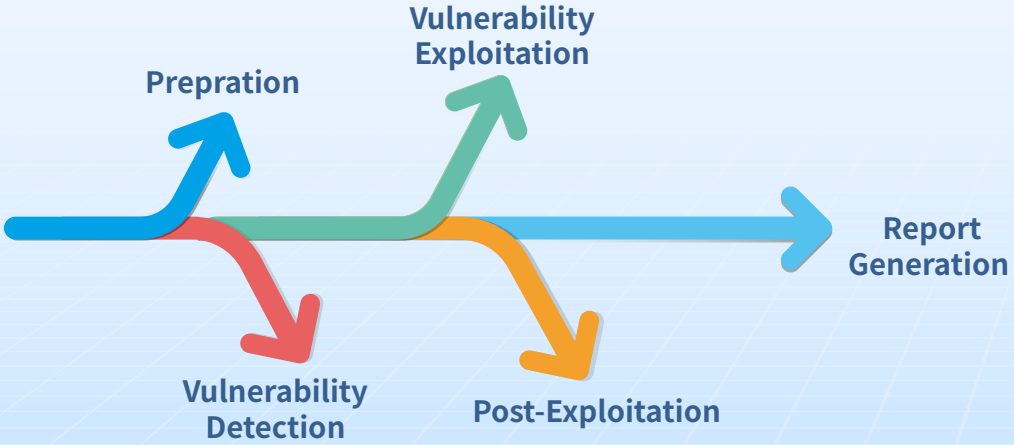
Post-Drill Analysis

Analyze data to assess employee awareness (e.g., click rates, response times, detection rates).
Generate actionable insights through reports or dashboards to inform training improvements and security strategy.

Behavior Monitoring & Logging

Track email delivery status (receipt time, open rates).
Record user interactions: link clicks, attachment downloads, form submissions, or reported suspicious activity.

Penetration Testing Workflow



Contact Information

David Zeng
Director of intemational Business Development,
Strategc Pianning Department

+86 135 2061 7806
+44 751 5548 957

zenghao3094@idss-cn.co

www.idss-cn.com

Building 9, Shibei First Center, No. 3,
Lane 1401, Jiangchang Road, Jing'an
District, Shanghai, China

Please scan the QR code to
add me as a friend

www.idss-cn.com

National Headquarters in Shanghai
Building 9, Shibei First Center, No. 3, Lane 1401, Jiangchang Road, Jing'an District, Shanghai, China

Production and Education Integration Base in Shanghai Lingang
Room 202 and Room 215, 2nd Floor, No. 800 Huanhu West 2nd Road, Nanhui New Town, Pudong New Area, Shanghai, China

National Headquarters in Beijing
8th Floor, Building A,China International Hi-teach Convention and Exhibition Center, No. 12 Yumin Road, Chaoyang District, Beijing, China

National Headquarters in Shenzhen
Room 3101, Office Building T1, Qianhai Financial Center, No.91 Guiwan 3rd Road, Qianhai Shenzhen-Hong Kong Cooperation Zone, Shenzhen, China

· The copyright of this promotional material belongs to GuanAn Info., and all rights are reserved.