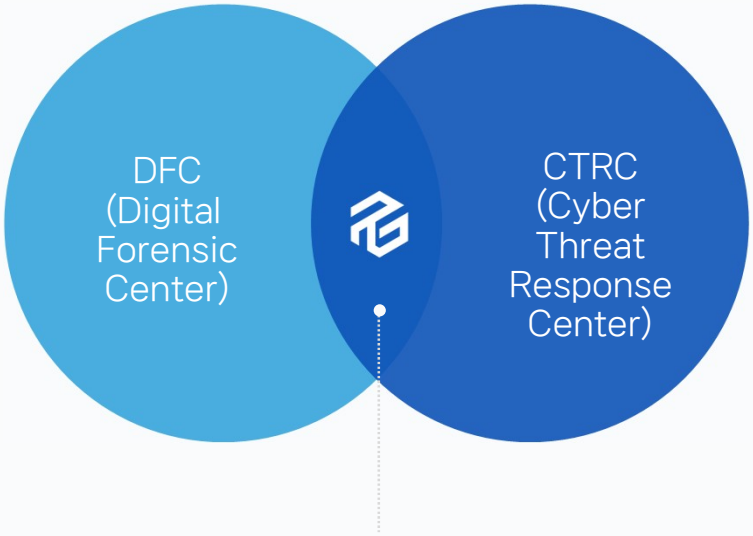
About PLAINBIT

PLAINBIT

PLAINBIT

PLAINBIT

The best experts in Korea who provide digital forensics-based services, to find the hidden meaning of the digital world and solve problems in the field.



"Providing total service based on digital forensics"

DFC, Digital Forensics Center

Internal Investigations | eDiscovery | Digital Evidence Analysis
Litigation Support | Digital Forensics Consulting
Reselling Digital Forensics Solutions | dForensics Lab

CRTC, Cyber Threat Response Center

AD Security Assessment | Security Risk Assessment | CERT-PLB
Digital Forensics & Incident Response | Compromise Assessment
IR Retainer | Cyber Threat Intelligence | R&D | IR Lab

PLAINBIT, leading the DFIR market – proven through experience

10+ YEARS
Incident Responses and Investigations

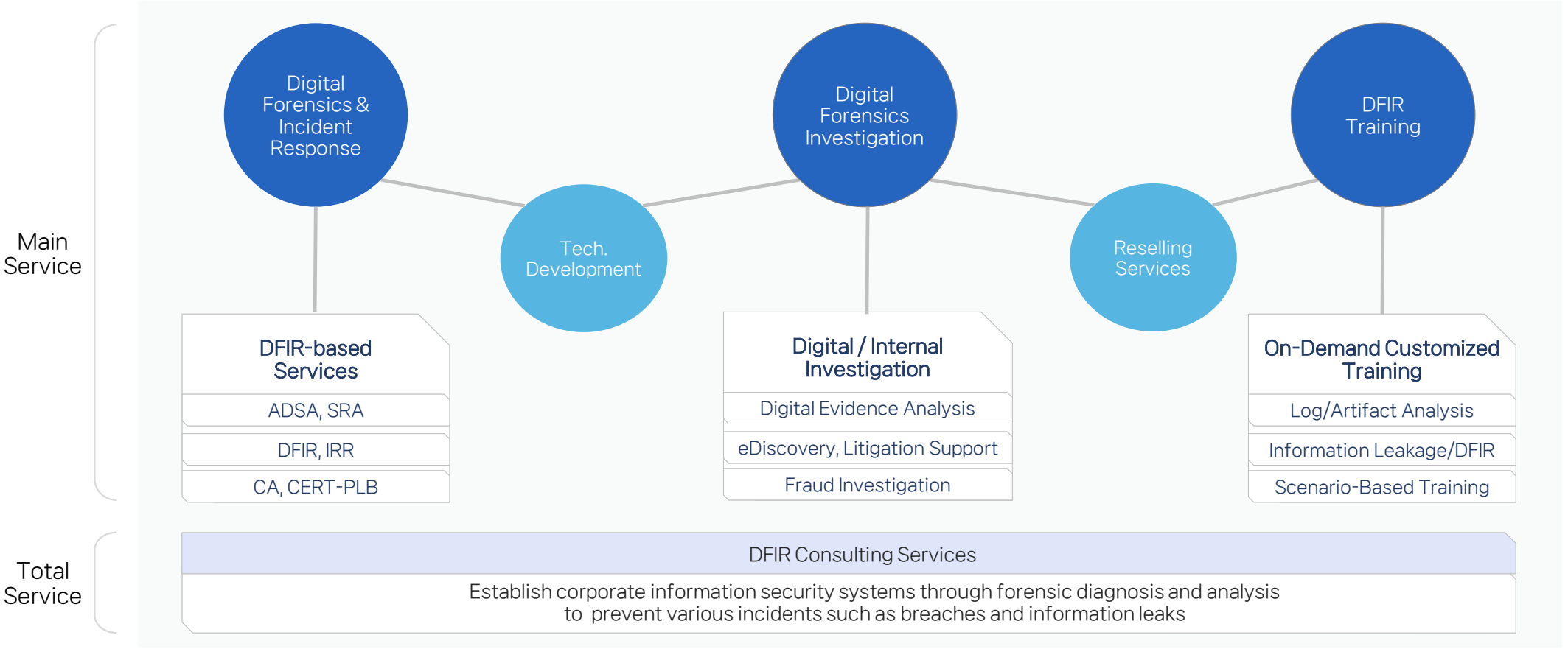
4,000+ CASES
Handled in the last 5 years

50+ CASES
Large scale incidents
(with various government agencies)

- Korea's only digital forensic expert group, comprised of top-tier DFIR specialists in Korea
- Since 2013, extensive experience and expertise in consulting and investigating cyber threats
- Over the past five years, conducted investigations for more than 4,000 incidents

  National-scale security incident response | Public and private sector security investigations
  Cybersecurity consulting services | Participation in joint public-private investigation teams
- A company trusted by regulatory agencies, law enforcement and private enterprises
- A company that advises security experts both domestically and internationally

We provide comprehensive digital forensic-based services through continuous technological research and the development of customized solutions tailored to our clients.



We solve issues at incident sites using digital forensic technology, and provide unique response strategies to enhance security levels in cyber environments.

Prevention

ADSA (Active Directory Security Assessment)

Providing response strategy services to enhance security levels in AD environments

SRA (Security Risk Assessment)

Systematic evaluation services to enhance the organization's cybersecurity level

CERT-PLB (Cyber Emergency Response Team)

Next-generation cyber threat monitoring service for real-time threat detection

Response

DFIR (Digital Forensics & Incident Response)

A to Z Digital Forensics and Incident Response

CA (Compromise Assessment)

A service that identifies hidden current and past incident threats to strengthen defense capabilities

IRR (Incident Response Retainer)

Annual subscription service for incident response

We provide digital forensic services that identify issues within the organization objectively using reliable data, by trusted experts with proven tools.

Internal Investigation

Digital forensic services for investigating issues in organization

- Fraud Investigation
- Information Leakage Investigation
- Patent and Trade secret infringement investigation
- Compliance Violation Investigation
- Ex-employee Investigation

eDiscovery

eDiscovery services supported by experts with extensive experience

- Data Collection
- Data Processing
- Document Review

Digital Forensics

Digital forensic services by trusted experts using proven tools

- Mobile Forensics
- IoT/Embedded Forensics
- Network Forensics
- Disk/Database Forensics
- Data Preservation Support

Litigation Support

Digital forensic consulting for litigation, investigations, and disputes

- Investigation response consulting
- Dispute Support
- Expert reports and statements
- Technical consulting on legal review

PLAINBIT+ is an educational brand created to share the expertise gained by PLAINBIT.
PLAINBIT+ consolidates PLAINBIT's 12 years of DFIR expertise to offer top-tier training

DFLI (Leakage Information)

Investigation for information leaks based on latest cases

- Scenario-based Practice
- Information Leakage Investigation
- Incident Data Selection and Collection
- Analysis of Leakage Traces in Various Forms

DFIR (Incident Response)

Web-based incident investigation and targeted internal attacks

- Overview of Incident Response
- Incident Data Collection and Evidence Management
- Web Attack Practice and Log Analysis
- Techniques and Artifacts related to Incidents
- Practice using Real Life Cases

Digital Forensics

Digital forensics training led by trusted expert instructors

- Mobile Forensics Analysis
- Fundamental and Advanced Disc Forensics
- Digital Forensic Tools
- Database Forensics
- Data Preservation

Customized Training

Customized training course by selecting DFIR modules

- Organized according to the Customer Needs
- Theory and Practice-Oriented Approach
- Evaluation Feedback After Training Sessions
- Flexible according to Personnel, Location, etc

Prevention Services

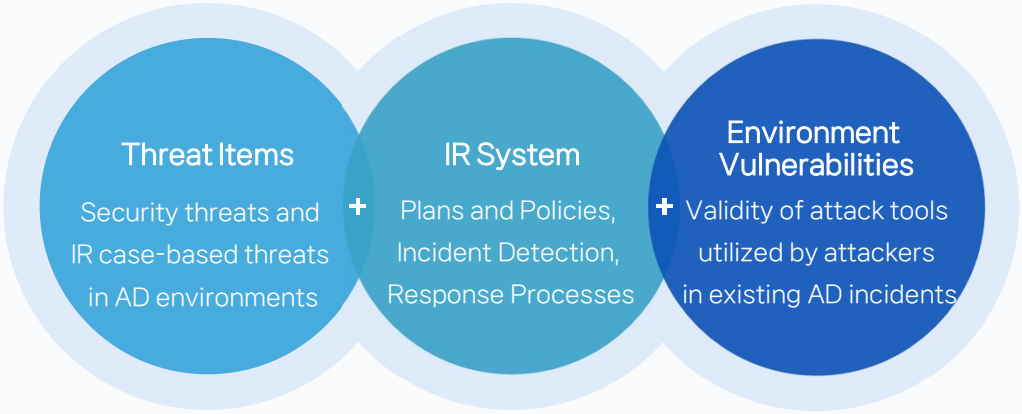
- ADSA, AD Security Assessment
- SRA, Security Risk Assessment
- CERT-PLB

PLAINBIT

PLAINBIT

PLAINBIT's proven expertise to evaluate your Active Directory environment with differentiation and precision and provides a response strategy

to improve the security level of your Active Directory environment.



Increase the security of your Active Directory environment

to better protect and enhance your infrastructure.

Point 1

Establish a plan to protect against cyber threats

Point 2

Prepare a response strategy to minimize damage

Point 3

Deliver insights for rapid incident response

Point 4

Strengthen the security of your AD environment and improve vulnerabilities

PLAINBIT

A comprehensive assessment of the security of your Active Directory environment can help you effectively secure and improve your Active Directory environment and supporting infrastructure.

Threat Items (GPO, Forensic artifact-based)

- Known security threats in Active Directory
- Threats derived from incidents that have occurred in AD environments within the last 3 years.

Assessment Items

- Group and User Management
- Access Control
- Authentication Control
- Security Policies and Compliance
- Server and System Security

IR System (Forensic artifact-based)

- Anomaly detection and response systems currently in place in AD environments

Assessment Items

- Server and System Security
- Log and Audit
- Backup and Recovery
- Threat Monitoring

Environment Vulnerabilities

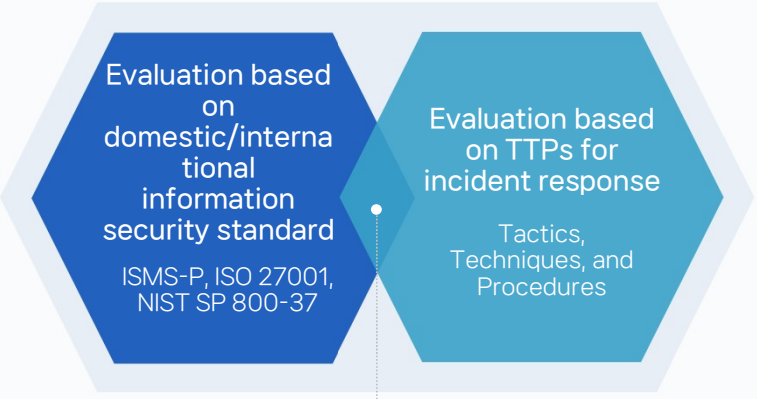
- Test for attack tools utilized in the AD environment (within the last 3 years)

Assessment Items

- Network Scanning
- LDAP Scanning
- Login Credentials
- Remote Access and Control
- Vaccine Neutralization
- System Monitoring and Control
- Brute Force

PLAINBIT

Service that systematically strengthens cybersecurity from all angles, elevating your organization's cybersecurity level by one step



- ISMS
- Policies, Organization, Asset Management
- Authentication Control
- System Service Operation and Security Control
- Access Control
- Sensitive Information Management
- Incident Prevention and Response
- Disaster Recovery

Improve the overall level of cybersecurity from every angle

Point 1	Comprehensive enhancement of cybersecurity threat response levels
Point 2	Formulating response strategies for actual threats
Point 3	Proactively identifying and addressing potentially vulnerable security environments

PLAINBIT

Based on years of accumulated experience and expertise in incident response consulting, we propose a safer and more robust security environment that can enhance overall security levels

Network

- Internal/External Network Configuration
- Firewall Configuration and Vulnerabilities
- Web Filter Settings
- Spam Filtering Settings
- IDS/IPS Review
- Configuration and Security Settings of Other Network Equipment

Server/Endpoint

- IT Asset Mgmt Process
- Performance and Incident Management
- Backup and Recovery
- Antivirus Management
- System Security Settings
- Log Management and Settings
- Server Update Process

Information Security

- Sensitive Data Mgmt
- Data Protection and Processing
- Security System Config.
- Endpoint Protection
- Patch Management
- Access Control
- Malware Control
- User Training
- Security Team Structure

Process/Policy

- Overall IT Policy
- Business Continuity Plan
- Media Control Policy
- Incident Prevention and Response System
- Anomaly Behavior Monitoring Plan
- Risk Management Process
- Protection Measure Requirements

Service where IR experts monitor threats within the organization using EDR and provide the necessary information for clients to respond appropriately

Threat monitoring in organization leveraging our extensive IR experience

using CrowdStrike EDR, the world's leading endpoint protection solution

Point 1	APT threat monitoring specialized for domestic and international contexts
Point 2	Monitoring internal user behavior
Point 3	Detecting threats specific to Korea (utilizing proprietary intelligence information)
Point 4	Expanding insights of organization's internal and external cyber threats
Point 5	Enhancing and improving the organization's cybersecurity framework

PLAINBIT

For everyday evolving cyber threats, we stay one step ahead by monitoring and detecting through the eyes of experts

Service Overview

CERT-PLB consists of following 2 services

Compromise Indicators

Strengthen monitoring by utilizing cyber threat intelligence provided by PLAINBIT

Offers

- Compromise Indicator
- Cyber Threat Indicator

Monitoring-Analysis-Response

Real-time monitoring, analysis, and response to endpoint threats

Offers

- Continuous monitoring
- Analysis of the causes of anomalies
- Response measures for anomalies

Service Details

We offer following on this service

Cyber Threat Monitoring

- Utilizing localized proprietary cyber threat intelligence information
- Employing proprietary playbooks reflecting know-hows
- Establishing a customized monitoring system

Threat Analysis and Review by Experts

Provide threat intelligence and response method guide

Response Services

- DFIR, Digital Forensics and Incident Response
- CA, Compromise Assessment
- IRR, Incident Response Retainer

PLAINBIT

Service to clearly identify the causes of incidents and their routes within the organization by using Digital Forensics technology, preventing the recurrence of similar incidents

"We solve issues of incident sites."

Incident Analysis

"The most effective service for preventing recurrence"

Provide the exact cause, propagation path, and impact of incidents, and solutions based on the analysis of experts with extensive experience.

Incident Response

"Professional on-site response service to minimize damage"

Experts with incident response capabilities jointly address threats on-site to minimize damage or neutralize the attacker's objectives

Analyze all incident contexts, identify issues, and propose solutions to minimize damage and prevent recurrence

Incident Investigation List

Initial Compromise

- File Download Traces
- Email Traces
- Vulnerability Exploitation Traces
- Remote Service Usage Traces
- External Media Connection Traces
- Network Ingress Traces
- External Service (WEB, DB, etc.) Traces

Compromise Execution

- Executable File Run Traces
- Script Execution Traces
- Document Access Traces
- Library Usage Traces
- Abnormal Filename Traces
- Additional Malware Download Traces
- External Service (WEB, DB) Traces

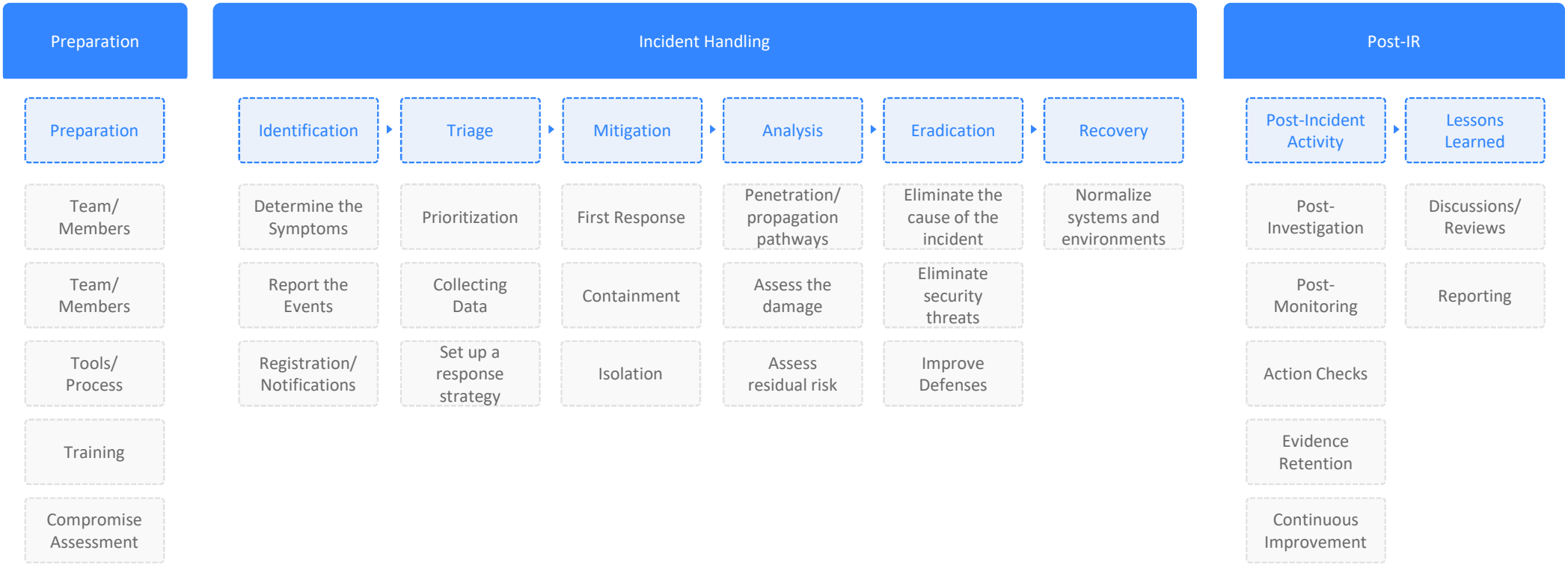
Compromise Persistence

- Account Creation/Modification
- Service Creation/Modification
- Autorun Registration Traces
- Malware Preferred Paths
- Task Scheduler Creation/Modification Traces
- Malware Hiding/Deletion Traces
- Anti-Forensic Traces
- External Service Traces

Compromise Propagation

- Sniffing/Spoofing Traces
- Email Propagation Traces
- Vulnerability Exploitation Traces
- Abnormal Authentication History
- Remote Service Access Traces
- Web/Email Traces
- Network Ingress Traces
- External Service Traces

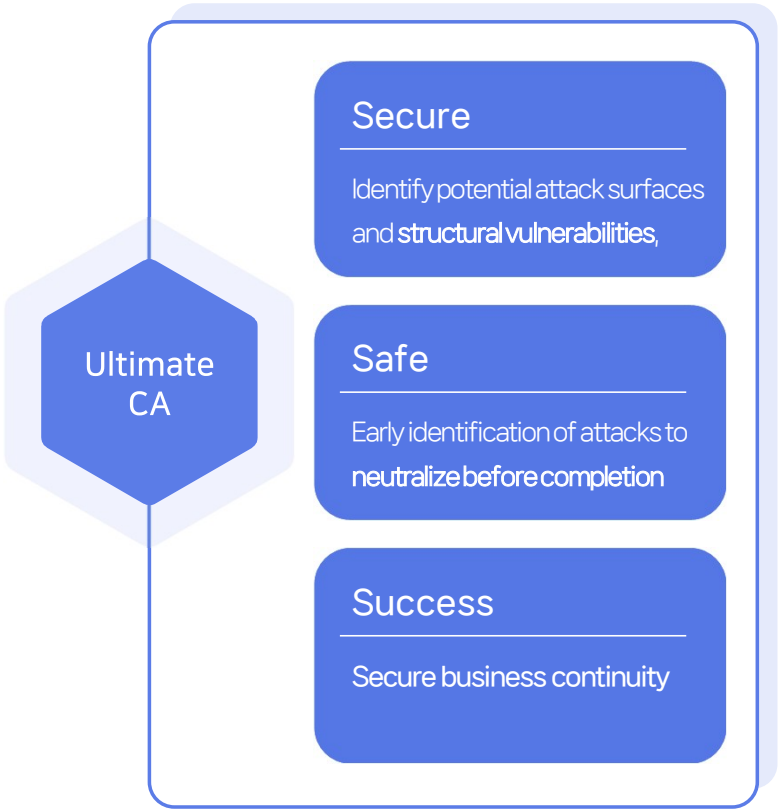
With years of DFIR experience, we have established a proven incident response process unique to PLAINBIT



PLAINBIT

Service to answer the question, 'is our company already hacked?'

by evaluating entire cyber environment, from network to host, from a breach perspective.



NCA
Network-based CA
NARUSECURITY

HCA
Host-based CA
PLAINBIT

MITRE ATT&CK based CA

Evaluate from known attacks to potential threats based on the attacker's TTP (Tactics, Techniques, Procedures)

- Identify initial compromise, foothold establishment, execution/persistence, propagation, and exfiltration/destruction

Zero Trust based CA

Monitor and evaluate all connection activities on the network and host

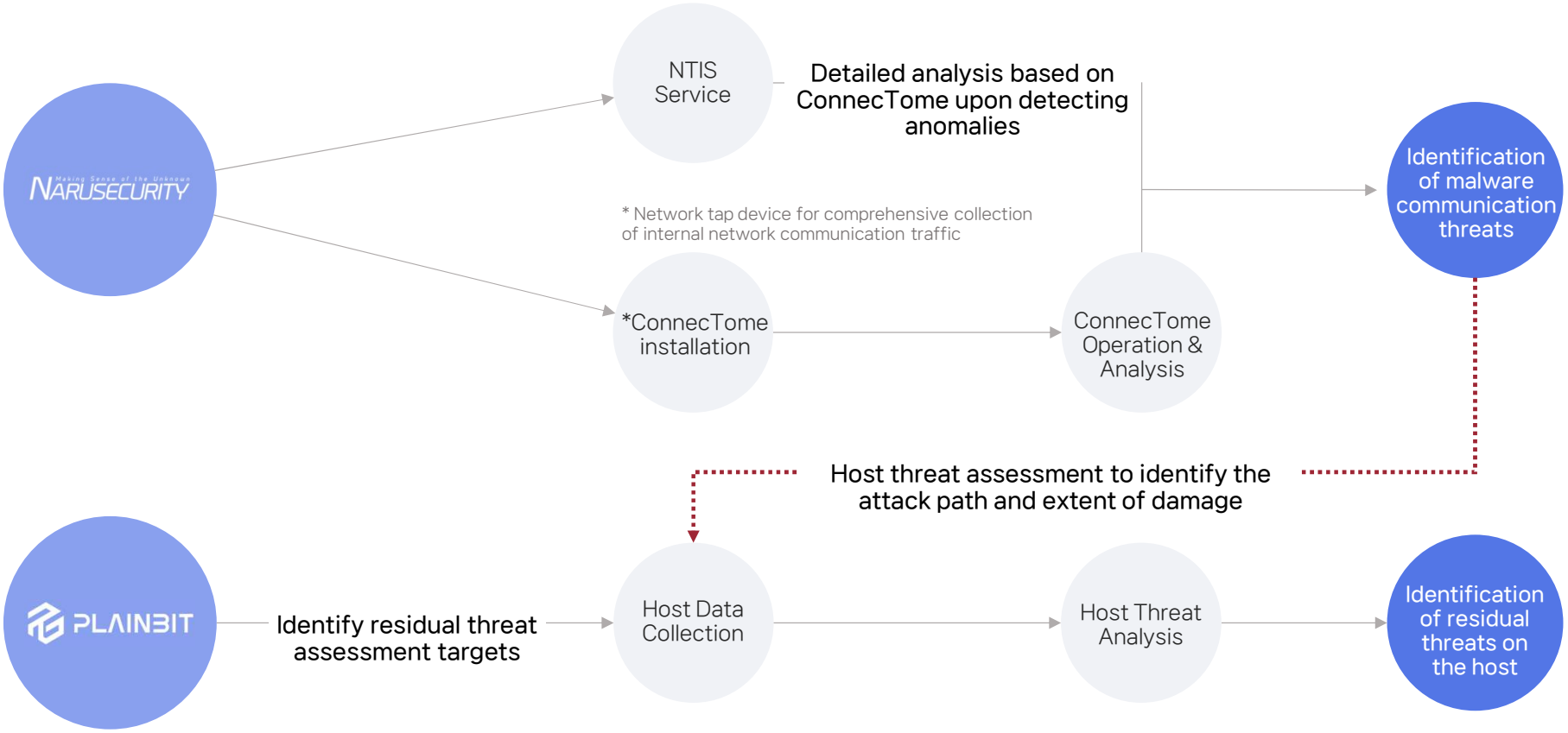
- Identify communication such as remote control, tunneling, proxy, abnormal DNS queries, etc.

Threat Indicators based CA

Evaluate threat indicators from cyber-attacks in the past 3 years

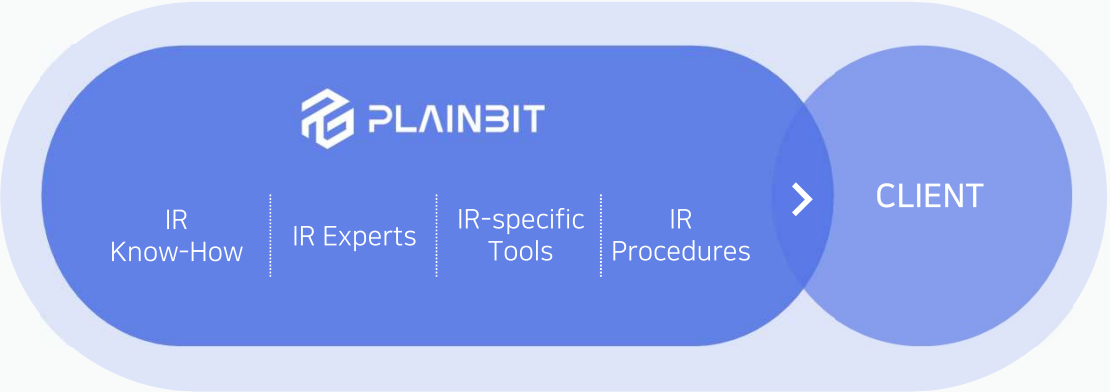
- Communication related to botnet, hacking relays, command control infrastructure, and attack tools

Diagnose all threats in the cyber environment from network to host to identify potential threats that may have been missed



PLAINBIT

An annual subscription service that secures the necessary resources and experts in advance to ensure immediate expert response in the event of a cybersecurity incident.



Point 1	Professional support for rapid response to cyber threats
Point 2	Enhancement of the organization's cyber threat response capabilities
Point 3	A variety of incident response services for versatile use
Point 4	Your security partner
Point 5	Cost and time saving to minimize operational disruptions

PLAINBIT

Have trusted incident response experts by your side, ready to assist at any time.
Guaranteed quick and effective responses in times of crisis

Service Level

Incident response retainer services are provided as follows. (Prepaid hours can be added)

Standard

- Response support **M-F 9 am to 5 pm**
- Remote support **within 6 hrs**
- Onsite support **within 48 hrs**
- IR Prep* **16 hrs**, Annual IR **50 hrs**
- Service period: **1 year**

Premium

- Response support **24/7**
- Assign **dedicated team**
- Remote support **within 4 hrs**
- Onsite support **within 24 hrs**
- IR Prep* **24 hrs**, Annual IR **100 hrs**
- Service period: **1 year**

- IR Prep Hours: Time to pre-assess the organization's cybersecurity level for the service

Service Details

Subscribe annually to the necessary incident response time for the organization in advance

Included Services

Incident/Threat Analysis | Incident/Threat Response |
Methodology for incident handling

Services that can be exchanged from prepaid hours

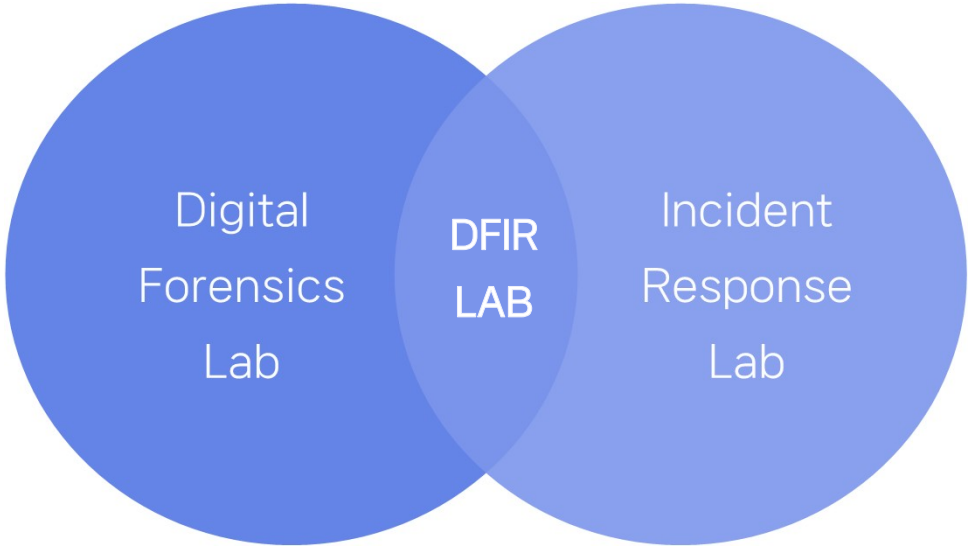
Incident Response Readiness Assessment |
Incident Security Risk Assessment | Digital Forensic Analysis
Cybersecurity Awareness Training |
Specialized Training for Incident Response

DFIR Lab

- Digital Forensics Lab
- Incident Response LAB

PLAINBIT

A DFIR lab, which stands for Digital Forensics and Incident Response lab, is a specialized environment focused on the investigation of cyber incidents and the forensic analysis of digital evidence.

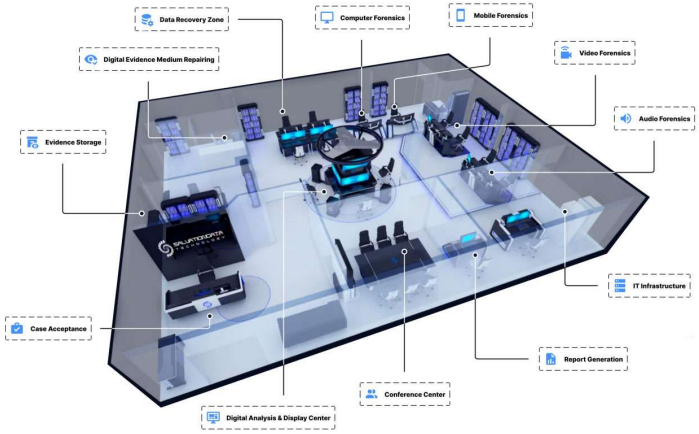


Focused on the process and environment for being admissible in court

Focused on rapid detection and response to cyber threats

A digital forensics lab is a specialized facility that conducts meticulous investigations and analyses of digital devices and data. This lab encompasses the processes of collecting, preserving, analyzing digital evidence, and ensuring its legal admissibility.

The primary purpose of a digital forensics lab is to investigate incidents related to cybercrime, data breaches, and security incidents, extracting relevant information and presenting it in a form suitable for use in court.



01. Hardware

- **Workstations**: High-performance computers with powerful processors and ample storage for processing and analyzing large volumes of data.
- **Storage Devices**: Secure storage solutions to archive evidence and analysis results, including network-attached storage (NAS) or cloud storage.
- **Forensic Tools**: Dedicated hardware such as write blockers, which prevent modification of data on storage devices being examined.
- **Data Acquisition Tools**: Devices used to create exact replicas of digital data, such as disk imagers.

02. Software

- **Forensic Collection Tools**: FTK Imager, Magnet ACQUIRE, Opensource
- **Forensic Analysis Tools**: Magnet AXIOM, X-Ways Forensics, EnCase
- **Mobile Forensics Tools** : Cellebrite, GrayKey, GMDSoft, Oxygen
- **Network Analysis Tools**: Programs for investigating network traffic and security breaches
- **Data Recovery Tools**: Software to recover deleted, damaged, or hidden data
- **Automate Workflows** : Magnet AUTOMATE

03. Personnel, Training and Certification

- **Personnel**: Digital Forensic Analysts, Network Security Experts, Malware Analysts, Legal Advisors, IT Support Specialists, Project Managers
- **Trained Personnel**: Staff should have knowledge of digital forensics principles and procedures.
- **Certifications**: CCE, CFCE, MCFE, X-PERT, EnCE, ...

04. Infrastructure

- **Secure Facility**: Physical security measures to protect evidence and ensure restricted access.
- **Evidence Storage**: Temperature-controlled and secure areas to store physical and digital evidence with strict access controls.
- **Backup Systems**: Robust backup solutions to prevent data loss.
- **Access Control**: Secure the lab and the equipment to protect evidence from tampering.
- **Environment Control**: Ensure the lab is physically secure and has a controlled environment to prevent damage to evidence.:

05. Working Environment

- **Working EnvironmentLab Layout**: Design an efficient workspace that facilitates collaboration and minimizes distractions.
- **Networking Equipment**: Reliable internet access and secure connections for remote analysis and communication.

06. Legal and Compliance Resources

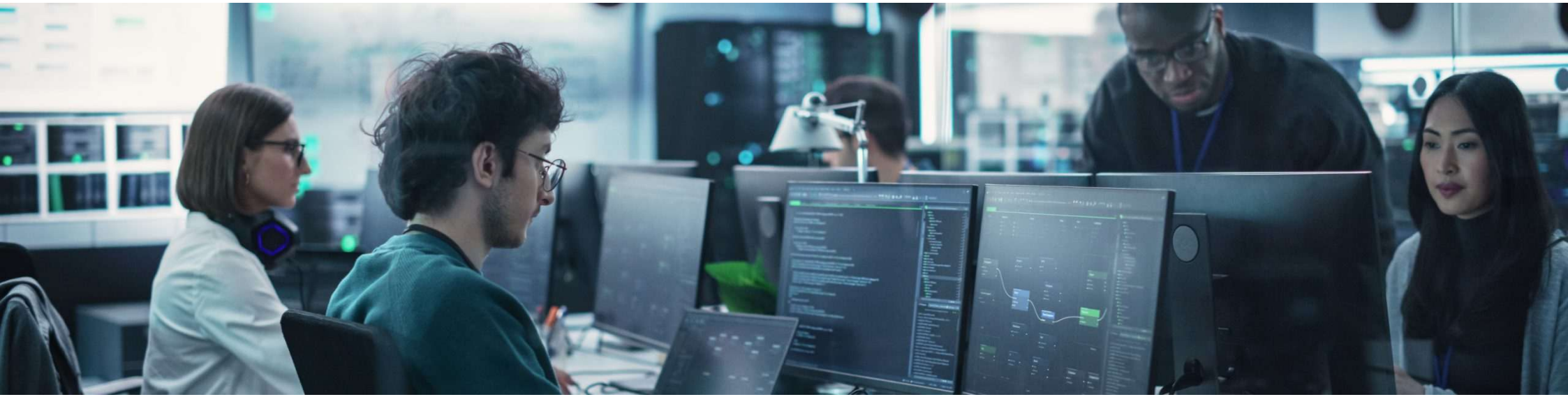
- **Chain of Custody Protocols**: Documentation practices to ensure all evidence is accounted for and its integrity is maintained.
- Standard Operating **Procedures (SOPs)**: Established methods to follow during investigations to ensure thoroughness and legal compliance.
- **Documentation Templates**: For maintaining chain of custody and documenting procedures and findings.
- **Legal Guidelines**: Understanding regulations and legal considerations surrounding digital evidence.

07. Supporting Resources

- **Reference Libraries**: Access to texts, manuals, and online resources for ongoing education.
- **Collaboration Tools**: Platforms for communicating and sharing information with team members or clients.

An Incident Response Lab is a specialized facility focused on preparing for, managing, and analyzing cybersecurity incidents. Its primary goal is to detect, respond to, manage, and recover from security breaches or cyberattacks on an organization's systems and data.

The lab typically comprises
skilled professionals, tools, and processes designed to effectively handle and mitigate incidents.



01. Personnel

- **Incident Response Team (IRT)**: A group of trained professionals, including incident responders, cybersecurity analysts, and forensics experts, who handle incident detection, investigation, and remediation.
- **Legal Advisors**: Individuals knowledgeable in cybersecurity law who ensure compliance and appropriate handling of legal issues during incident responses.
- **Communications Staff**: Team members responsible for internal and external communications, including notifying stakeholders about incidents.

02. Tools and Technologies

- **Security Information and Event Management (SIEM) Systems**: Tools that aggregate and analyze log data from various sources to identify suspicious activities.
- **Intrusion Detection/Prevention Systems (IDS/IPS)**: Technologies that monitor networks for malicious activities and can take action to block potential threats.
- **Incident Management Software**: Platforms for documenting, tracking, and managing incidents throughout their lifecycle (e.g., ticketing systems).
- **Forensics Tools**: Software and hardware used to analyze compromised systems and gather evidence (e.g., X-Ways Forensics, Magnet AXIOM).
- **Malware Analysis Tools**: Solutions for examining and understanding malware behavior.

03. Infrastructure

- **Secure Workstations**: Dedicated computers for incident responders, equipped with necessary tools and isolated from the main organizational network.
- **Storage Solutions**: Secure storage for preserving incident-related data and evidence, including cloud and on-premises options.

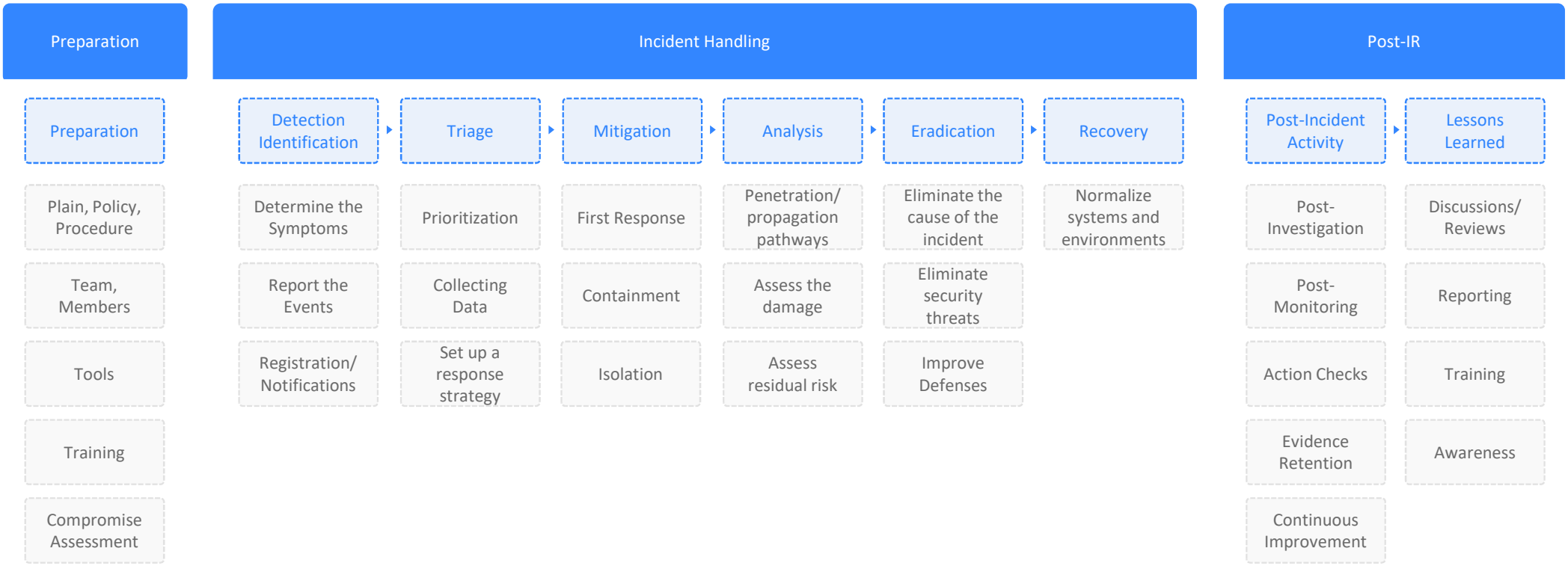
04. Processes and Procedures

- **Incident Response Plan**: A documented procedure for responding to incidents, detailing roles, responsibilities, and steps for detection, containment, eradication, and recovery.
- **Communication Protocols**: Established guidelines for internal and external notifications during an incident, including escalation procedures.
- **Post-Incident Review Process**: A structured approach for analyzing incidents after resolution, including documenting lessons learned and improving future responses.

05. Training and Awareness

- **Regular Training Programs**: Ongoing training for incident response team members to keep their skills current and familiarize them with new tools and tactics.
- **Security Awareness Programs**: Initiatives for all employees to recognize and report potential security threats.

DFIR Process



The compromie should not lead to an incident.

PLAINBIT