GETSecure™
Your security is the key to our success!

AFIRM

active forensics intelligent response method

The S.A.N.E. approach to computer forensics

GETSecure
110 North Patterson Blvd.
Dayton, Ohio 45402
Phone: 937/461-6755
Fax: 937/461-4473
www.getsecure.com

GETSecure™
Your security is the key to our success!

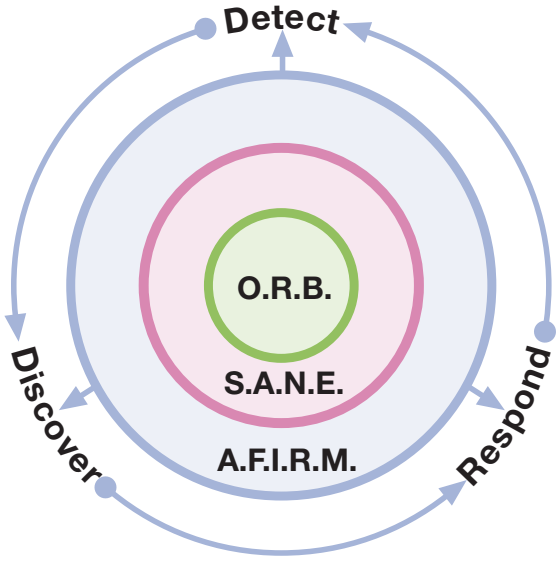
Abstract

Traditional computer forensic techniques and tools are inadequate to meet the threats facing today's information infrastructures. Vital systems are taken off-line to secure evidence and assess damage. This activity is generally more costly than the attacks themselves and totally unacceptable in production environments. The traditional approach also does not address the need for real-time decision support capabilities.

As cyber attacks become more frequent, the inadequacies of current forensic methodologies could severely jeopardize national security. A hybrid approach is required, based on active forensics, adaptive security, and integrated with intelligent response capabilities. This improved forensics approach consists of a comprehensive methodology and the necessary support to implement it.

Our approach is cognitive of evidentiary procedure and flexible enough to respond to any cyber threat. Our model provides a constant forensics presence that becomes an integral part of a total information security program.

Adaptive Computer Forensics Model



Background Information

Computer forensics is concerned with the collection, analysis, preservation and presentation of digital evidence. This evidence is usually used for criminal & civil litigation. Non-repudiation is the key to effective computer forensics.

Many organizations have invested large amounts of resources in security technology. Regardless of the components chosen, very few organizations effectively leverage this investment. There are many reasons for this phenomenon. Security components are thought of as stand-alone devices as opposed to part of a system. Often there is not enough in-house talent to adequately address the problem. Many times, the biggest problem is the lack of commitment from decision-makers.

Traditional computer forensics is an antiquated and cloistered discipline. Exclusively the realm of government/law enforcement, large research concerns and boutique shops, practitioners are not easily developed. This accounts for the current shortage of Certified Computer Forensics Technicians (CCFT). We anticipate this condition to worsen as litigation involving digital evidence increases.

"Today when new FBI agents graduate from our training academy in Virginia, they leave with their firearms and their badges, but they also leave with a laptop computer…When they serve law enforcement search warrants, they seize hard drives and disks instead of the boxes and boxes of records and books and ledgers that their predecessors, myself included, used to seize to support our cases" stated by Louis J. Freeh, Director of the FBI, at the 1997 International Computer Crime Conference, New York, New York, March 4, 1997,

Current and pending legislation will likely provide the compelling event in regards to computer forensics. The demand for computer forensics technicians could increase a hundred-fold overnight. Unfortunately, the lack of skilled CCFTs will leave many court cases open to appellate scrutiny.

Many computer technology workers and security professionals engage in computer forensic activity on a daily basis. However, they do not consider themselves forensic technicians. It is our position that these individuals represent a potential army of CCFTs. By providing a practical methodology to a readily available workforce, the foundation for *audit friendly* computer environments can be created.

All content © 2000/2001 GETSecure. All rights reserved.

GETSecure™

Your security is the key to our success!

The Problem

Currently, computer forensics adds limited value to enterprise network environments. It is reactive and passive - a direct descendent of traditional criminal theory and law enforcement investigative practices. It's utility is only engaged after an intrusion or seizure has occurred. Often this is too late to help prevent a catastrophic event. This is unfortunate, considering the value such techniques could provide in overall network security. A more systematic and proactive approach is required.

While there are effective ways to retrieve corrupted, encrypted, or damaged data, there is currently no way to effectively produce the details of an unrecorded event. For example a CCFT cannot audit log entries that were never recorded. This is why a proactive strategy suggests a standard level of “auditability”. Unfortunately, this level of awareness is often resource intensive.

The difficulty in securing systems connected to public, untrusted networks is compounded by the sheer volume of transactions on those networks. Users are constantly demanding new services and more access. Security and IT personnel are being asked to do more with less. The only way to maintain information superiority is to aggressively exploit multiple technologies. When vital systems are forced to utilize vulnerable technologies, contingencies for defending against those weaknesses must be built into the information infrastructure itself.

“Thus, the NIPC is housed in the FBI to enable it to utilize the appropriate authorities to gather and retain the necessary information and to act on it. Now, this does not mean that the ultimate response to a cyber attack is limited to criminal investigation and prosecution. The response will be determined by the facts that are uncovered. Thus, for instance, if it is determined that a cyber intrusion is part of a strategic military attack, the President may determine that a military response is called for. But no such determination can be made without adequate factual foundation, and the NIPC's role is to coordinate the process for gathering the facts, analyzing them and making determinations about what is going on, and determining what responses are appropriate” stated by Michael A. Vatis, Director, National Infrastructure Protection Center Federal Bureau of Investigation, before the Senate Armed Service Committee, a subcommittee on Emerging Threats and Capabilities, Washington, D. C., March 16, 1999.

To this end, a new approach is warranted. Our approach supports the deployment of an adaptive computer forensics presence, including support collateral, training and maintenance capabilities.

Benefits

1. Provides immediate utility to national security concerns, protecting and supporting the 21st century's information command and control infrastructures.

2. Provides an immediate and long-term solution to securing and protecting information infrastructures across all sectors of society.

3. Provides a competitive advantage to organizations that effectively implement its teachings.

4. Will stimulate economic development by providing more secure cyber commerce environments.

5. Will ensure the continued expansion and technological evolution of the Internet, thereby preserving the global communication phenomena.

All content © 2000/2001 GETSecure. All rights reserved.

GETSecure™

Your security is the key to our success!

The Project

In order to promote the acceptance and use of proactive computer forensics techniques, we have made our initial research publicly available. We hope that by making it widely available to computer security experts, computer forensic specialists, and others that it will be embraced and enhanced. It is our desire to produce open source code and promote/support open source developers who subscribe to our methodology.

We recognize that an organization's most valuable asset is information. The most valuable capability is its ability to wield that information effectively. Information networks provide resources and conduits for wielding information assets. In order to secure those assets and exploit their potential, systems must be able to define risks and immediately respond to information incursions.

Initial R&D Highlights:

- Identified gap in the market
- Defined current procedural shortcomings in computer forensics and network security
- Analyzed current defensive and offensive capabilities
- Developed a practical methodology that is flexible and scalable (AFIRM)
- Created a open and extensible software architecture (SANE)
- Developed and refined scenario modeling techniques
- Developed and refined decision support capabilities
- Implemented SANE prototypes in multiple production environments
- Supported the model by developing certification training for its practitioners

Commercial products only satisfy part of the need. In order to effectively incorporate internally developed tools and off-the-shelf tools, we created a common user-interface, database, and infusion capability. Communications to data collection points and data control points are provided through secure channels. These components are collectively known as Secure Adaptive Network Environment (S.A.N.E.).

Results

Our efforts have resulted in the first proactive computer forensics model. It is proactive in the sense that it accommodates the need for real-time discovery and decision support capabilities. The model consists of two main components:

1. Active Forensic Intelligent Response Method (AFIRM) – This methodology stresses simplicity and leverages existing capabilities. Its no-nonsense approach to enterprise security is bolstered by field-proven techniques. All pertinent network activity is captured, consolidated, analyzed, and preserved. It could emerge as a standard for making information systems “Audit-Ready” and less vulnerable to attack. The utility of this approach can be realized within any computing environment.

2. Secure Adaptive Network Environment (SANE) – This represents the suite of software tools and APIs, that support the efforts of security professionals and CCFTs in the field. SANE incorporates all the teachings of AFIRM, providing both active monitoring and defensive capabilities combined with powerful investigative and discovery tools. An integral part of SANE is the Object Repository Base (ORB). This is where all "in-house" discovery data is stored. It fuels the discovery engine. Constantly growing, it evolves with the environment. Once a compelling event occurs, the system scales to provide the appropriate response, extracting valuable intelligence that is infused back into the ORB.

The digital landscape represents very rough terrain. The modular nature of AFIRM and SANE provide the flexibility that is required for rapid discovery and response. This enables powerful tactical or offensive capabilities as well as support for criminal prosecution and civil litigation. Our solution can scale and adapt to support varied sectors of society including government, corporate, and private.

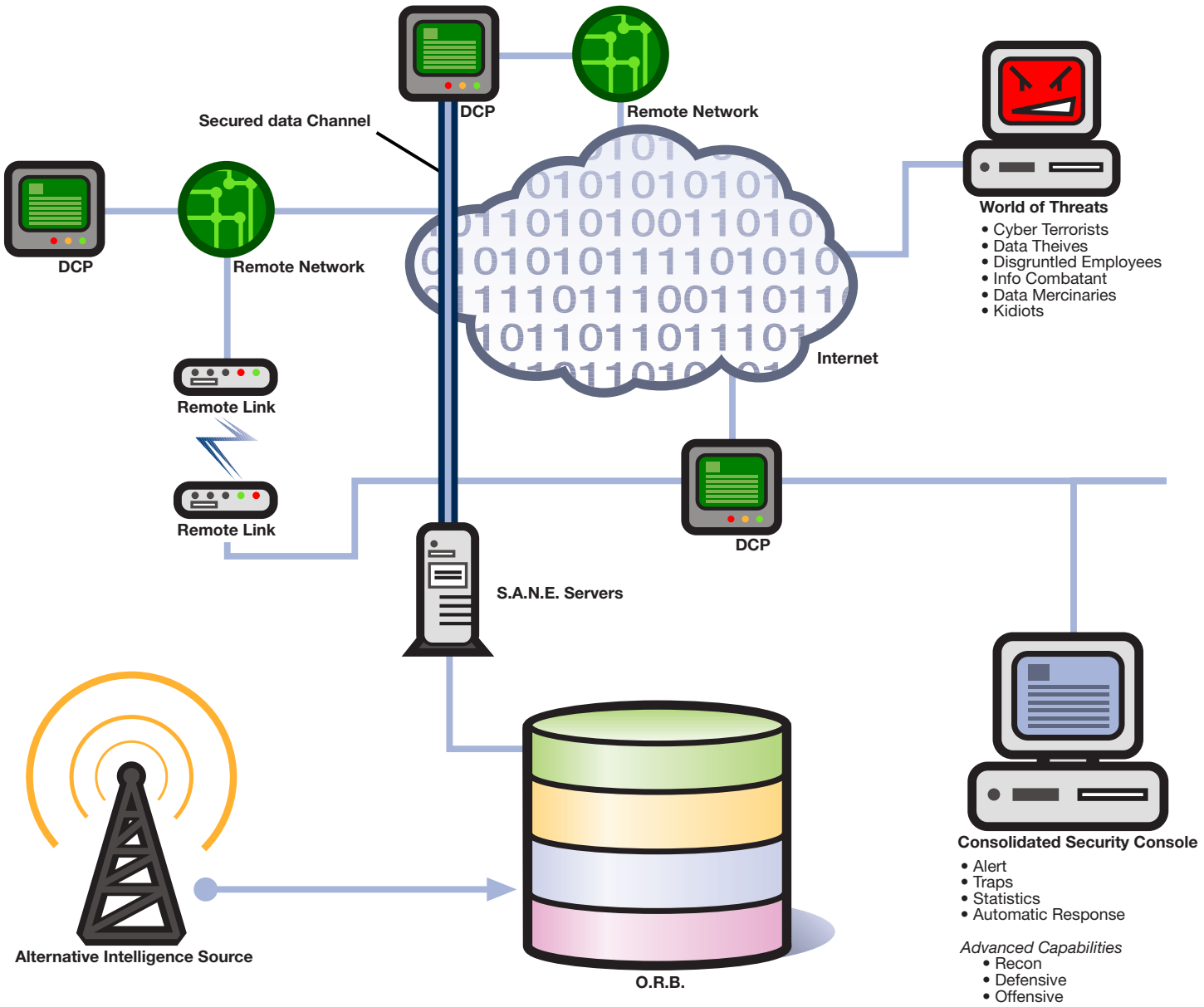
As cyber threats evolve, so must the ability to recover from them and formulate appropriate responses. In addition to the myriad of potential threats that our solution addresses, our approach also provides the capability to maintain compliance with current and pending legislation. Corporate security policies and military directives can be supported in the same way.

All content © 2000/2001 GETSecure. All rights reserved.

GETSecure™

Your security is the key to our success!

Active Forensic Itelligent Response Method (A.F.I.R.M.) in Action



All content © 2000/2001 GETSecure. All rights reserved.

GETSecure™

Your security is the key to our success!

A.F.I.R.M.™ Introduction

This document is NOT meant to be a complete guide to AFIRM. We will be releasing more detailed public information related to AFIRM in the weeks and months to come. Real-time decision support and proactive network forensics are the ultimate goal of using AFIRM!

Assumptions

1. Security is a pain!
2. Traditional computer forensics is a cloistered and specialized discipline.
3. Organizations have a fiduciary responsibility to protect information assets.
4. Compelling events will mandate a higher level of security and accountability when connecting to public infrastructures.
5. Increases in criminal prosecution and civil litigation will highlight the shortage in computer forensics standards and CCFTs.

In order for the Active Forensic Intelligent Response Method to be exploited, the following prerequisites* must be met:

1. A distributed network environment (running at least TCP/IP)
2. An organizational security policy
3. Support/participation by upper management and HR
4. Discipline and resolve

AFIRM is predicated on the belief that, by effectively utilizing existing technology, an acceptable level of risk can be achieved. However, the inverse is also true. Unless one can effectively utilize the technology they currently wield, no level of acceptable risk can be achieved.

**typical heterogeneous environments contain the following elements (firewall, router, ids, NT and UNIX)*

AFIRM stresses the following fundamental rules:

1. Simple is better
2. Know your environment
3. Trust nothing verify everything
4. Practice scenario planning
5. Utilize/leverage existing infrastructure and resources
6. Protect the confidentiality, integrity and availability of information assets
7. Non-repudiation is the most important aspect of forensics
8. Information is power only if it is collected, cataloged, and processed
9. All discovery and response activity should be treated as transactions
10. Always utilize multiple information sources

All content © 2000/2001 GETSecure. All rights reserved.

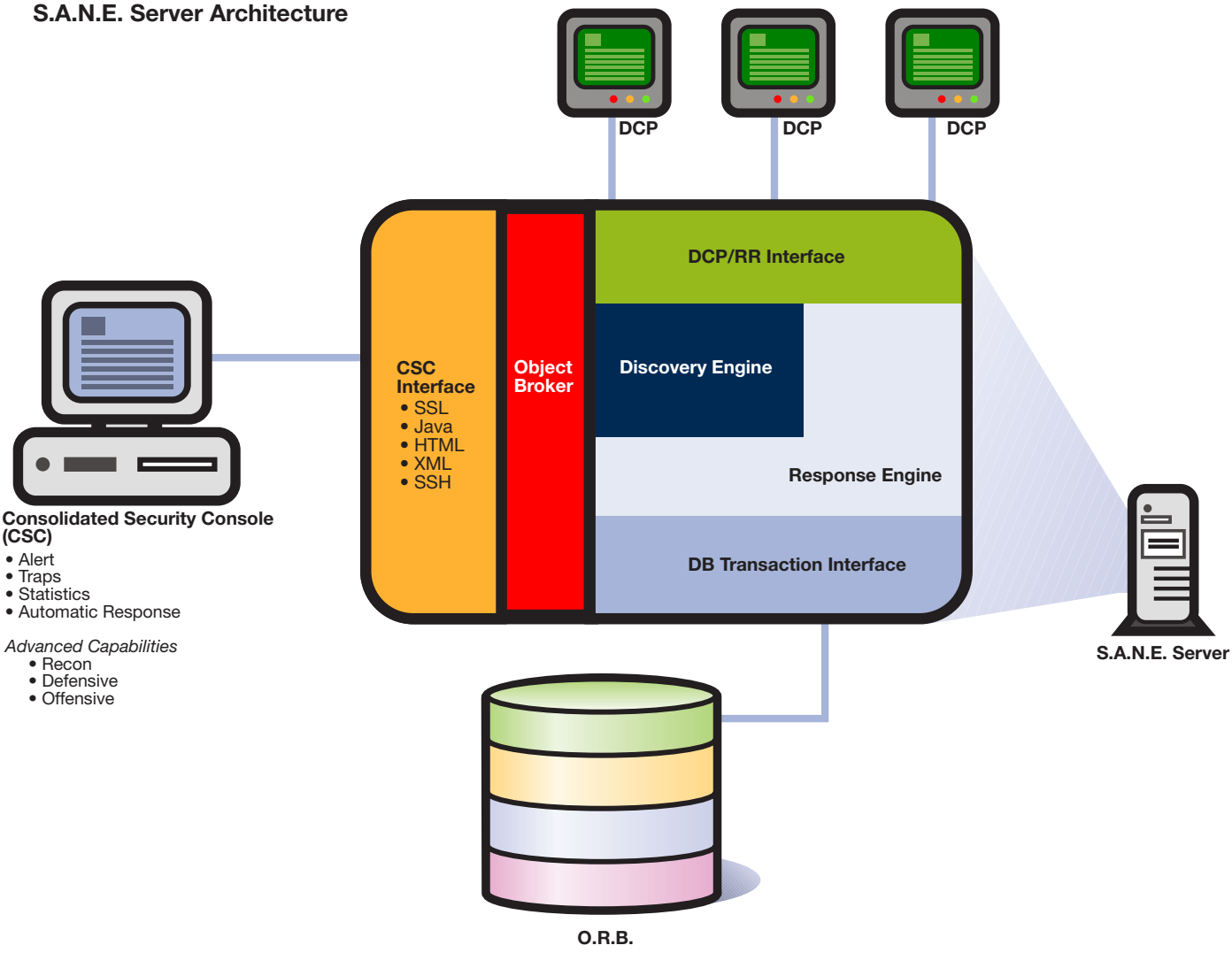
GETSecure™

Your security is the key to our success!

S.A.N.E.™

By utilizing all existing auditing and security capabilities, augmenting existing capabilities and providing the glue to pull it all together, SANE provides the foundation for supporting AFIRM requirements. Our architecture supports the addition of new network components and provides a reliable object-handling infrastructure.

S.A.N.E. Server Architecture



All content © 2000/2001 GETSecure. All rights reserved.

GETSecure™

Your security is the key to our success!

DCP - Data Collection Points/Data Control Points are distributed throughout the network. They come in many shapes and sizes. Essentially, any network device capable of collecting data or directly effecting data can be considered a DCP. Firewalls, routers, syslog daemons, gateways, and intrusion detection systems are all considered DCPs.

CSC - Consolidated Security Console provides the integrated user interface for controlling all discovery and response activities. It provides the framework for personalized/customized interfaces. This accommodates the varied nature of most enterprise network environments. By supporting technologies like HTML, Java, SSL, XML, IPSEC and others, we ensure extensibility is persevered.

DCP/RR Interface - This is the layer that provides access to and from the DCPs. It also provides access to rapid response capabilities.

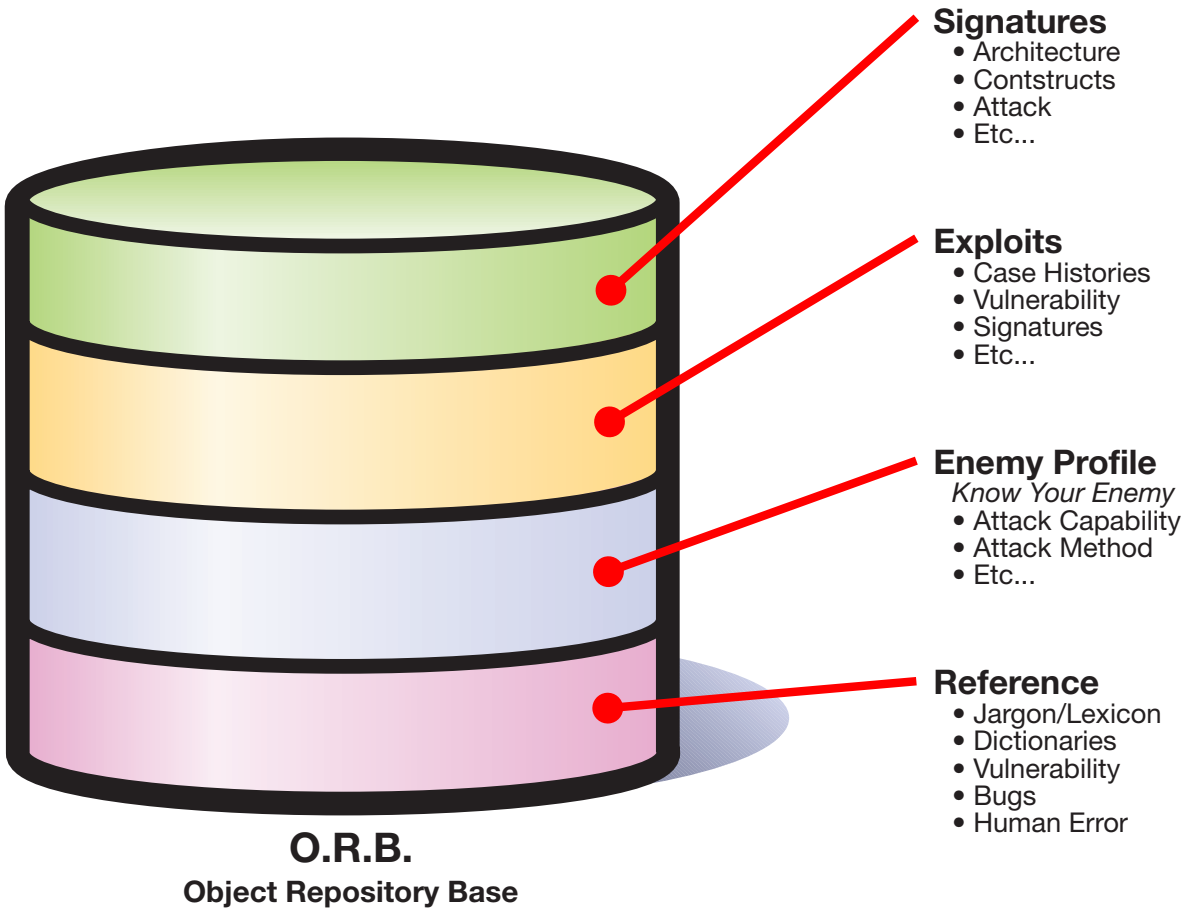
Discovery Engine - Contains the discovery logic objects.

Response Engine - Contains the response logic objects.

DB transaction Interface - Provides access to and from ORB elements. It also provides a mechanism for documenting all discovery and response activity.

Object Broker/Logic - This component is responsible for brokering all discovery requests and response directives. It also contains logic for deciding if requests are handled in-house or need to be brokered externally.

ORB - Object Repository Base is the database of all in-house intelligence used for discovery and response activities.



All content © 2000/2001 GETSecure. All rights reserved.

Summary

Adaptive network security and proactive computer forensics are a natural response to the current and ever changing cyber threat. AFIRM provides a "no-nonsense" approach to securing information assets and creating *audit friendly* networks.

The SANE software architecture and product set allow you to exploit the power and simplicity of the AFIRM approach. It also provides the flexibility to use the solutions that we provide, you develop, or are created by third-party vendors.

We are actively using AFIRM in our security practice. Now you can maximize your infrastructure investment and leverage field-proven techniques. We are soliciting practitioners and suitable network environments interested in partnering/collaborating. We also intend to solicit stronger relationships with key vendors and development partners.

We will closely monitor the effectiveness of our approach. This will give us the feedback necessary to refine the process and ensure continued utility. We welcome outside commentary and have created several vehicles for public participation.

1. **http://www.afirm.org**
   The AFIRM homepage will provide public access to all pertinent information related to AFIRM and SANE. Including white papers, toolkits, and products.

2. **http://www.pr0filer.com**
   This is the first SANE certified project ever! Project pr0filer is an open source pilot that began in July of 1999. The desired result is a publicly available enemy profiling database and the development of effective profiling logic.

GETSecure
110 North Patterson Blvd.
Dayton, Ohio 45402
Phone: 937/461-6755
Fax: 937/461-4473
www.getsecure.com

All content © 2000/2001 GETSecure. All rights reserved.