

DSF© and Cyber Forensic

Vinayak Godse
Sr. Manager- Security Practices, DSCI

Seminar on Cyber Forensics
28th November 2009

Agenda

1 Best Practices

- Approach towards best practices
- Best Practices- Security Principles
- DSCI Security Framework (DSF[©])
- DSF[©]- Services and Technical Model
- Best Practices
- Document Ecosystem

2 DSF[©]- Forensic Practices

- What is Forensic
- Computer Forensic
 - Building Forensic capability
- Investigation Approach
- Cyber Criminal, Anti-Forensic
- Computer Forensic for IT/ITES

Security Approach

The **“extensive disciplines of security”** such as APS, INS, BDM, MIM, PEN, DSC .. demand **“specialized treatment and skills”**

All of these disciplines require **“understanding from strategic, tactical and operational perspective”**

Maturing security defense at one layer (infrastructure) shifts attention of evolving security threats to higher layer (application), **“requiring continuous vigil over new approaches and changing trends”**

“Assurance over ever increasing role of security function”, expanding security activities and everyday addition of new elements in an organization’s security **“demand a complete visibility”**

The nature of a security threat to exploit system vulnerabilities demands security initiatives to **“cover all elements that is a reason for the vulnerability & ensure accuracy”** of protection measure

“Persistent effectiveness of control measures” requires effective tactical governance mechanisms

“Expanding compliance regimes” emphasize a need of building demonstration capabilities out of security initiatives

Specialized treatment to the disciplines

Strategic, tactical & operational view of the disciplines

Vigil over recent approaches, understandings & trends

Complete visibility over security

Coverage & Accuracy of security initiatives

Tactical governance mechanisms

Demonstration Capabilities

DSF[©] -Basic Rationale

Should reflect “**evolution of security**”, & relate to “**current understanding & approaches, trends**”

- Market Research reports,
- Leading global practices,
- Technology trends
- Interaction with global organizations & institutes in security

“**Strategic, tactical and operational**” understanding of security & its disciplines

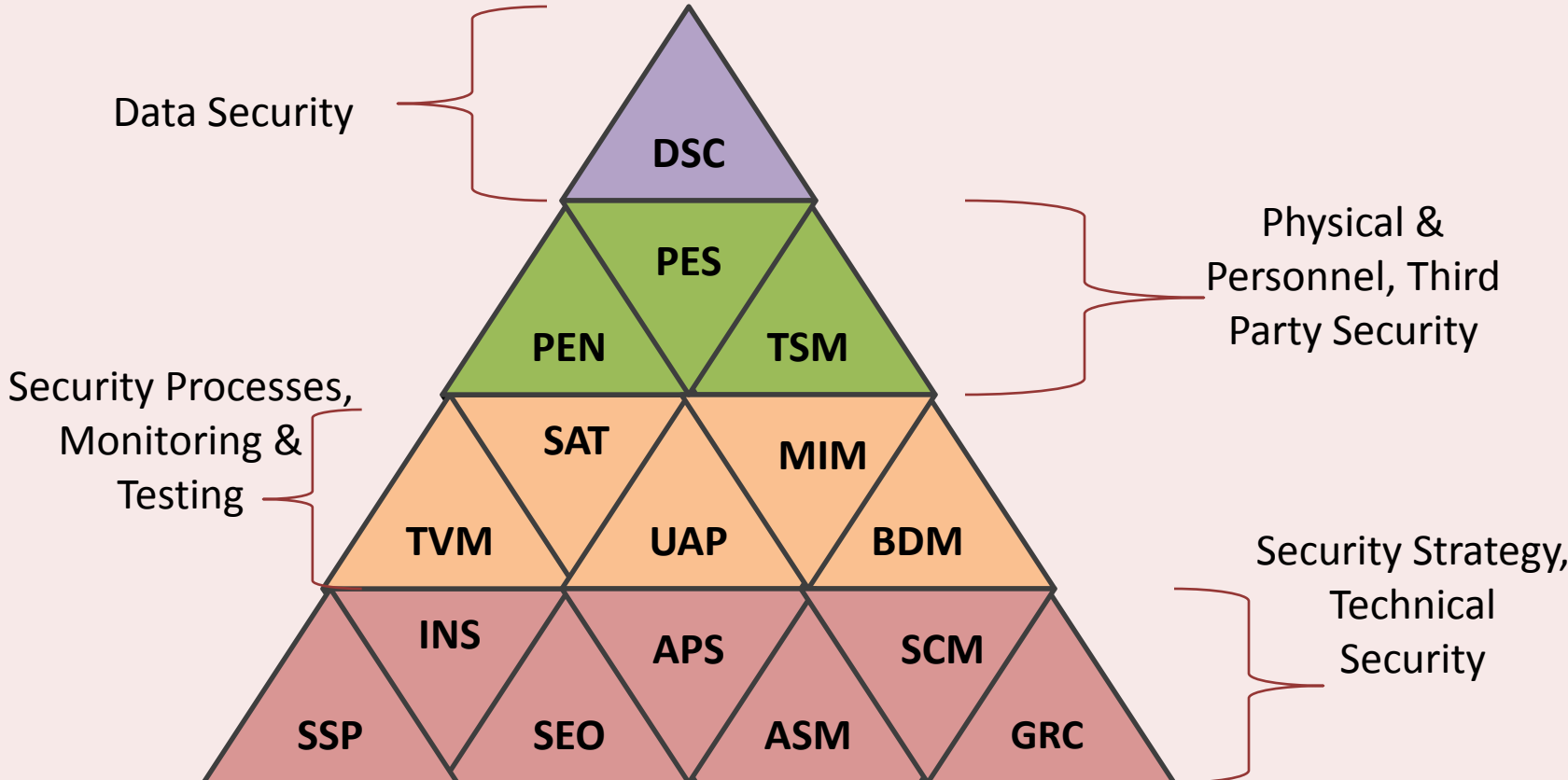
“**Focus on emerging disciplines**”, and where “**momentum of security**” is concentrated- APS, BDM, MIM etc

“**Aligning**” the security initiatives “**to end goal**” of data security. This ensures “**compliance to all emerging data protection regulations**”

Represents expanding security **profession-**

- Organization’s layer -strategy, tactical, operational)
- Discipline–Application, Infrastructure, data etc
- Technology - technology offerings, products
- Service services offering, ESPs

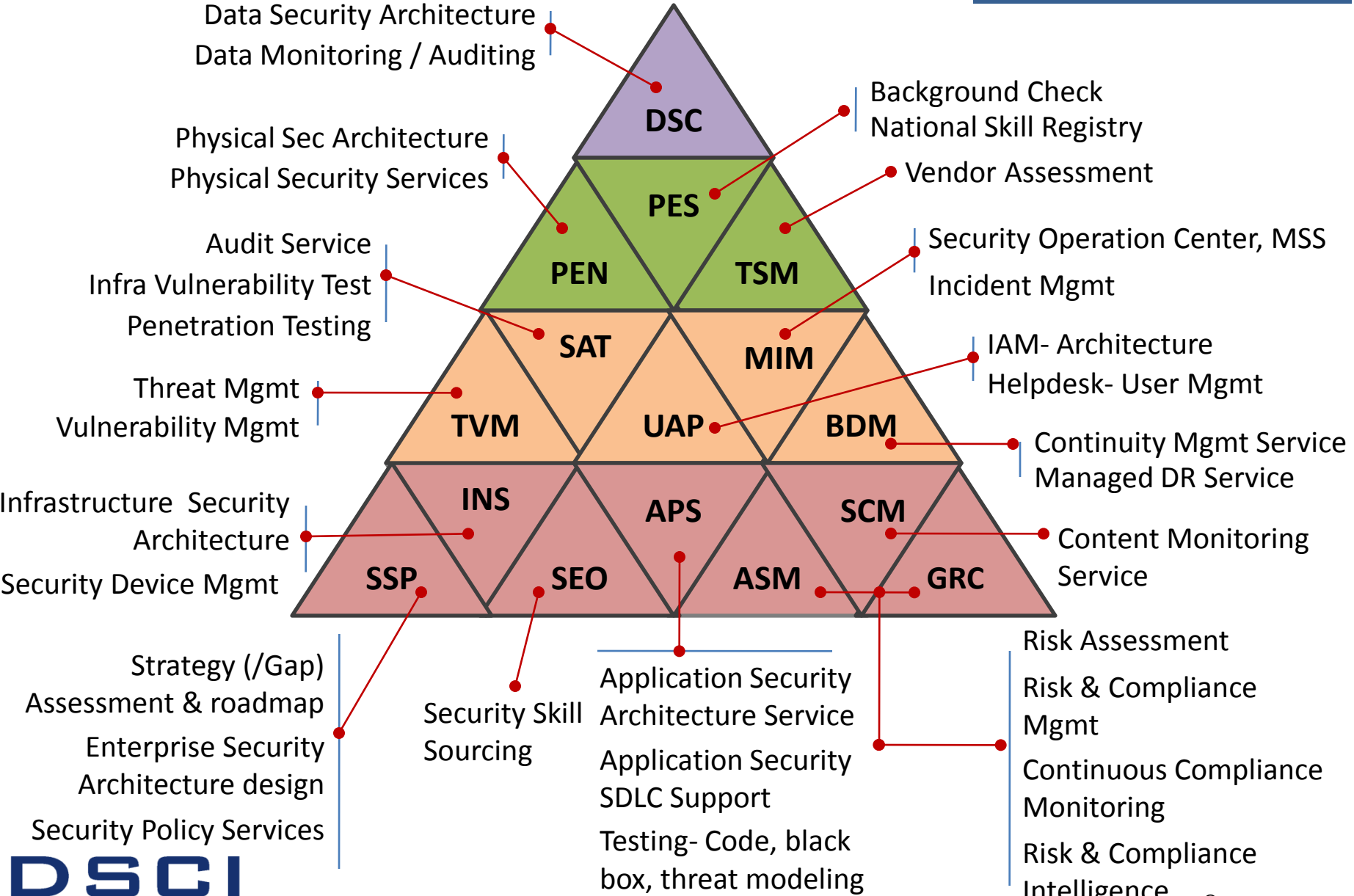
DSCI Data Security Framework



SSP – Security Strategy & Policy	SEO – Security Organization	ASM – Asset Management	GRC – Governance, Risk & Compliance
INS – Infrastructure Security	APS – Application Security	SCM – Security Content Management	TVM – Threat & Vulnerability Management
UAP – User, Access & Privilege Management	BDM – Business Continuity & Disaster Management	SAT – Security Audit & Testing	MIM – Monitoring & Incident Management
PEN – Physical & Environmental Security	TSM – Third Party Security Management	PES – Personnel Security	DSC – Data Security

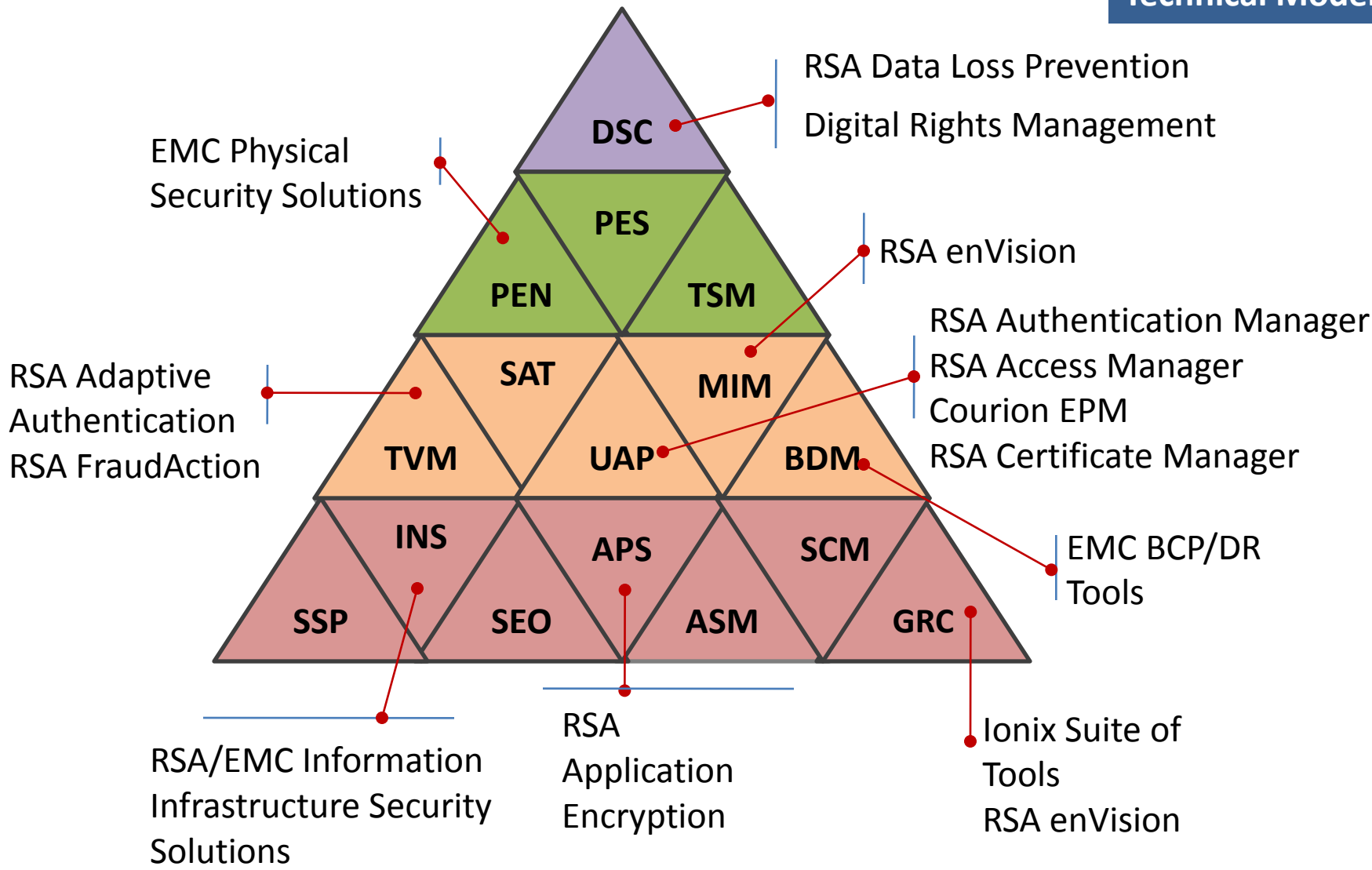
DSCI Best Practice Framework

Security Services Model

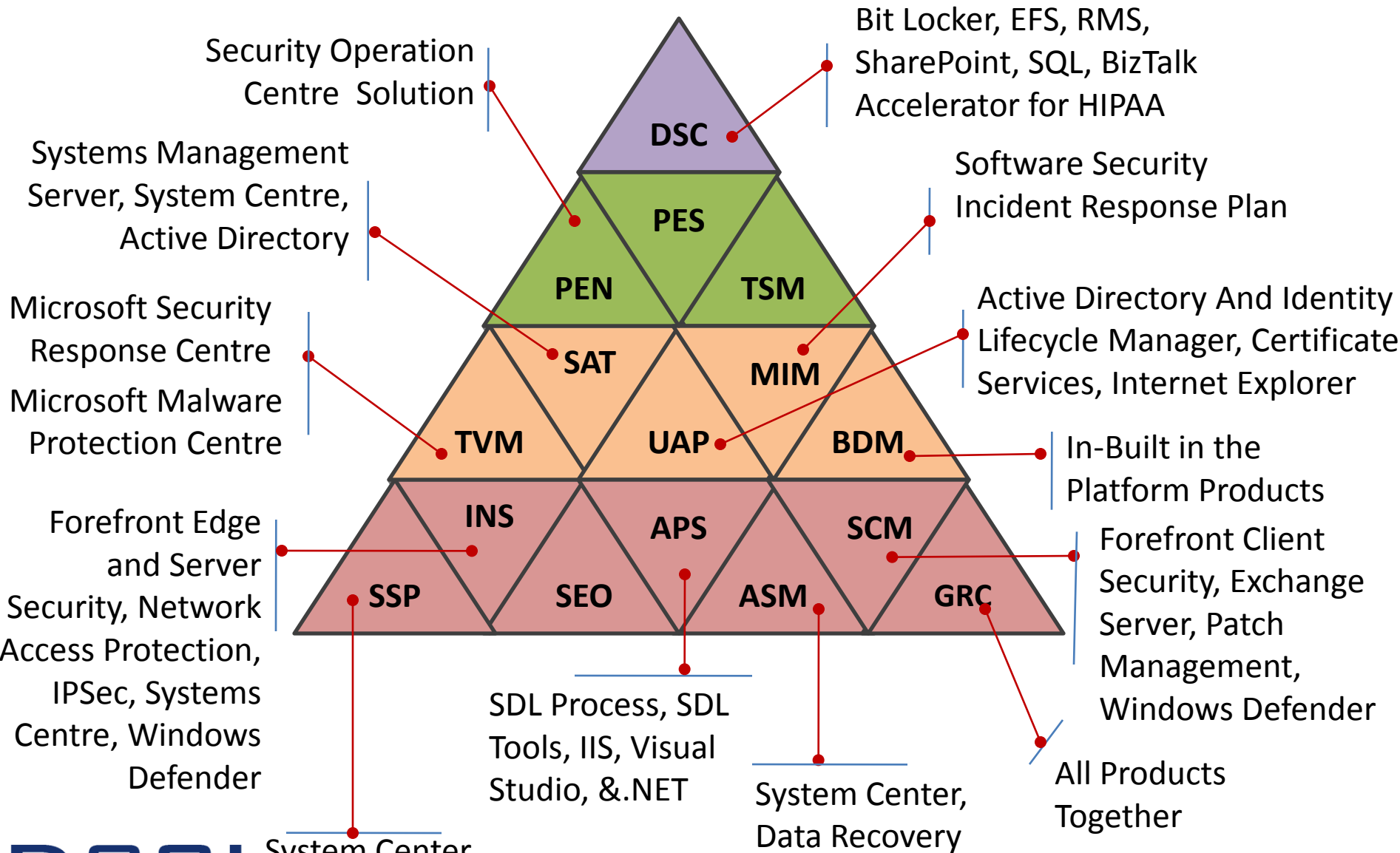


DSF[®]-Mapping With RSA Security Solutions

Technical Model



DSF[®]-Mapping With Microsoft Security Solutions



Best Practices

APS

Application Security Function

- Dedicated function for APS
- Roles & responsibilities APS function
- Responsibility of associated functions & LOBs
- Standards & Guidelines
- Resources and efforts for APS
- Collaboration platform

Protection at Application layer

- Visibility over current protection level
- Flow analysis, threat modeling and penetration testing
- Focusing real risk, proportionate measures
- Integration of protection capabilities with IT & Incident Mgmt

Application Security Strategy

- Enterprise application portfolio
- Criticality of each application
- LOBs involvement
- Catalog of all compliance requirements
- Visibility over application exposure
- Security ratings to all applications
- Application security architecture
- A strategic roadmap for APS
- APS program coverage

Security Intelligence

- APS specific information mgmt
- APS Knowledge mgmt

Security in SDLC processes

- A catalog all of ALM elements
- Technical & process design for integration
- Responsibility & accountability for integration
- Involvement of ADM function
- Tools, techniques & services
- Responsibility of support functions
- Securing packaged applications
- Metrics for application vulnerability mgmt

Application Security Testing

- APS testing requirements
- Test management processes
- A catalog of testing services
- Resources and skills
- Response to emerging threats
- APS testing tools and techniques
- Test results management

Maturity of Application Security Function

Comprehensiveness & accuracy of coverage	Integration with SDLC process
Visibility over application security activities	Tools & technology direction
Adequacy of protection	Involvement of ADM function
Intelligence over application security information	Adequacy of resources and skills
Architectural treatment to application security	Responsiveness to threats
Alignment with overall security strategy	Compliance demonstration

DSF[©]- Document Ecosystem

Implementation
Methodology

Guidance note on
implementation

Compilation of **strategic options** for baseline improvement- approaches, technology, services, tactical steps, process, best practices



Assessment methodology
Maturity Assessment



Micropractices- address specific challenge

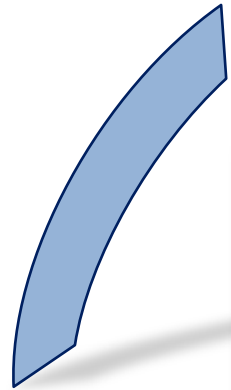


Forensic Investigation Practices

Best Practices compilation under 16 disciplines



DSCI Approach to 16 best practice disciplines



Document Ecosystem

Agenda

1 Best Practices

- Approach towards best practices
- Best Practices- Security Principles
- DSCI Security Framework (DSF[©])
- DSF[©]- Services and Technical Model
- Best Practices
- Document Ecosystem

2 DSF[©]- Forensic Practices

- What is Forensic
- Computer Forensic
 - Building Forensic capability
- Investigation Approach
- Cyber Criminal, Anti-Forensic
- Computer Forensic for IT/ITES

Transborder Data Flow- What and how

- Personally identifiable Information
- Personal financial information
- Business strategy documents, board presentations, MoMs etc
- Business plan, marketing plan, proposals, RFPs, presentations etc
- IPR data
- Credit Card Numbers and its authorization information
- Critical design, images, and diagrams
- Application design, product design
- Databases, data files, spreadsheets,
- Project plans, project reports etc
- Source code, libraries and reusable components etc.
- Financial information- payroll, receipts and expenditure, transaction logs and reports
- Knowledge assets, research and market analysis reports
- Media files

Access to application hosted at client side

Application hosting at outsource service provider

Access to underlying systems and servers

Direct sharing of the data for processing

Access to collaboration tools- SharePoint, mails

Access to development, test and production systems

Test data sharing

Outbound/ inbound calls to/ from client and client customers

Transborder Data Flow- Security Concerns

Call Center data theft

Trojan infection

Social Engineering

VOIP threats

Personal Information Leak

Compromised Credit Card details

Network Penetration

Botnets

Hack into servers

Credential stealing

Malware propagation

Network Sniffing

Unauthorized access

Man-in-middle attack

WLAN- Compromise

Storage Leakage

Corporate data loss

Database worms

Complex regime of Data Protection Legislations...us

Computers & Communications

- Computer Fraud and Abuse Act of 1986 (CFAA)
- The Electronic Communications Privacy Act (1986)
- Telephone Consumer Protection Act of 1991
- Communications Opportunity, Promotion and Enhancement Bill – 2006 COPE
- Telecommunications Act of 2005
- Wireless Communications and Public Safety Act (1999)
- Cable Communications Policy Act of 1984
- Cyber Security Enhancement Act of 2002
- Cyber Security Act 2009
- U.S. Safe Web Act

Children's Privacy

- **Children's Online Privacy Protection Act – 1998 (COPPA)**
- Children's Internet Protection Act of 2001 (CIPA)
- Children's Online Protection Act of 1998 (COPA)

Financial Information

- **Gramm-Leach-Bliley Act (1999)**
- Fair Credit Reporting Act (1970)
- Fair and Accurate Credit Transactions Act (2003)
- Right to Financial Privacy Act (1978)
- **Federal Trade Commission Act**
- Taxpayer Browsing Protection Act (1997)
- Electronic Funds Privacy Act (EFTA)

Privacy of Government Collections

- Census Confidentiality Statute of 1954
- **Freedom of Information Act - 1966 (FOIA)**
- **Privacy Act of 1974**
- Computer Security Act of 1987
- Homeland Security Act 2002
- US Patriot Act 2001
- E-government Act of 2002
- Federal Information Security Management Act of 2002 (FISMA)

Health / Medical Records

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- 21 C.F.R

Miscellaneous Records and Activities

- Administrative Procedure Act
- **Family Education Rights and Privacy Act (1974)**
- Privacy Protection Act of 1980
- Video Privacy Protection Act of 1988
- Employee Polygraph Protection Act of 1988
- Driver's Privacy Protection Act of 1994
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
- Do-Not-Call Implementation Act of 2003
- Americans with Disabilities Act (ADA)
- Consumer Credit Reporting Reform Act of 1996 (CCRRA)

History of Forensic

1248 C.E.
Hi DuanYu
*"The Washing
Away of Wrongs"*

1892 C.E.
*Fingerprint
Identification*

1921 C.E.
*Polygraph
Test
Developed*

1930 C.E.
*First Physical
Forensic Lab
Established*

1950 C.E.
*First Computer
Developed
(ENIAC)*

1984 C.E.
*Computer
Forensic
Experts*

1989 C.E.
*First Person
Indicted
Under Title 18
Section 1030
(*"Morris"*)*

1991 C.E.
*FBI CART
Team
Established*

1996 C.E. DNA
*Evidence First
Used at
Trial in U.S.*

2002 C.E.
*FISMA Mandates
Incident
Response
Capabilities*

Ref: First Responder Guide to Computer Forensics, CMU

What is Forensic?

Forensics is the process of using scientific knowledge in the collection, analysis, and presentation of evidence to the courts.

..... *The word forensics means “**to bring to the court.**”*

Computer forensics – “**recover, analyze and present computer based material**” in such a way that it is “**useable as evidence in a court of law**”



While strong **cyber defense** is essential, **no defense is perfect**



Cyber forensics, “the art and science of extracting data from digital media.”



Cyber defense uses cyber forensics to identify threats and respond to incidents

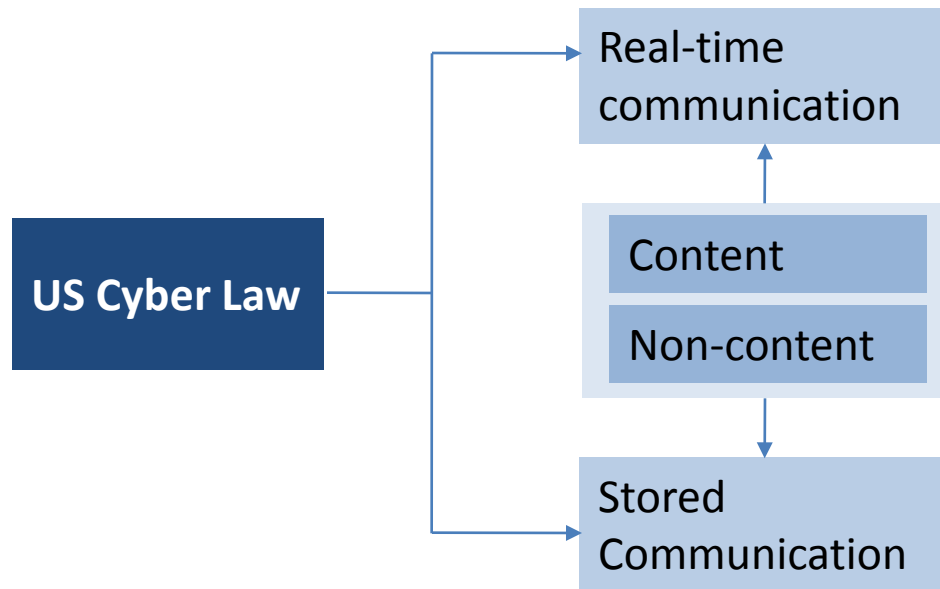
Legal Governance- Retention & Monitoring

U.S. Statutory Law

18 U.S.C. §§ 2510-22 Wiretap Act

18 U.S.C. §§ 3121-27 Pen/Trap and Trace

18 U.S.C. §§ 2701-12 Stored Electronic Communication ActReal



ITAA, 2008- Interception or Monitoring

Intermediary to provide facilities

Interception or monitoring or decryption of any information generated, transmitted, received and stored in computer system

Intermediary to designate officers to receive & handle requisition

Designate an officer to receive requisition and another to handle such requisition

To provide all facilities, cooperation, and assistance for interception or monitoring or decryption

Maintenance of records

What Information? Whose information? To whom information disclosed?

Decryption key holder to disclose key or provide decryption assistance

If decryption direction or a copy handed over to the key holder

- (i) Disclose the decryption key; or
- (ii) Provide the decryption assistance

Computer Forensic

HIPAA, SOX, California-1798
 Data breach notification
 Legal Governance- retention, monitoring & collection
FFIEC Guidance- Banking Security

Legal Regime

Rising Cyber Crime



Cyber Forensic



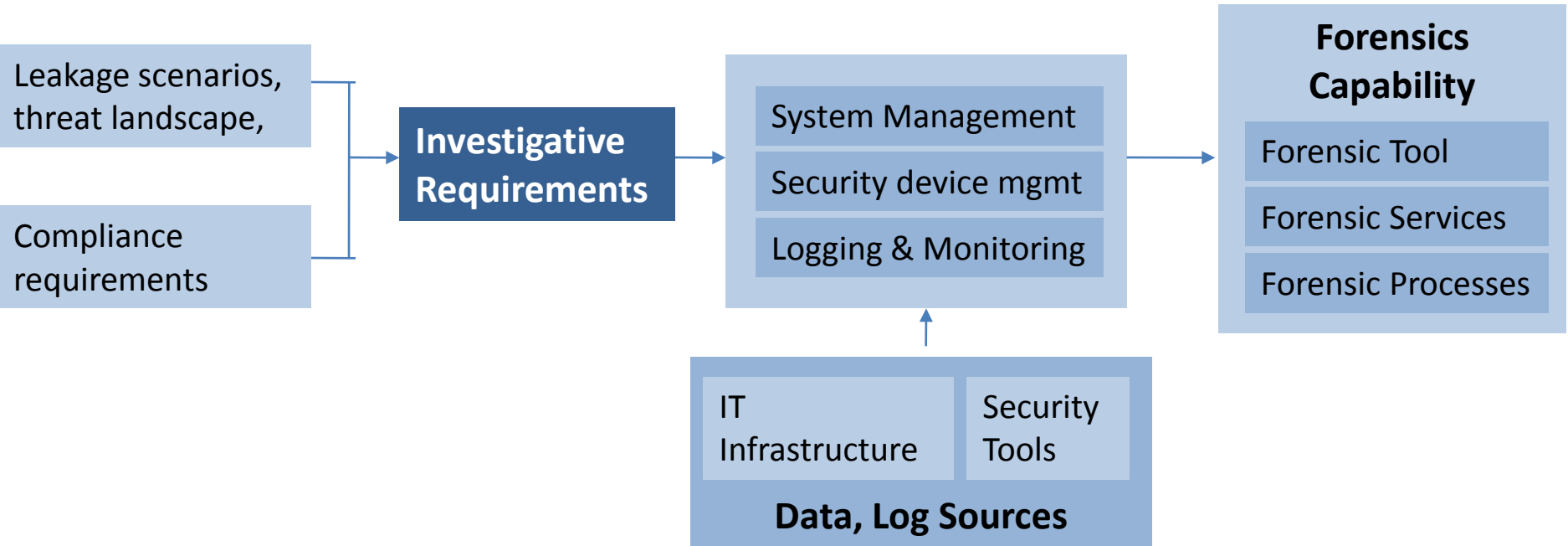
Forensic Sources

Server, Workstation hard drives
 Log files Application data
 Security tools Portable devices

Result of Internet-committed online
 Old-style crimes-use hi-tech, going online
 Rising concern of security of data
 Increased online fraud

Tools	Cyber Forensic	
	Fraud Management	
	eDiscovery	
	Case Management	
	Litigation Support	
	SIEM, IAM	
Process	Collect	Preserve
	Analyse	Report
	Chain of Custody	
Services	Investigation	
	Data Discovery	
	Forensic Imaging	
	Forensic Audit	
	Managed Services	
Skill	SANS- GCFA	

Building Forensic capability



Enterprise Forensic capability: Best Practice

Who collected the evidence?

How and where was it collected?

Who took possession of the evidence?

How was the evidence stored and protected while in storage?

Who took it out of storage and why?

Create and follow a **specific sequence in conducting a forensic investigation** to ensure the best possible results and to provide essential **transparency**.

Ensure that the **collection of data** is necessary and **legally defensible**.

Preserve original **evidence** in a safe, physically controlled environment, conducting all analysis using a working copy.

Seek outside **expert help** if your enterprise is inexperienced in forensic technology.

Enterprise Forensic capability: Best Practice

Overall plan or strategy for **investigation requirements** that takes into account both the technical and policy issues.

Do not allow the use of **nonstandard encryption** on workstations. If encryption is needed for laptops (and it *is generally needed*), **choose a corporate standard product** and enforce a **standard configuration**.

Ensure that authorized **administrators have the ability to decrypt** the drives on those workstations, so that routine maintenance, clear text backup, data recovery and remote investigations are possible.

Institute a **policy of retaining the hard drive of departing employees** who are leaving **especially sensitive jobs**, or who are **leaving under controversial** circumstances.

Before **redeploying a PC or hard drive**, use **data-wiping mechanisms** to completely remove all data.

Develop an "**investigative protocol**" (**process**) specifying the types of investigations that will be performed by which people and under what circumstances. This policy and process document must be approved by the managers of the corporate, security, legal, IT and HR departments. This should be in place before performing investigations.

Forensic Investigation: Approaches

Forensic Practice: “evidence in a court of law”

demands —
robustness,
accuracy
process documentation



Traditional Investigation

Primary evidence is an original hard drive
Sealed in an evidence bag
Forensically duplicated
Stored in a locker



Sending staff to collect evidence is expensive, it makes target system unavailable
Investigators (internal or external) are spending too much time (and money) travelling



Remote Forensic Management

Agent on the target system
Surveillance over a period of time
Operate on the desktop in a stealth mode

Guidance Software, AccessData, ProDiscover, Paraben, SMART from ASR Data, OnLineDFS, MacQuisition CF

Criminal Profiling

Entity extraction: the process of identifying names, places, dates, and other words and phrases that establish the meaning of a body of text—is critical to software systems that process large amounts of unstructured data coming from sources such as email, document files, and the Web. By locating certain types of phrases and associating them with a category, applications such as text analysis software can perform functions such as concept extraction.

Clustering technique: group data items into classes with similar characteristics to maximise or minimise interclass similarity- for example, to identify suspects who conduct crimes in similar ways or distinguish among groups belonging to different gangs (Chau, Xu & Chen, 2002).

Deviation detection: researcher deploy this technique to detect fraud, network intrusion detection, and other crime analysis that involve tracing some activities which can be appear sometimes to be abnormal.

Classification: finds common properties among different crime entities and organises them into predefined classes. This technique has been used to identify the

Ref- Examination of cyber criminal behaviour,

H. Jahankhani, Ph.D. , Ameer Al-Nemrat University of London, UK

Case Management tools

Financial services market

Investigate any events that may be indicative of money laundering

Fraud Management

Actimize, ACI worldwide, Aithent, Chordiant, Digital Harbor, Fair Issac, Loss Control Solutions Syfact

Law enforcement

Case Management

Records management system

Compudyne; Crimesoft; CrimeCog; Denali; Global Fraud Solutions; ISYS Search; Spillman; Pen-link New World, Sungard

Legal

Used by lawyer community

Thomson elite Law Manager, Elite Case Manager

Retail case management

track both internal & external sources of fraud

Aspect Loss Prevention, Datavantage, Epicor (CRSLoss Prevention), March Networks (Trax Retail) and Retail Expert

Corporate security

Physical security- recording loss & crime events

Aithent, Archer Technologies, Axcelia, D3, PPM2000 and Zylab

Anti-Forensics

Forensics

Data Recovery
Data Parsing
Data Analysis

Anti-Forensics

Defeat the tool,
defeat the analyst



Reduce the quantity & quality of
evidential data



Data Destruction
Data Contraception
Data hiding



Tools

Necrofile
Klismafile
Metasploit anti forensic toolkit
haxh - hacker's shell
Toy backdoor in AWK
sqleez

Thank You