Data Loss Leakage/Prevention - Fundamentals

- Fundamentals.
- Regular Expressions.

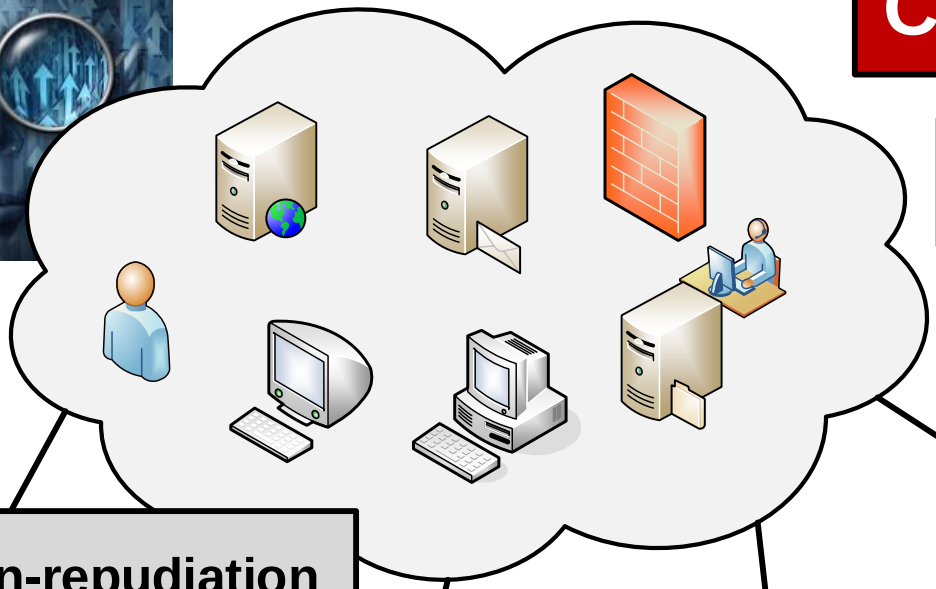
http://asecuritysite.com/dlp

Author: Prof Bill Buchanan

Data Loss Detection/ Prevention

Introduction

Author: Prof Bill Buchanan



C **Confidentiality**
Encryption, firewalls, passwords...

I **Integrity**
Checksums, logs, hash values ...

A **Availability**
Backups, failover, UPS ...

Non-repudiation
Users cannot deny that an action actually occurred

Authentication
Verification that users identify themselves correctly

Access control
Only valid users are allowed

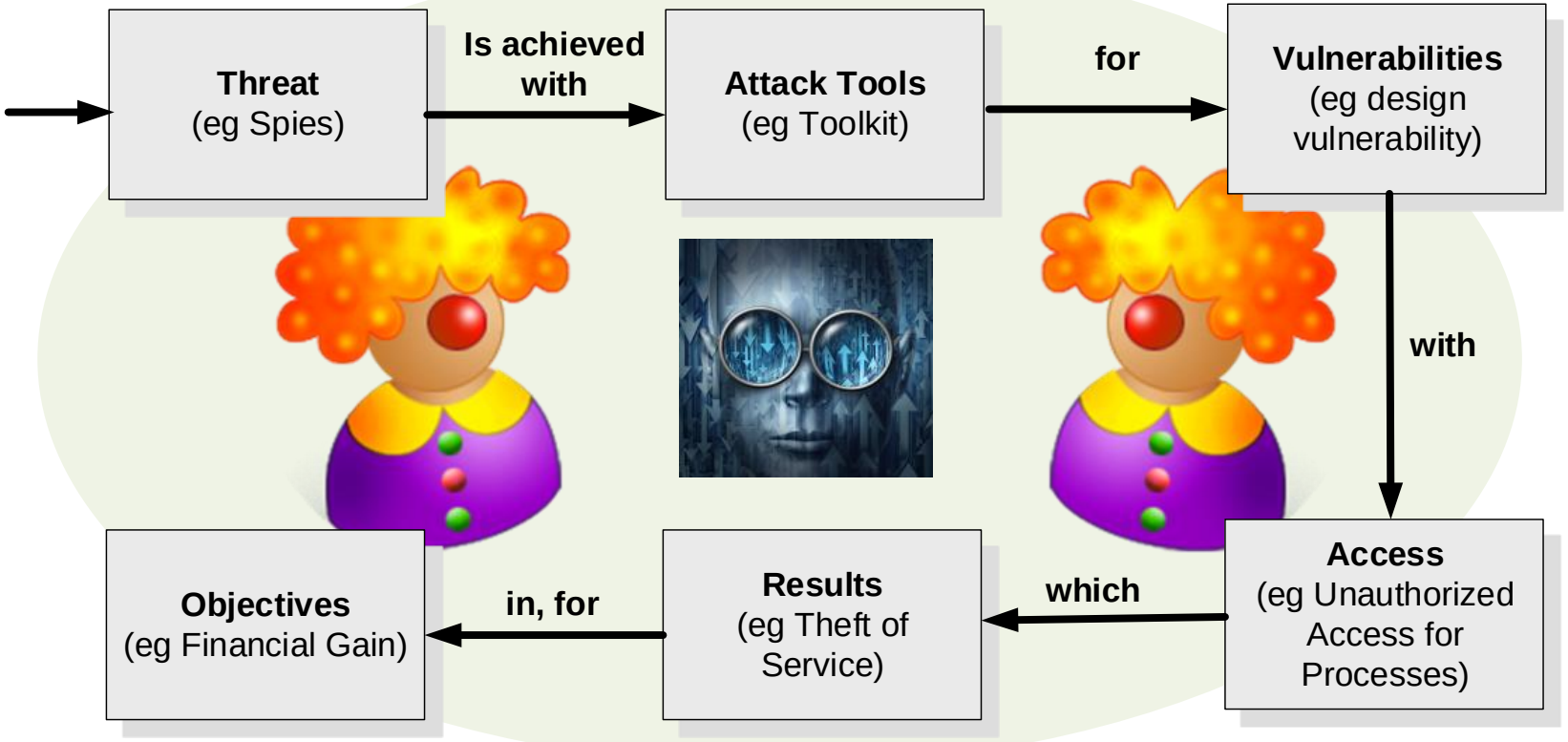
Privacy
Users has control of information to them and how it is exposed

Audit
Recording of authorized actions

A Threat:
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:
- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:
- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.

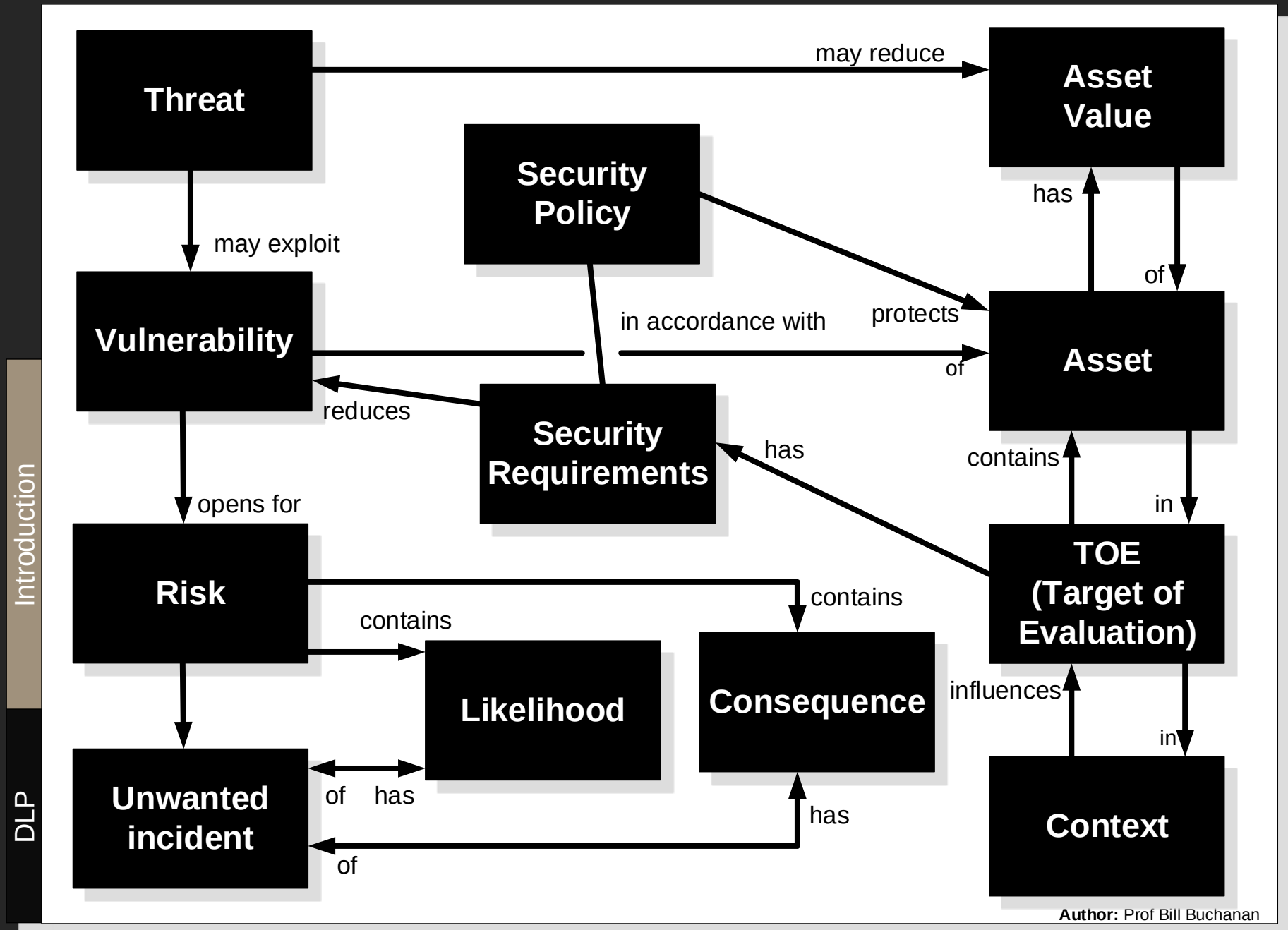


for Objectives:
- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

which Results in:
- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:
- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan



Security relationships (CORAS)

Aims/objectives of the organisation

Audit/compliance

Legal, moral and social responsibilities

Technicial feasability

External audit

Policy Definition

Policy Implementation

Evaluation

Verification

Audit

Operating System rights

Firewall rules

Domain rights

Event log definition

Application rights

Author: Prof Bill Buchanan

IT Policy
Mitigation
Virus/Threat
Firewall
Update
management

Protect

Deter

Security Policy

General Policy
Organisational
role
Disaster recovery
Business
continuity

Audit/
verify

Log

**User
Policy**
Passwords,
Internet usage,
System usage

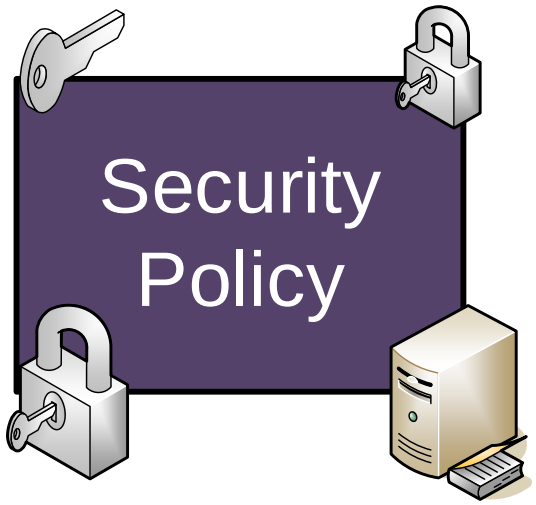
React

Recover

Introduction

DLP

Author: Prof Bill Buchanan



Why?

- **Gramm-Leach-Bliley Act** (US reg to allow banks, security firms and insurance companies to merge/ share data)
- **US Health Insurance Portability and Accountability Act (HIPAA)**.
- **Security and Freedom through Encryption (SAFE)**. define the rights of US Citizens to the use of encryption without key escrow.
- **Computer Fraud and Abuse Act**. Reduce hacking by defining penalties against incidents.
- **Privacy Act of 1974**. Respects the rights of the individual unless permission is given.
- **Federal Information Security Management Act (FISMA)**. Aims to strengthen US federal government security by the use of yearly audits.
- **Economic Espionage Act of 1996**. Aims to criminalise the misuse of trade secrets.
- **Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT)**. Permits the government to monitor hackers without a warrant.
- **Sarbanes-Oxley (SOX) Act**. Relates to transparent account and reporting of companies

Data Loss Detection/ Prevention

Data Leakage

Author: Prof Bill Buchanan

Patient Information

Financial Information

Intellectual Property (IP)

User activity

Credit card details

Data Leakage
"accidental or unintentional distribution of private or sensitive data to an unauthorized entity"

System config

Usernames/ passwords

User activity

Customer details

Data Leakage

DLP

Data Leakage

DLP

Direct Losses

Violation of regulations (fines, etc).
Customer compensation.
Investigation costs.
Litigation.
Reduced sales.
Restoration fees.

FSA hit **Zurich UK** with a fine of £2.275m for loss of 46,000 customers' personal details (2010).

NHS trust fined £325,000 by a data protection watchdog after highly sensitive files of tens of thousands of patients, including details of HIV treatment (2012).

Data Leakage

"accidental or unintentional distribution of private or sensitive data to an unauthorized entity"

Target – credit card loss of over 70 million customers – profit drop 50%

Indirect Losses

Share price fall.
Company reputation.
Customer loss of faith.
IP Loss to competitors.
Brand reputation.

Data Leakage Losses

Standard security methods

Firewalls.
IDSs.
Anti-virus.
Thin-clients.
User/customer training.
Polices.
Domain restrictions.

"systems focus on standard fingerprints and/or rules for detection"

Encryption and Access Control

Strong device control.
Encryption.
Rights Management System (RMS).

"systems that prevent access from unauthorized entities"

Data Leakage Detection and Prevention

Data Loss Prevention Systems

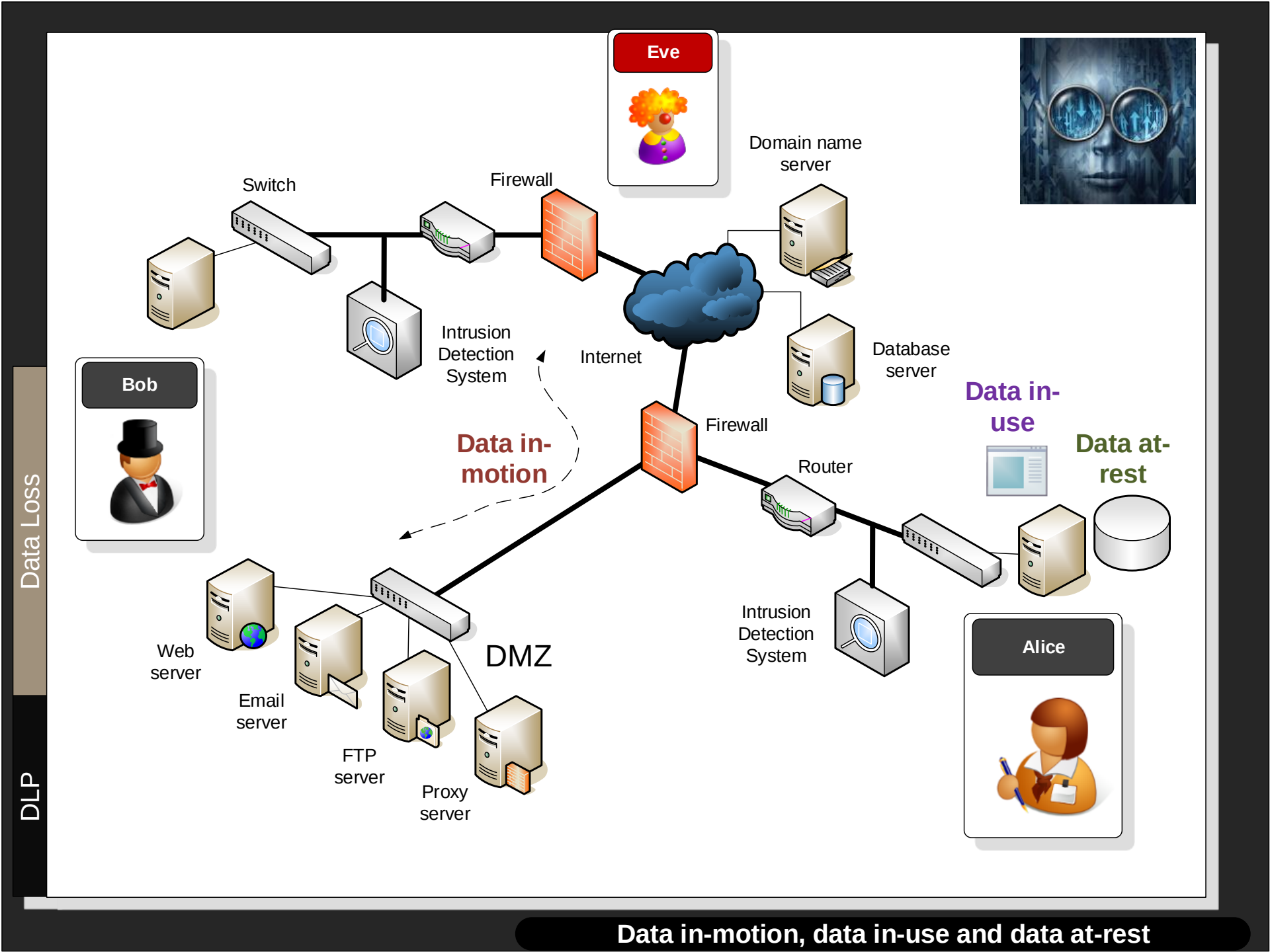
Network traffic scanning ("Data in-motion")
Application scanning ("Data in-use")
Storage scanning ("Data at-rest")

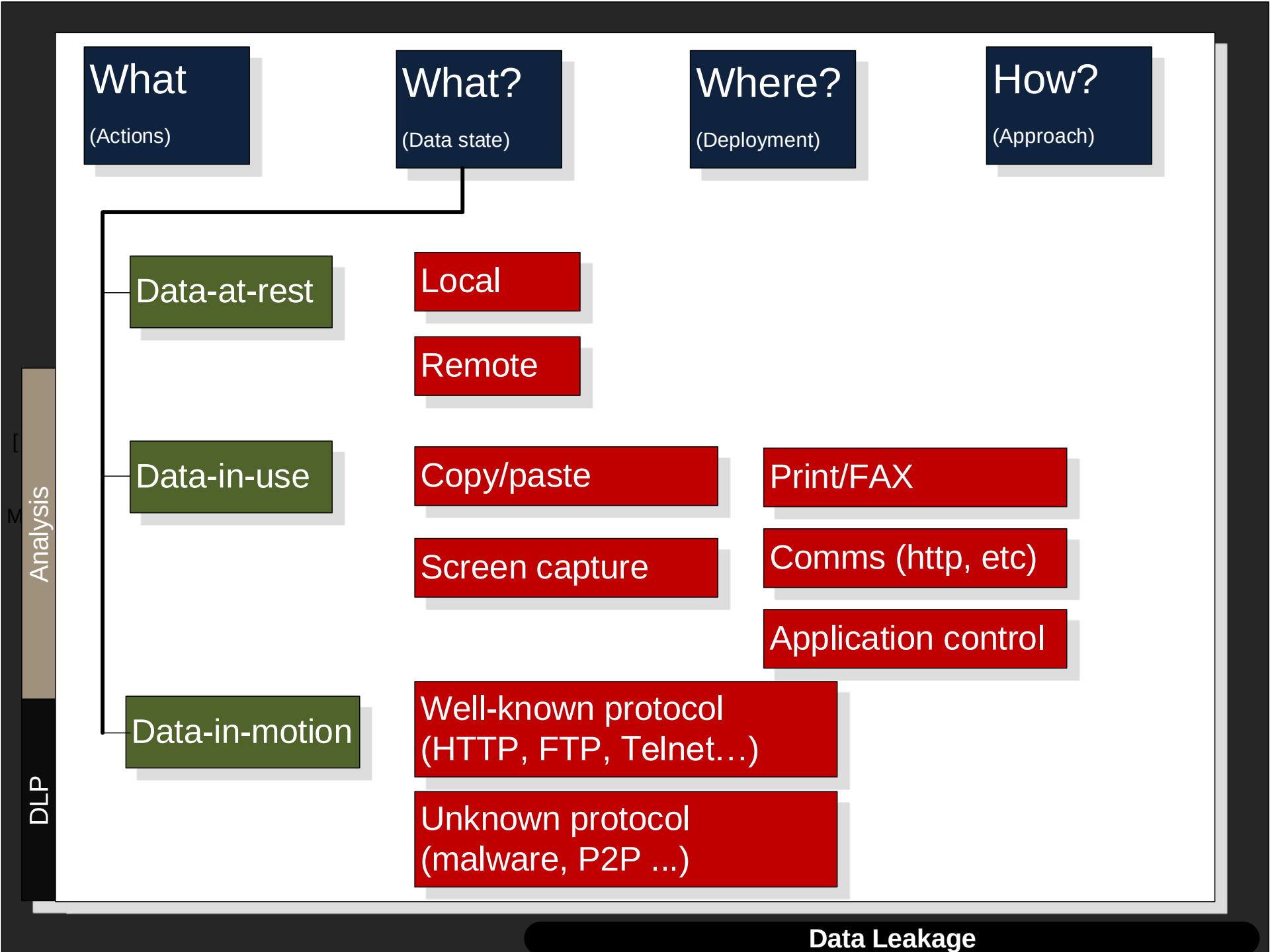
"systems that monitor and enforce polices on fingerprinted data"

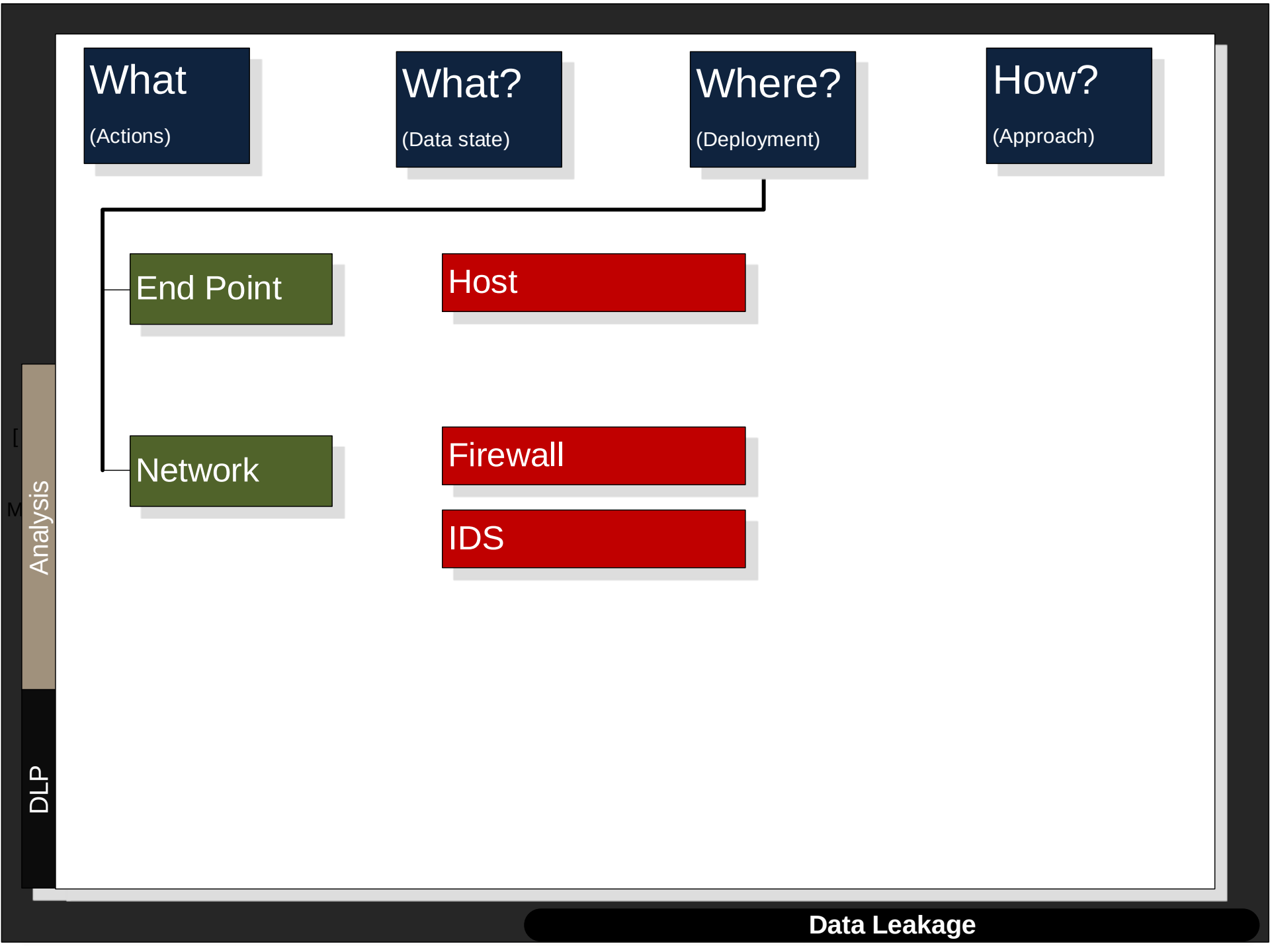
Advanced Security/ Intelligent Methods

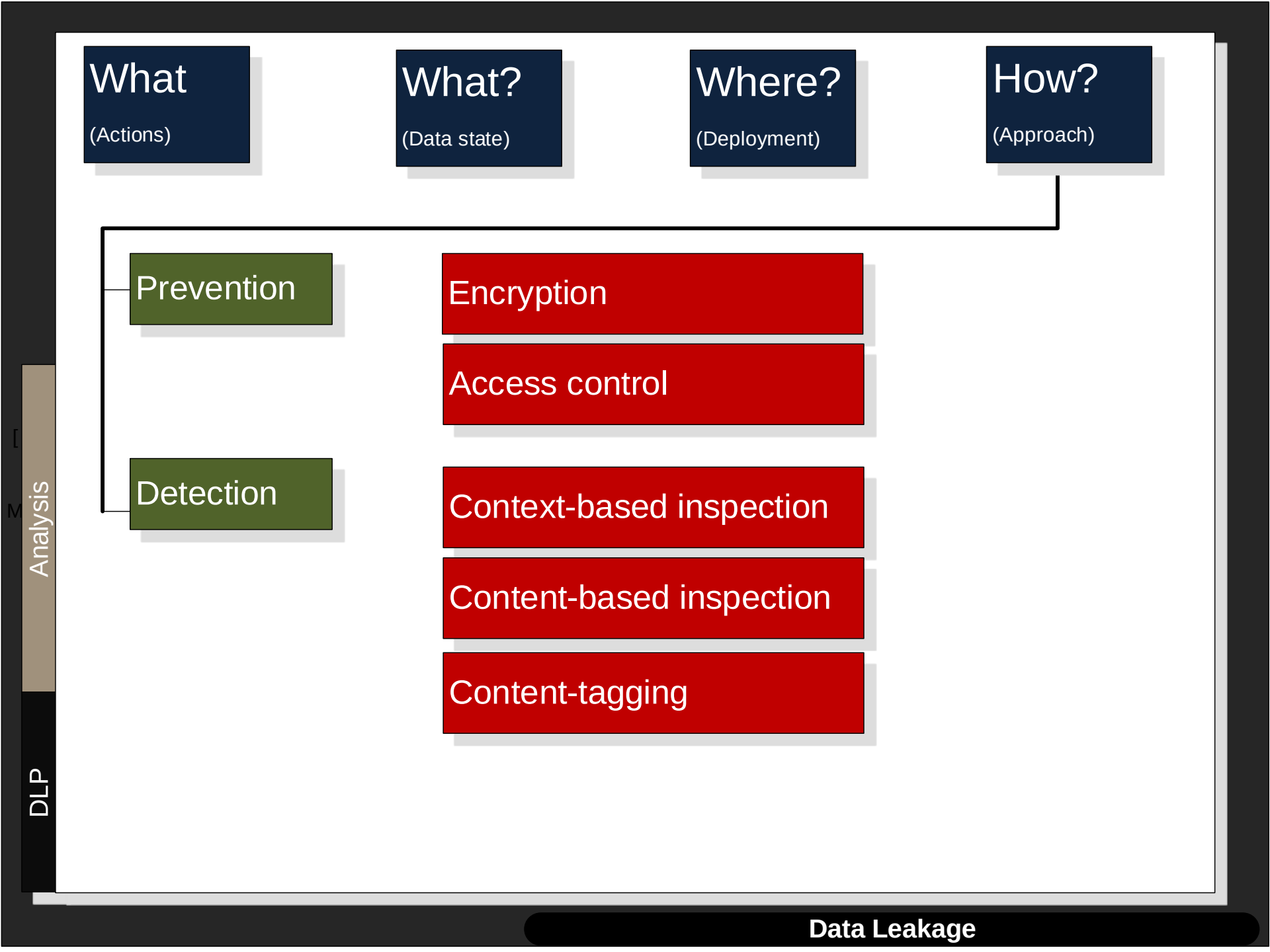
Honeypots.
Anomaly detection.
Activity-based verification.

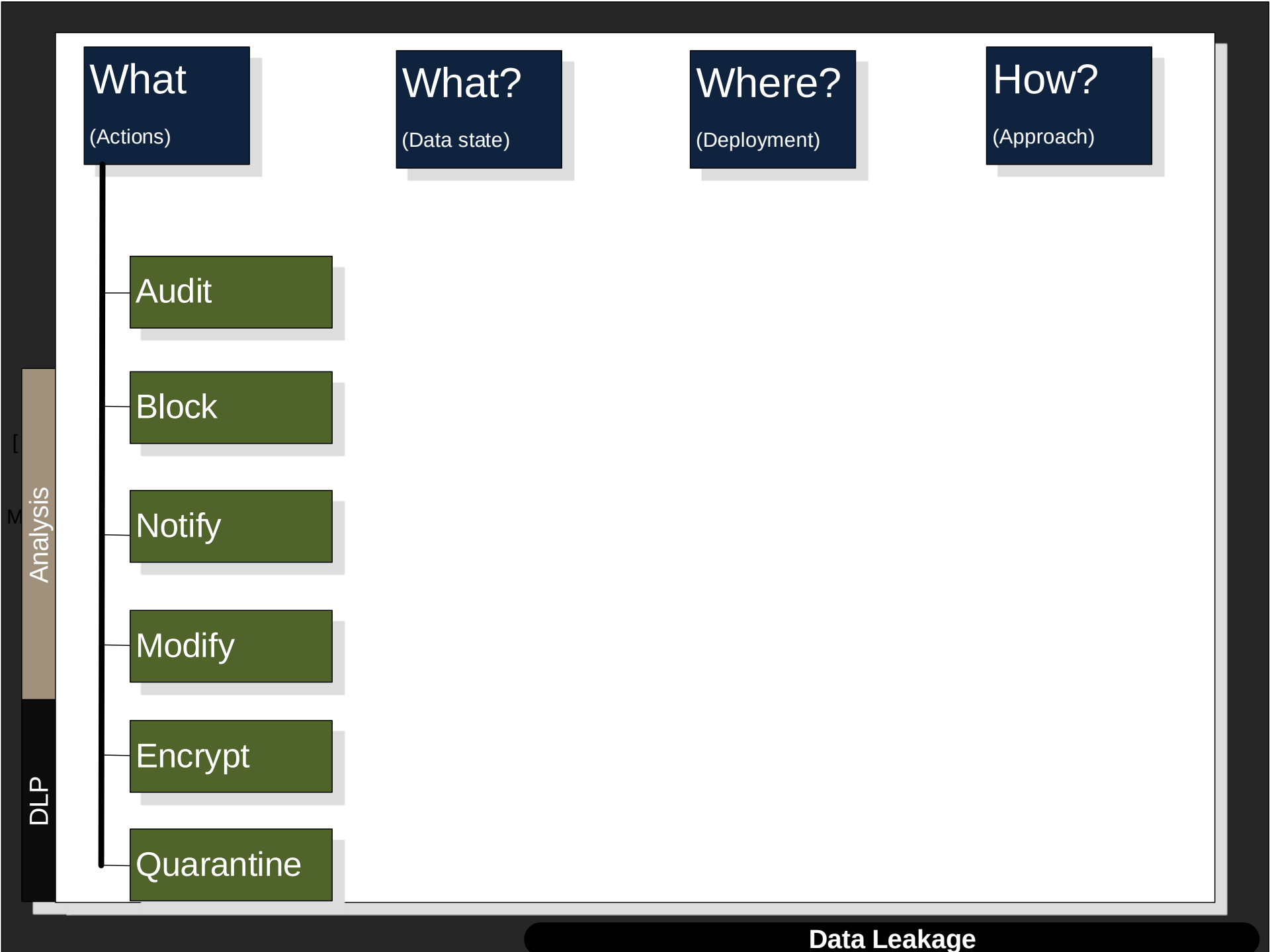
"systems that use: machine-learning; temporal reasoning; activity-based verification (eg key stroke analysis); abnormal detection; or entrap malicious activity)"


Eve
Domain name server
Switch
Firewall
Intrusion Detection System
Internet
Database server
Bob
Data in-motion
Firewall
Data in-use
Data at-rest
Router
Intrusion Detection System
Alice
Web server
Email server
FTP server
Proxy server
DMZ
Data Loss
DLP
Data in-motion, data in-use and data at-rest


What
(Actions)
What?
(Data state)
Where?
(Deployment)
How?
(Approach)
Data-at-rest
Local
Remote
Data-in-use
Copy/paste
Print/FAX
Screen capture
Comms (http, etc)
Application control
Data-in-motion
Well-known protocol
(HTTP, FTP, Telnet…)
Unknown protocol
(malware, P2P ...)
Analysis
DLP
Data Leakage


What
(Actions)
What?
(Data state)
Where?
(Deployment)
How?
(Approach)
End Point
Host
Network
Firewall
IDS
Analysis
DLP
Data Leakage

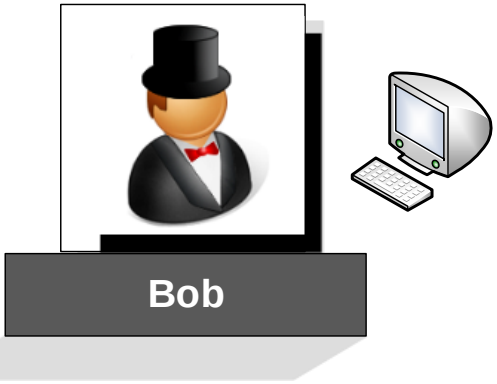

What
(Actions)
What?
(Data state)
Where?
(Deployment)
How?
(Approach)
Prevention
Encryption
Access control
Detection
Context-based inspection
Content-based inspection
Content-tagging
Analysis
DLP
Data Leakage


What
(Actions)
What?
(Data state)
Where?
(Deployment)
How?
(Approach)
Audit
Block
Notify
Modify
Encrypt
Quarantine
Analysis
DLP
Data Leakage

Data Loss Detection/ Prevention

Data Formats

Author: Prof Bill Buchanan



13610163252

Octal

Hex

5e 20 e6 aa

Base-64

XiDmqg==

'A' 'B' 'C' 'D'

ASCII characters

01000001 01000010
01000011 01000100

Byte values

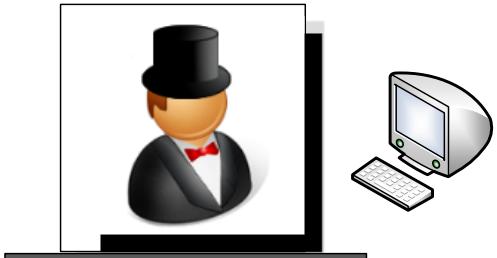
Encryption/
Encoding

01011110 00100000
11100110 10101010

^ æª

ASCII

Decimal	Binary	Oct
0	000	0
1	001	1
2	010	2
3	011	3
4	100	4
5	101	5
6	110	6
7	111	7



Bit stream

0101 1110 0010 0000 1110 0110 1010 1010

Hex

5 e 2 0 e 6 a a

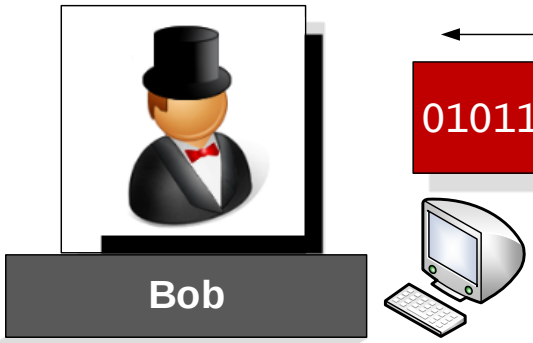
What is 0100111011110001?

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

0101 1110 0010 0000 1110 0110 1010 1010

24-bit width

010111 100010 000011 100110 101010 100000 = =



Bit stream

010111 100010 000011 100110 101010 100000

X I D m q g = =

Base-64

Val	Enc	Val	Enc	Val	Enc	Val	Enc
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

abc	24 bits	(4*6)	YWJj
abcd	32 bits	(5*6) + (2+4) + 12 bits	YWJjZA==
abcde	40 bits	(8*6) + (2+4) + 4 bits	YWJjZGU=

hello

MD5 5D41402ABC4B2A76B9719D911017C592

128 bits (32 hex characters)

SHA-1 AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D

160 bits (40 hex characters)

SHA-256 SHA-384 SHA-512

```
$ cat hello.txt
Hello
$ openssl md5 hello.txt
MD5(c:\hello.txt)=
5d41402abc4b2a76b9719d911017c592

$ echo -n "hello" | openssl md5
     (stdin)= 5d41402abc4b2a76b9719d911017c592
```

[character_group]	Match any single character in character_group Example: gr[ae]y – gray, grey
[^character_group]	Match any single character in character_group Example: gr[^ae]y – grby, grcy
[a-z]	Character range Example a, b, c … z
{n}	Matches previous character repeated n times
a{n,m}	Matches between n and m or a
\d	Matches a digit
.	Single character
(a | b)	Matches a or b
a?	Zero or one match of a
a*	Zero or more match of a
a+	One or more match of a
$	Match at the end
Escape:	\s (space)

Telephone: \\d{3}[-.]?\\d{3}[-.]?\\d{4}

444.444.2312

Year: [0-9]{4}

1961

test@home.com

Email: [a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]

5555-1234-3456-4312

```
Master:    5\\d{3}(\\s|-)?\\d{4}(\\s|-)?\\d{4}(\\s|-)?\d{4}
Am Ex:     3\\d{3}(\\s|-)?\\d{6}(\\s|-)?\\d{5}
Visa:      4\\d{3}(\\s|-)?\\d{4}(\\s|-)?\\d{4}(\\s|-)?\d{4}
```

1.2.3.4

IP: [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}.[0-9]{1,3}

Data Formats

DLP

RegEx

Data Loss Leakage/Prevention - Fundamentals

- Fundamentals.
- Regular Expressions.

http://asecuritysite.com/dlp

Author: Prof Bill Buchanan