



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

July 10, 2013



# ISOAG July 2013 Agenda

- |      |   |   |
|------|---|---|
| I.   | Welcome & Opening Remarks                       | Michael Watson, VITA                    |
| II.  | Data Loss Prevention                            | Rosario Igharas, Va529                  |
| III. | Undercover Clicker                              | Ed Miller, VITA                         |
| IV.  | UAC & DEP:<br>Protection Mechanisms for Windows | Bob Baskette, VITA                      |
| V.   | Upcoming Events & Other Business                | Michael Watson, VITA                    |
| VI.  | Partnership Update                              | Bob Baskette, VITA<br>Michael Clark, NG |

# Data Loss Prevention



Rosario Igharas, Director of Information Security  
July 10, 2013

# At a Glance.....



## The Virginia529 College Saving Plan is...

- An independent state agency
- An administrator of Internal Revenue Code §529 Qualified Tuition Programs
- The country's largest 529 plan with more than 2.3 million accounts and \$44B assets under management as of May 31, 2013

## Investment options:

- Virginia529 prePAID<sup>SM</sup>
- Virginia529 inVEST<sup>SM</sup>
- CollegeAmerica<sup>®</sup>
- CollegeWealth<sup>®</sup>



*Data Loss Prevention (DLP) is a system that is designed to detect potential data breach/data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while **in-use** (end-point actions), **in-motion** (network traffic) and **at-rest** (data storage) ~ Wikipedia*

## Confidential Data Types

- Customer Data
  - SSN
  - Credit Card Numbers
  - Protected Health Info
- Corporate Data
  - Financials
  - Merger and Acquisitions
  - Employee Data
- Intellectual Property
  - Source Code
  - Design Documents
  - Pricing

## Data Loss Prevention Drivers

- 1:400 messages contain confidential data
- 1:50 network files is wrongly exposed
- 4:5 companies lost data on laptops
- 1:2 companies lost data on USB drives

# Why DLP?

**DATA LOSS db**  
open security foundation

login | signup **SPONSORED BY**   
**CREDANT**  
We Protect What Matters

ABOUT SEARCH SUBMIT NEW PRIMARY SOURCES LAWS REPORTS STATS DOWNLOAD MAIL LISTS THE BLOTTER FRINGE SUPPORTERS

**Main** Latest Incidents Largest Incidents Most Discussed Incidents Recently Updated Incidents

<b>LOST MEDIA</b>	<a href="#">ID: 3209: Lost portable drive exposes 280,000 names, addresses and health information</a> Date: 2010-10-20 Records Lost: 280,000 Source: Inside Accidental Submitted by: kirniki Location: PA, US Organizations: Keystone Mercy Health Plan
<b>STOLEN MEDIA</b>	<a href="#">ID: 3210: Stolen digital camera containing newborn baby pics with id tags with names, addresses, dates of birth, medical insurance numbers</a> Date: 2010-10-19 Records Lost: Unknown Source: Outside Submitted by: kirniki Location: Little Rock AR, US Organizations: University of Arkansas for Medical Sciences
<b>FRAUD-SE</b>	<a href="#">ID: 3201: Temporary employee stole county workers names and Social Security numbers</a> Date: 2010-10-18 Records Lost: 30 Source: Inside Malicious Submitted by: Christine Location: Milwaukee WI, US Organizations: Milwaukee County Human Resources
<b>EMAIL</b>	<a href="#">ID: 3199: Third party contractor downloads patients medical details to USB then incorrectly emails the records to wrong person</a> Date: 2010-10-17 Records Lost: 1,500 Source: Inside Accidental Submitted by: admin Location: Dublin Fingal, IE Organizations: Health Service Executive
<b>WEB</b>	<a href="#">ID: 3197: File posted on public facing server exposes 3000 Social Security numbers</a> Date: 2010-10-16 Records Lost: 3,000 Source: Inside Accidental Submitted by: kirniki Location: Socorro NM, US Organizations: New Mexico Tech
<b>SNAIL MAIL</b>	<a href="#">ID: 3205: Financial documents of about 900 patients stolen from courier</a> Date: 2010-10-16 Records Lost: 900 Source: Outside Submitted by: pi3rce Location: Sacramento CA, US Organizations: University of California Davis, UltraEx Courier
<b>HACK</b>	<a href="#">ID: 3196: Hacked server exposes 106,884 Names, Social Security numbers and dates of birth</a> Date: 2010-10-15 Records Lost: 106,884 Source: Outside Submitted by: kirniki Location: Jacksonville FL, US Organizations: University of North Florida
	<a href="#">ID: 3194: Programming/mailing error exposes 6,299 Social Security numbers</a>

# Why DLP?

<b>SNAIL MAIL</b>	<a href="#">ID: 3194: Programming/mailling error exposes 6,299 Social Security numbers</a> Date: 2010-10-14 Records Lost: 6,299 Source: Inside Accidental Submitted by: kirniki Location: US Organizations: U.S. Department of Veterans Affairs, Office of Performance Analysis & Integrity
<b>STOLEN LAPTOP</b>	<a href="#">ID: 3195: Accomack County laptop stolen from employee on vacation exposes 35,000 names, addresses and SSN compromised</a> Date: 2010-10-14 Records Lost: 35,000 Source: Outside Submitted by: Christine Location: Accomac VA, US Organizations: Accomack County Virginia
<b>FRAUD-SE</b>	<a href="#">ID: 3190: Employee steals 17 customers financial information to transfer funds</a> Date: 2010-10-13 Records Lost: 17 Source: Inside Malicious Submitted by: kirniki Location: Patuxent River MD, US Organizations: Navy Federal Credit Union
<b>HACK</b>	<a href="#">ID: 3189: Credit Card Numbers and medical information exposed after attack provides unauthorized access to the password-protected section of website</a> Date: 2010-10-11 Records Lost: Unknown Source: Outside Submitted by: jkouns Location: Winnipeg MB, CA Organizations: College-Of-Physicians-&-Surgeons-Of-Manitoba
<b>WEB</b>	<a href="#">ID: 3181: Flawed website exposes thousands of volunteers names addresses and Social Security numbers</a> Date: 2010-10-08 Records Lost: Unknown Source: Inside Accidental Submitted by: Christine Location: Washington DC, US Organizations: AmeriCorps
<b>WEB</b>	<a href="#">ID: 3183: 3,000 personnel records posted online for several weeks</a> Date: 2010-10-08 Records Lost: 3,000 Source: Inside Accidental Submitted by: Christine Location: Jackson MS, US Organizations: Mississippi National Guard
<b>STOLEN DOCUMENT</b>	<a href="#">ID: 3180: Stolen documents expose 121 customers personal financial information</a> Date: 2010-10-07 Records Lost: 121 Source: Unknown Submitted by: kirniki Location: Beaumont TX, US Organizations: Carolina West Wireless
<b>DISPOSAL DOCUMENT</b>	<a href="#">ID: 3173: Patient medical records found in recycling dumpster</a> Date: 2010-10-05 Records Lost: Unknown Source: Inside Accidental Submitted by: Christine Location: Omaha NE, US Organizations: Gastroenterology Consultants
<b>DISPOSAL DOCUMENT</b>	<a href="#">ID: 3164: Closed hospital building auctioned with former employees personal record</a> Date: 2010-10-04 Records Lost: Unknown Source: Inside Accidental Submitted by: pi3rce Location: Port St Joe FL, US Organizations: Gulf Pines Hospital
<b>HACK</b>	<a href="#">ID: 3165: POS terminals hacked, unknown number of customers credit card details stolen</a> Date: 2010-10-01 Records Lost: Unknown Source: Outside Submitted by: Christine Location: US Organizations: US Bank

## 2012 Cost of Cyber Crime Study by the Ponemon Institute

- **Cyber crimes continue to be costly**

Average annualized cost of cyber crime:

**2012:** \$8.9m per year, with a range of \$1.4m - \$46 million

**2011:** \$8.4 million. Increase of 6 percent or \$500,000

- **Cyber attacks have become common occurrences**

**2012:** 102 successful attacks per week

1.8 successful attacks per company per week.

**2011:** 72 successful attacks on average per week

42% increase

## Cost of a Data Breach



- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of costumers
- Erosion of shareholder value
- Fines and civil penalties
- Litigation and legal action
- Regulatory action and sanctions
- Significant cost and effort to notify affected parties  
and recover from the breach

~Ernst and Young, Data Loss Prevention: Risk Assessments and Considerations



### **Prevent inadvertent, unintentional data leaks by employees within the organization**

- Wrong email address and trailing emails
- Hidden fields in documents
- Lost USB sticks or laptops
- Cloud storage/applications

### **Prevent against malicious, intentional theft of data by insiders**

- Disgruntled employees
- Access to sensitive data

### **Prevent data loss through external attacks**

- Key loggers and other malware
- Hacking

# DLP Project Tasks

## **Data Classification**

- Identify sensitive data in various business units throughout the Agency
- Identify legitimate uses of sensitive data

## **Policy Formulation**

- Define incidents
- Define process for handling incidents

## **Technical design and Installation**

- Design
- Acquisition of DLP solution
- Installation
- Audit/Monitoring mode

## **Training and Communication**

- Communicate. Communicate. Communicate.

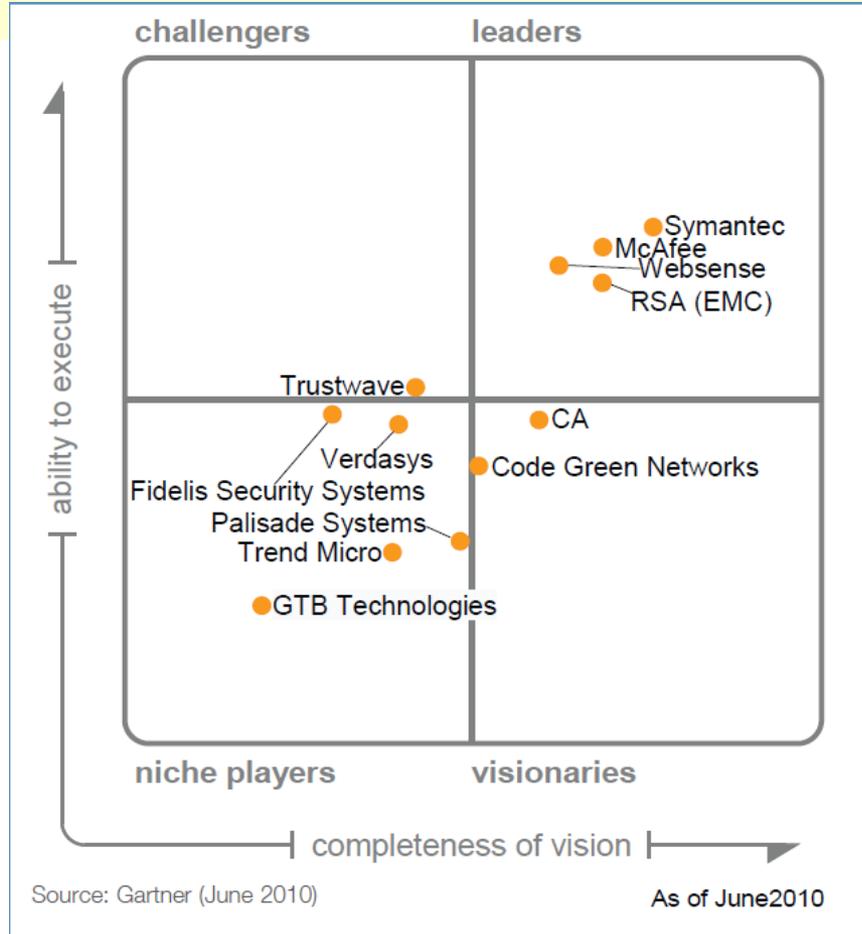
# DLP Project Team



**Customer Service**  
**Program Processing**  
**Program Benefits**  
**Program Distributions**  
**Investment Operations**  
**Accounting Operations**  
**Marketing and**  
**Communications**  
**Administrative Services**

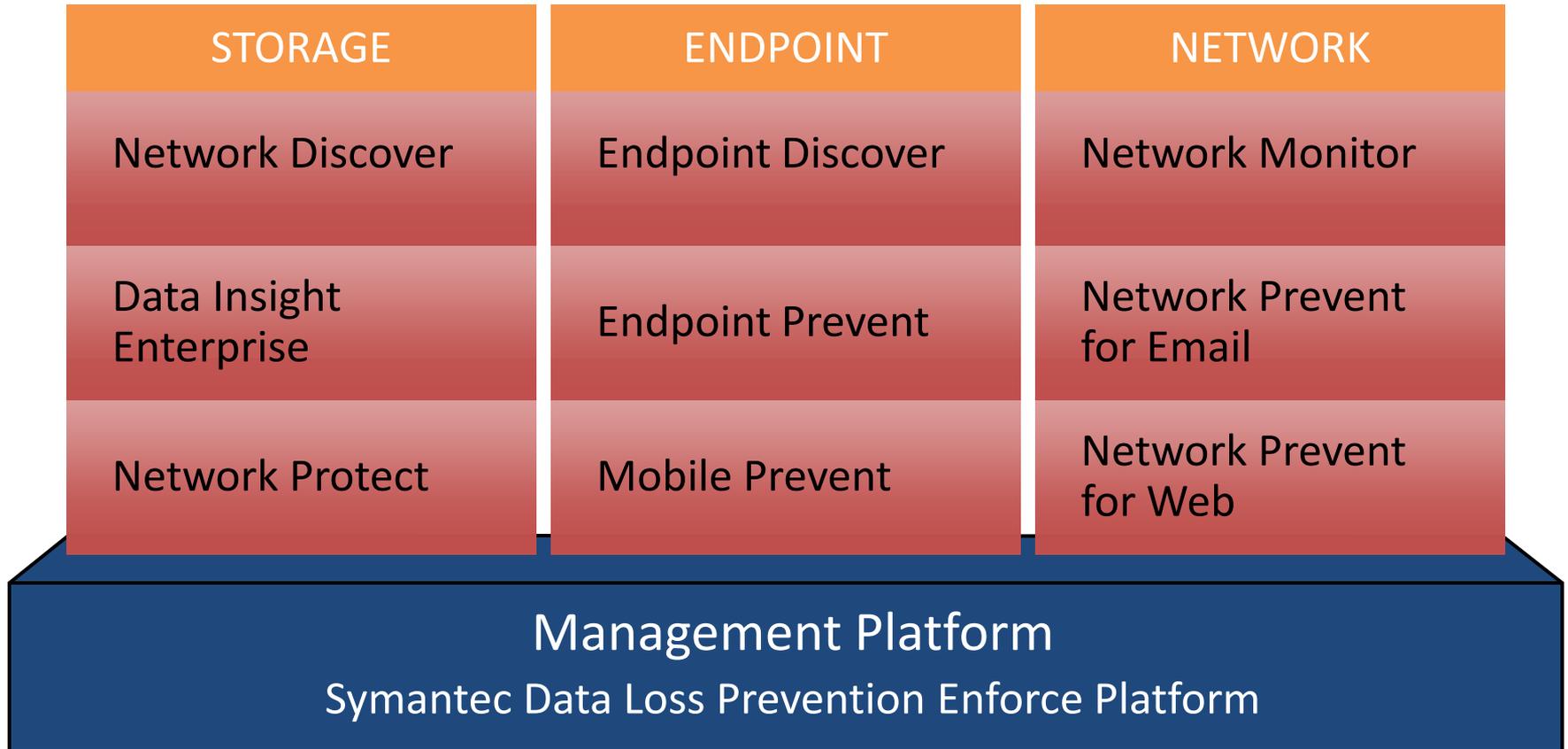
**Legal**  
**Human Resources**  
**Compliance**  
**Information Security**  
**Information Technology**  
**Operations**  
**Compliance**  
**Information Security**  
**Information Technology**  
**Operations**

# Vendor Selection



***We evaluated all four leaders and visionaries in the Gartner Magic Quadrant for content-aware data loss prevention.***

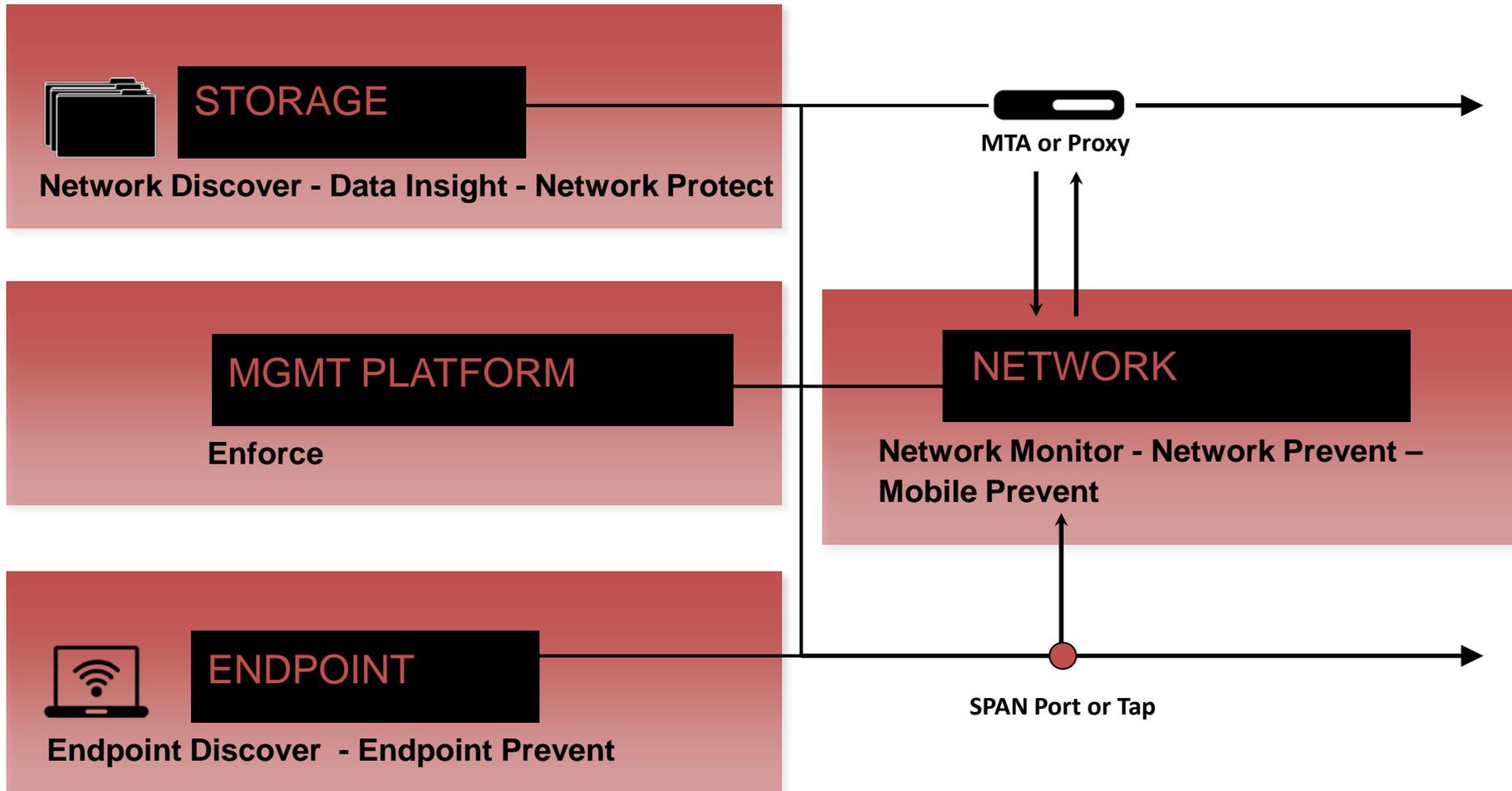
# Symantec DLP Products



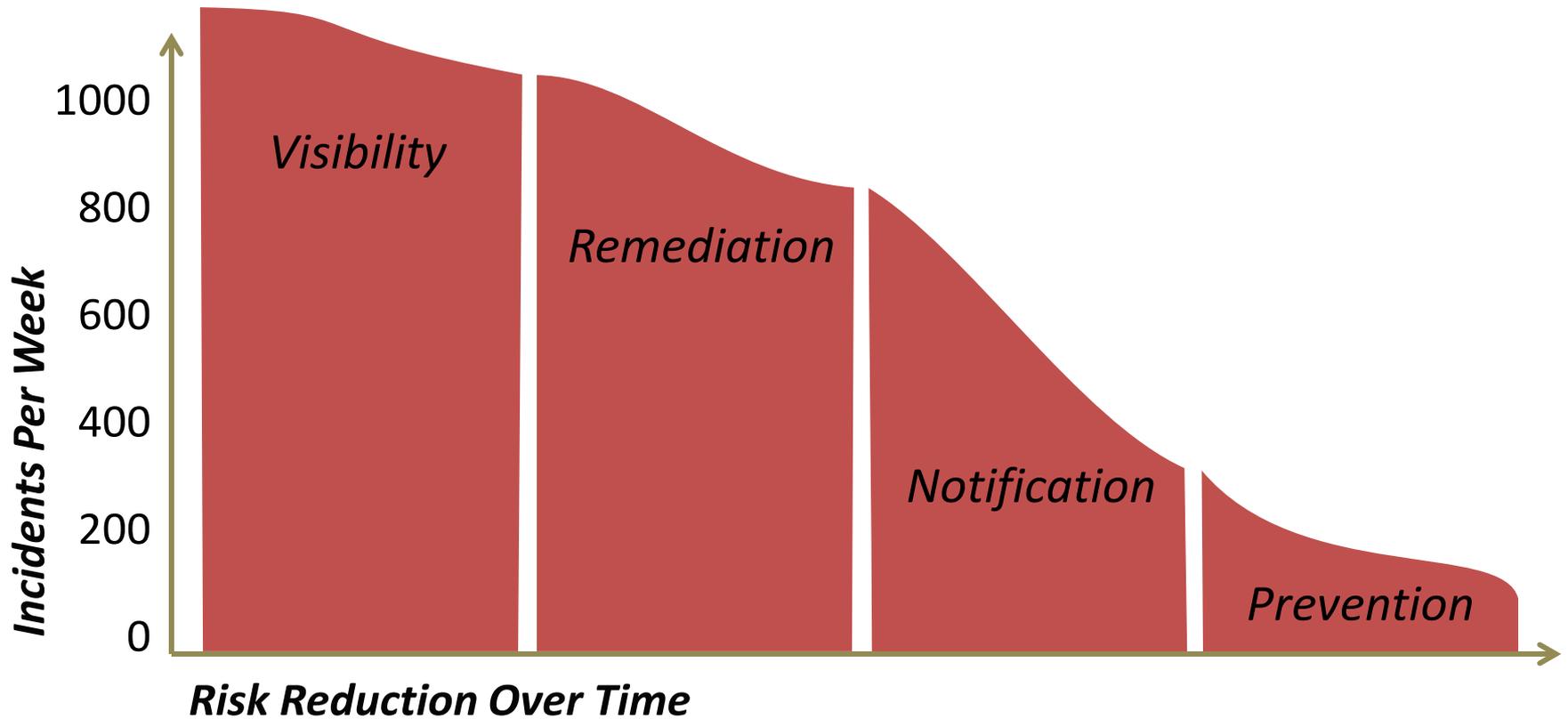
# Symantec Data Loss Prevention Architecture

Secured Corporate LAN

DMZ



# Continuous Risk Reduction



## Identify sensitive data

- What data do you want to protect? How are they used?
- This will determine which DLP components need to be installed

## Consider hiring a consultant

- DLP is a complex set of solutions
- Weigh in house experience and skill set against cost

## Involve all stakeholders

- Make sure each area in the organization is involved in the project
- Get management buy in as early as possible
- Solicit end user input for policy formulation
- Communicate and Train. Rinse. Repeat.

## Continue to refine DLP policies over time

**DLP is not a silver bullet but a very useful tool in the information security arsenal.**



**The next few slides will be screen shots of various modules of the Data Loss Prevention Modules.**



From: dp\_system@virginia529.com  
To: Rosario Igharas  
Cc:  
Subject: Gramm-Leach-Bliley was violated by

Sent: Mon

Daisy Team,

The Gramm-Leach-Bliley was violated by [REDACTED]

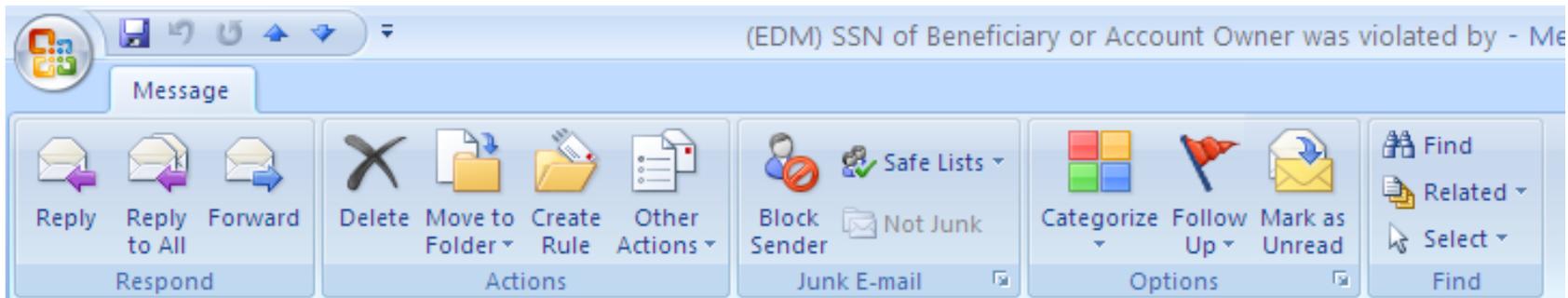
The policy was violated by sending a data transmission via Endpoint HTTPS with a match count of 2.

Please follow up with the department head to clarify the security policy around this type of data.

For further details please look at Incident [#Incident Snapshot](#)

Thank you,

VCSP Security Team



From: dlp\_system@virginia529.com  
To: Rosario Igharas  
Cc:  
Subject: (EDM) SSN of Beneficiary or Account Owner was violated by

Daisy Team,

The (EDM) SSN of Beneficiary or Account Owner was violated by .

The policy was violated by sending a data transmission via HTTP with a match count of 1.

Please follow up with the department head to clarify the security policy around this type of data.

For further details please look at Incident [#Incident Snapshot](#)

Thank you,

VCSP Security Team

**Choose a type of policy to add, then click next**

- Add a blank policy  
*Create a policy from scratch*
- Add a policy from a template  
*Create a policy based on a template, which can then be modified to suit your needs*

# Symantec Data Loss Prevention



Home



Incidents



**Policies**



System

**Policy List**

Response Rules

Endpoint User Groups

Discover Scanning

Policies > Policy List > Configure Policy

Cancel Save

## General

Name

Description

Policy Group

- Status
- Last Modified
- Detection** Groups
- 
- Rules:
- Exceptions:
- Select Policy Group...
  - Confidential Data Protection
  - Discover Policies
  - Endpoint Policies
  - Regulatory Enforcement (EDM)
  - Regulatory Enforcement for Web
  - System Wide
  - Testing Policy Group
  - TestProxy

This policy contains no rules.

This policy contains no exceptions.

[Export this policy as a template](#)

## Add Detection Rule

Rule Type	Product	Technology
<b>Content</b>		
<input type="radio"/> Content Matches Regular Expression <i>Detect incidents using regular expressions.</i>	  	 (DCM)
<input type="radio"/> Content Matches Exact Data From: <input type="text" value="Account, SSN and Owners Name"/>  <i>Detect incidents from exact data profiles. Select the appropriate exact data profile.</i>	  	 (EDM)
<input type="radio"/> Content Matches Keyword <i>Detect incidents containing keywords or keyphrases.</i>	  	 (DCM)
<input type="radio"/> Content Matches Document Signature From: <input type="text" value="No Document Profiles Available"/>  <i>Match content contained in indexed document profile.</i>	  	 (IDM)
<input type="radio"/> Content Matches Data Identifier: <input type="text" value="Choose Data Identifier..."/>  <i>Detect incidents by searching for data identifiers.</i>	  	 (DCM)
<b>File Properties</b>		
<input type="radio"/> Message Attachment or File Type Match <i>Use this rule to find specific types of documents, such as Office or PDF files.</i>	  	 (DCM)
<input type="radio"/> Message Attachment or File Size Match <i>Match attachment or files over or under a certain size.</i>	  	 (DCM)
<input type="radio"/> Message Attachment or File Name Match <i>Match attachment filenames by exact name or by pattern.</i>	  	 (DCM)
<b>Protocol</b>		
<input type="radio"/> Protocol or Endpoint Destination <i>Detects incidents on the Network or Endpoint. Based on method of detection or communication.</i>	 	 (DCM)
<input type="radio"/> Endpoint Location <i>Detect Endpoint incidents depending on the network location of the endpoint.</i>		 (DCM)

## Add Detection Rule

Rule Type	Product	Technology
<b>Content</b>		
<input type="radio"/> Content Matches Regular Expression <i>Detect incidents using regular expressions.</i>	  	 (DCM)
<input type="radio"/> Content Matches Exact Data From: <input type="text" value="Account, SSN and Owners Name"/>  <i>Detect incidents from exact data profiles. Select the appropriate exact data profile.</i>	  	 (EDM)
<input type="radio"/> Content Matches Keyword <i>Detect incidents containing keywords or keyphrases.</i>	  	 (DCM)
<input type="radio"/> Content Matches Document Signature From: <input type="text" value="No Document Profiles Available"/>  <i>Match content contained in indexed document profile.</i>	  	 (IDM)
<input type="radio"/> Content Matches Data Identifier: <input type="text" value="Choose Data Identifier..."/>  <i>Detect incidents by searching for data identifiers.</i>	  	 (DCM)
<b>File Properties</b>		
<input type="radio"/> Message Attachment or File Type Match <i>Use this rule to find specific types of documents, such as Office or PDF files.</i>	  	 (DCM)
<input type="radio"/> Message Attachment or File Size Match <i>Match attachment or files over or under a certain size.</i>	  	 (DCM)
<input type="radio"/> Message Attachment or File Name Match <i>Match attachment filenames by exact name or by pattern.</i>	  	 (DCM)
<b>Protocol</b>		
<input type="radio"/> Protocol or Endpoint Destination <i>Detects incidents on the Network or Endpoint. Based on method of detection or communication.</i>	 	 (DCM)
<input type="radio"/> Endpoint Location <i>Detect Endpoint incidents depending on the network location of the endpoint.</i>		 (DCM)

Content Matches Document Signature From: No Document Profiles Available

*Match content contained in indexed document profile.*



Content Matches Data Identifier: Choose Data Identifier...

*Detect incidents by searching for*



### File Properties

Message Attachment or File Type

*Use this rule to find specific types*



Message Attachment or File Size

*Match attachment or files over or*



Message Attachment or File Name

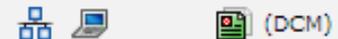
*Match attachment filenames by ex*



### Protocol

Protocol or Endpoint Destination

*Detects incidents on the Network*



Endpoint Location

*Detect Endpoint incidents depend*



Network DLP Endpoint DLP

Indexed Document Matching Desc

Choose Data Identifier...

#### North American Personal Identity :

- US Social Security Number (SSN)
- Canadian Social Insurance Number
- US Individual Tax Identification Number (ITIN)
- Driver's License Number- CA State
- Driver's License Number- IL State
- Driver's License Number- NJ State
- Driver's License Number- NY State
- Driver's License Number- FL, MI, MN States

#### Financial :

- Credit Card Number
- ABA Routing Number
- CUSIP Number
- SWIFT Code
- Credit Card Magnetic Stripe Data
- IBAN West
- IBAN Central
- IBAN East

#### Healthcare :

- National Drug Code (NDC)
- Australian Medicare Number

#### Information Technology :

- IP Address

#### European Personal Identity :

- Codice Fiscale
- Spanish DNI ID
- Burgerservicenummer
- UK Driver's Licence Number
- UK Tax ID Number

## General

Rule Name

## Severity

Add Severity

Default

High 

## Conditions

➤ Content Matches

Data Identifier:

*Data Identifier:* US Social Security Number (SSN)

Personal identification number issued by the Social Security Administration of the United States government. Although primarily used for administering the Social Security program, it is widely used as a personal identification number in many purposes. ([more info](#))

- Breadth:*
- wide Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
  - medium Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, or periods. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
  - narrow Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit. Also requires the presence of a Social Security-related keyword.

*Optional Validators:*  Require beginning characters

*With this option selected, any of the following list of values are required at the beginning of the matched data.*

*Enter a comma-separated list of values WITHOUT any dashes or other separators. Each value can be of any length.*

## Severity

Add Severity

Default

High

## Conditions

Protocol or Endpoint Destination

*Endpoint or Network Protocol*

**Detect incidents over the Network and at the Endpoint using selected protocols:**

Email/SMTP

HTTP

HTTPS/SSL

IM:MSN

IM:AIM

IM:Yahoo

FTP

*Network Protocol*

**Detect incidents over the Network using selected protocols:**

NNTP

TCP:BitTorrent

TCP:DirectConnect

TCP:EDonkey

TCP:FastTrack

TCP:Gnutella

TCP:IRC

TCP:Napster

TCP:Pop3

TCP:SSH

TCP:SSL

TCP:Telnet

TCP:ip-based

*Endpoint Destination*

**Detect when users move data on the endpoint to these places:**

Local Drive

CD/DVD

Removable Storage

Printer/Fax

Clipboard

*Match On:*

Envelope

Body

Attachments

Also Match: Match...



Add

## Severity

Add Severity

Default

High

## Conditions

Protocol or Endpoint Destination

*Endpoint or Network Protocol*

**Detect incidents over the Network and at the Endpoint using selected protocols:**

Email/SMTP

HTTP

HTTPS/SSL

IM:MSN

IM:AIM

IM:Yahoo

FTP

*Network Protocol*

**Detect incidents over the Network using selected protocols:**

NNTP

TCP:BitTorrent

TCP:DirectConnect

TCP:EDonkey

TCP:FastTrack

TCP:Gnutella

TCP:IRC

TCP:Napster

TCP:Pop3

TCP:SSH

TCP:SSL

TCP:Telnet

TCP:ip-based

*Endpoint Destination*

**Detect when users move data on the endpoint to these places:**

Local Drive

CD/DVD

Removable Storage

Printer/Fax

Clipboard

*Match On:*

Envelope

Body

Attachments

Also Match: Match...



Add

## Add Detection Exception

Exception Type	Product	Technology
<b>Content</b>		
<input type="radio"/> Content Matches Regular Expression <i>Detect incidents using regular expressions.</i>	  	 (DCM)
<input type="radio"/> Content Matches Keyword <i>Detect incidents containing keywords or keyphrases.</i>	  	 (DCM)
<input type="radio"/> Content Matches Document Signature From: <input type="text" value="No Document Profiles Available"/> 	  	 (IDM)
<input type="radio"/> Content Matches Data Identifier: <input type="text" value="Choose Data Identifier..."/> 	  	 (DCM)
<b>File Properties</b>		
<input type="radio"/> Message Attachment or File Type Match <i>Use this rule to find specific types of documents, such as Office or PDF files.</i>	  	 (DCM)
<input type="radio"/> Message Attachment or File Size Match <i>Match attachment or files over or under a certain size.</i>	  	 (DCM)
<input type="radio"/> Message Attachment or File Name Match <i>Match attachment filenames by exact name or by pattern.</i>	  	 (DCM)
<b>Protocol</b>		
<input type="radio"/> Protocol or Endpoint Destination <i>Detects incidents on the Network or Endpoint. Based on method of detection or communication.</i>	 	 (DCM)
<input type="radio"/> Endpoint Location <i>Detect Endpoint incidents depending on the network location of the endpoint.</i>		 (DCM)



Network DLP



Endpoint DLP



Storage DLP



Indexed Document Matching



Described Content Matching



Exact Data Matching

### General

Exception Name

Apply Exception to  Entire Message  
 Matched Components Only

### Conditions

Content Matches

Regular Expression

*Match* Regular Expression:

*Match Counting:*  Check for existence (don't count multiple matches)  
 Count all matches and only report incidents with at least  matches

*Match On:*  Envelope  
 Body  
 Attachments

Also Match:

## Policy List

olicies > Pol

Cancel OK

### General

Exception Na

Apply Except

### Conditions

Content

Regular Expr

Match

Also Match:

- Content Matches Data Identifier: IBAN Central
- Content Matches Data Identifier: IBAN East
- Content Matches Data Identifier: IBAN West
- Content Matches Data Identifier: IP Address
- Content Matches Data Identifier: National Drug Code (NDC)
- Content Matches Data Identifier: People's Republic of China ID
- Content Matches Data Identifier: Singapore NRIC
- Content Matches Data Identifier: South Korea Resident Registration Number
- Content Matches Data Identifier: Spanish DNI ID
- Content Matches Data Identifier: SWIFT Code
- Content Matches Data Identifier: Swiss AHV number
- Content Matches Data Identifier: Taiwan ROC ID
- Content Matches Data Identifier: UK Driver's Licence Number
- Content Matches Data Identifier: UK Electoral Roll Number
- Content Matches Data Identifier: UK National Health Service (NHS) Number
- Content Matches Data Identifier: UK National Insurance Number
- Content Matches Data Identifier: UK Passport Number
- Content Matches Data Identifier: UK Tax ID Number
- Content Matches Data Identifier: US Individual Tax Identification Number (ITIN)
- Content Matches Data Identifier: US Social Security Number (SSN)
- Content Matches Keyword
- Content Matches Regular Expression
- Endpoint Location
- Message Attachment or File Name Match
- Message Attachment or File Size Match
- Message Attachment or File Type Match
- Protocol or Endpoint Destination
- Recipient Matches Pattern
- Sender/User Matches Pattern
- User Matches Endpoint User Groups

Match...

anning

Protected Content

Add



Home



Incidents



**Policies**



System

Policy List

Response Rules

Endpoint User Groups

Discover Scanning

**Protected Content**

Policies > Protected Content > Exact Data > Add Exact Data Profile

Cancel Next >

### General

Name

Data Source

*For a Directory Profile, include one or more sender/recipient identifying fields.*

Upload Data Source to Server Now

Reference Data Source on Manager Host

None Selected

Use This File Name

Number of Columns:

Column Names

Read first row as column names

Error Threshold (max % of rows with errors before indexing stops)

%

Column Separator Char

Tab ( )

File Encoding

ISO-8859-1 (Latin-1)



Home



Incidents



**Policies**



System



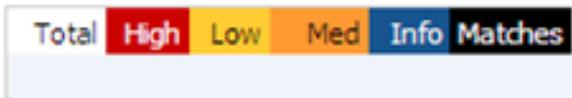
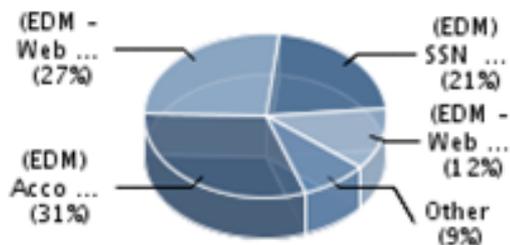
- Policy List
- Response Rules**
- Endpoint User Groups
- Discover Scanning
- Protected Content

Policies > Response Rules

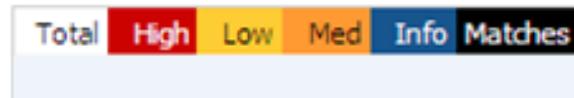
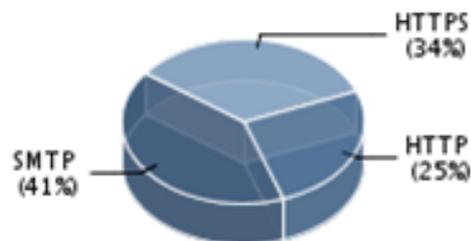
Add Response Rule

Rule	Actions	Conditions	
Block Copy to Removable Media	<b>Endpoint Prevent: Block</b> <b>All: Set Status:</b> Escalated	<i>when</i> Severity Is Any Of High <i>and</i> Protocol or Endpoint Destination Is Any Of Endpoint CD/DVD, Endpoint Removable Storage Device	
Block Endpoint	<b>Endpoint Prevent: Block</b>	Execute Always	
Block SMTP Email	<b>Network Prevent: Block SMTP Message</b> <b>All: Set Status:</b> Escalated <b>All: Send Email Notification</b>	<i>when</i> Protocol or Endpoint Destination Is Any Of SMTP	
Block SMTP for Encrypted and Password Protected Files	<b>All: Send Email Notification</b> <b>Network Prevent: Block SMTP Message</b> <b>All: Set Status:</b> Escalated	<i>when</i> Protocol or Endpoint Destination Is Any Of SMTP	
Block Web Communication	<b>All: Set Status:</b> Escalated <b>Network Prevent: Block HTTP/HTTPS</b>	<i>when</i> Protocol or Endpoint Destination Is Any Of FTP, HTTP, HTTPS <i>and</i> Severity Is Any Of High	
Copy Stored File	<b>Network Protect: Copy File</b>	<i>when</i> Severity Is Any Of Medium	
Dismiss, Bus. Process Issue	<b>All: Set Attribute:</b> Dismissal Reason <b>All: Set Status:</b> Broken Business Process	Manually Executed	
Dismiss, False Positive	<b>All: Set Attribute:</b> Dismissal Reason <b>All: Set Status:</b> False Positive	Manually Executed	
Endpoint Pop-Up Notification	<b>Endpoint Prevent: Notify</b>	<i>when</i> Endpoint Location Is Any Of Off the Corporate Network	
Escalate for Investigation	<b>All: Set Status:</b> Investigation	Manually Executed	
Notify and Resolve	<b>All: Set Status:</b> Resolved <b>All: Send Email Notification</b> <b>All: Set Attribute:</b> Resolution	<i>when</i> Severity Is Any Of Low	
Notify Incident Team on Violation and Escalate	<b>All: Send Email Notification</b> <b>All: Set Status:</b> Escalated	Execute Always	
Notify Manager	<b>All: Send Email Notification</b>	Manually Executed	
Notify of Medium Severity Incident and Escalate	<b>All: Send Email Notification</b> <b>All: Set Status:</b> Escalated	<i>when</i> Severity Is Any Of Medium	
Open Investigation	<b>All: Set Attribute:</b> External Reference <b>All: Set Status:</b> Investigation	Manually Executed	
Remove Web Content	<b>Network Prevent: Remove HTTP/HTTPS Content</b> <b>All: Set Status:</b> Escalated	<i>when</i> Protocol or Endpoint Destination Is Any Of HTTP, HTTPS, IM:MSN, IM:AIM, IM:Yahoo, FTP, NNTP <i>and</i> Severity Is Any Of High	

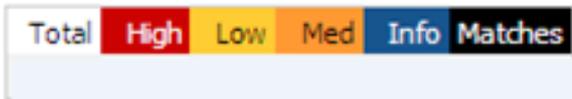
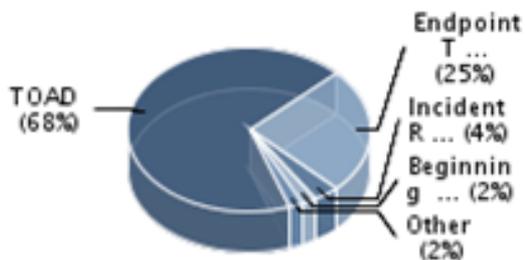
## Policy Summary



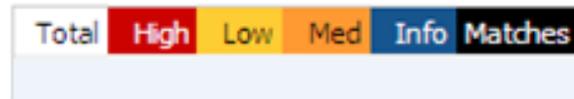
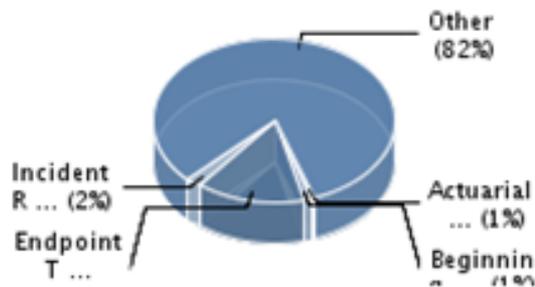
## Incidents per Protocol



## Target Summary



## Policy by Target





# Symantec Data Loss Prevention



Home



Incidents



Policies

Servers

Agents

System Reports

System

User Management

Roles

Add Role

Name	Description
Accounting	This role is for the Accounting and Inves
Administration	This Role allows view of incidents from t
Administrative	Role to view Scholarships, Marketing, Ma
CFO	This role has access to the Finance, Cus
Compliance	This role is to view incidents that are fr



Home



Incidents



**Policies**



System

Policy List | Response Rules | Endpoint User Groups | **Discover Scanning** | Protected Content

Policies > Discover Scanning > Discover Targets

New Target ▾

Target▲	Scan	Run Time	Items Scanned	Bytes Scanned	Errors	Incidents
Actuarial Data	Ready					
	7/11/12 12:12 PM	00:00:00:04	3	11,107,196	0	1
	7/11/12 12:01 PM	00:00:00:18	3	11,107,196	0	1
	7/5/12 2:19 PM	00:00:00:04	3	11,107,196	0	1
	<a href="#">show all scans...</a>					
Beginning Balances	Ready					
	3/2/11 9:21 AM	00:00:00:01	2	1,843,478	0	2
	3/2/11 9:15 AM	00:00:00:08	2	1,843,513	0	2
	3/1/11 4:05 PM	00:00:00:01	2	1,843,513	0	0
	<a href="#">show all scans...</a>					
Endpoint Test Scan	Running on Endpoint 1	882:01:46:05	22,497,290	9,271,991,968,871		
	99% done, Agents completed:					
	1/25/11 4:00 PM	54:22:36:08	546,718	150,590,520,203		
	<a href="#">show all scans...</a>					
Incident Report	Ready					
	7/11/12 12:06 PM	00:00:00:13	49	20,415,749	0	4
	7/6/12 8:10 AM	00:00:00:13	49	20,415,749	0	4
	7/6/12 8:09 AM	00:00:00:20	49	20,415,749	0	4
	<a href="#">show all scans...</a>					



**Servers** | Agents | System Reports | Settings | Incident Data | User Management

System > Servers > Overview

Add Server Upgrade

**Servers**

Status	Server	Messages (Last 10 sec)	Messages (Today)	Incidents (Today)	Incident Queue
▶ Running	Enforce Server	N/A	N/A	N/A	0
▶ Running	Discover 1 (Network Discover)	0	17	0	0
▶ Running	Discover 1 (DMZ) (Network Discover)	0	0	0	0
▶ Running	Endpoint 1 (Endpoint)	0	153,456	0	0
▶ Running	Monitor 1 (Network Monitor)	24	160,511	0	0
▶ Running	Email Prevent (Network Prevent for E-mail)	0	597	4	0
▶ Running	Web Prevent (Network Prevent for Web)	1	1,628	0	0

**Recent Error and Warning Events | show all »**

Type	Time	Server	Host	Code	Message
✖	July 9, 2013 1:45:59 PM EDT	Monitor Tramp	192.168.200.150	3310	No TCP:FastTrack Traffic Captured
✖	July 9, 2013 1:45:59 PM EDT	Monitor Tramp	192.168.200.150	3310	No TCP:DirectConnect Traffic Captured
✖	July 9, 2013 1:45:59 PM EDT	Monitor Tramp	192.168.200.150	3310	No TCP:Napster Traffic Captured
✖	July 9, 2013 1:45:59 PM EDT	Monitor Tramp	192.168.200.150	3310	No TCP:BitTorrent Traffic Captured
✖	July 9, 2013 1:45:59 PM EDT	Monitor Tramp	192.168.200.150	3310	No TCP:Gnutella Traffic Captured

**License**

Products Network Monitor, Network Discover, Network Protect, Endpoint Prevent, Endpoint Discover, Mail Prevent, Web Prevent, Data Insight

# Virginia529

College Savings Plan



**[righaras@virginia529.com](mailto:righaras@virginia529.com)**

**9001 Arboretum Parkway  
Richmond, Virginia 23236  
Toll Free: 1-888-567-0540  
On the web: [Virginia529.com](http://Virginia529.com)**

 [Facebook.com/Virginia529](https://www.facebook.com/Virginia529)

 [Twitter.com/VA529](https://twitter.com/VA529)



Virginia Information Technologies Agency

# Undercover Clicker

Ed Miller CISA, CISM,  
CIA, CIPP/IT





*Virginia Information Technologies Agency*

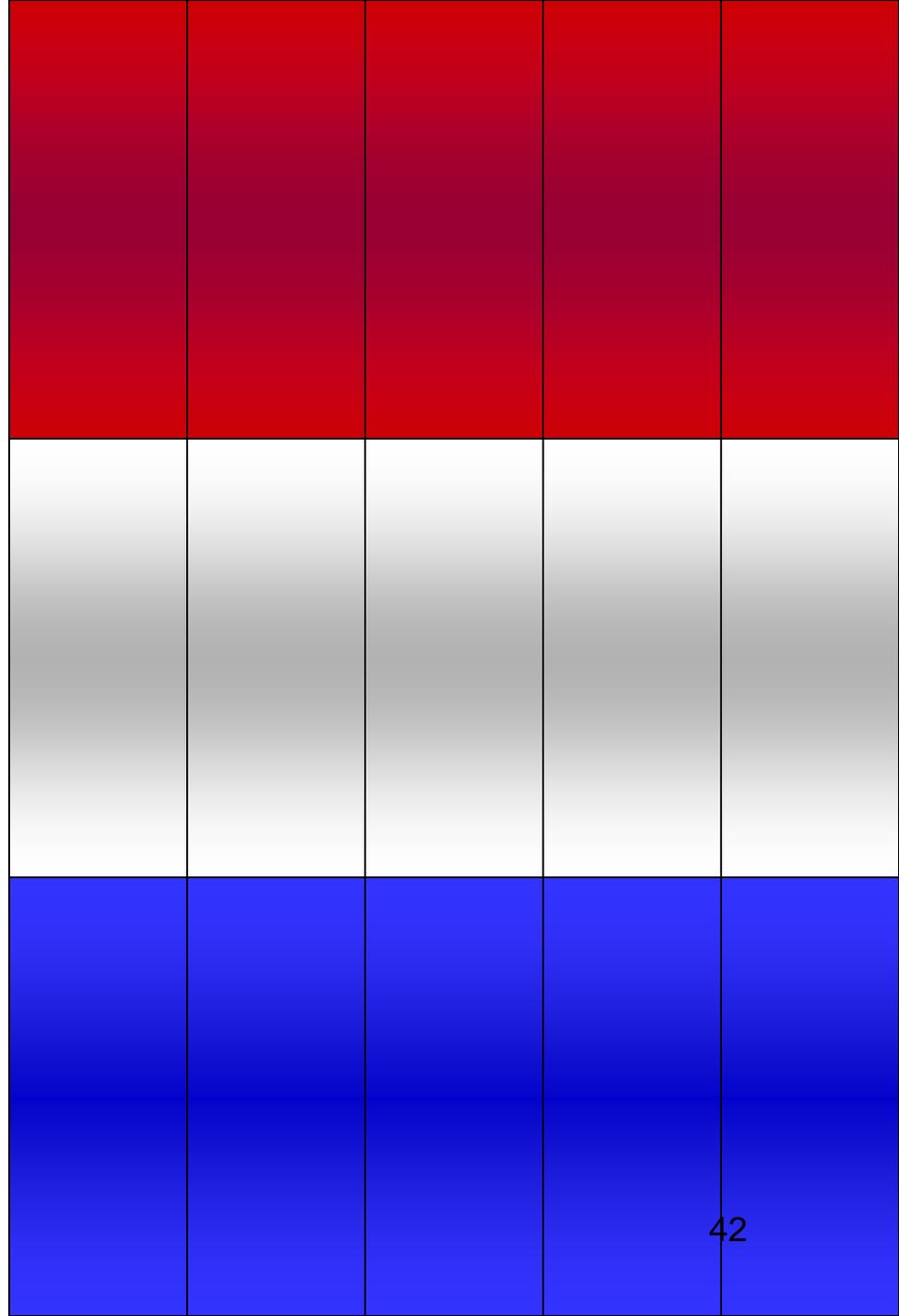
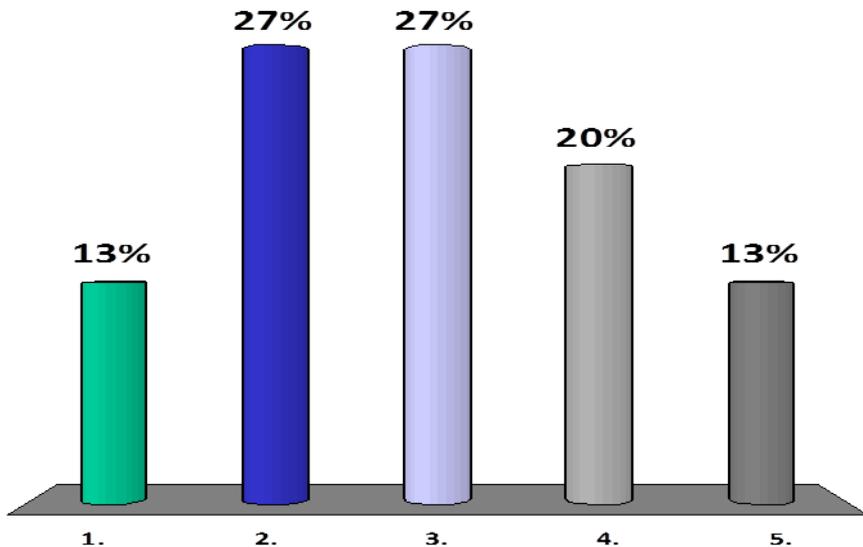
# Undercover Clicker Rules

- Object of the game is to identify the hidden image that is “undercover”.
- A picture or an image will be uncovered piece by piece.
- When you recognize the picture, choose the best answer.



This image represents something that is unwanted in your email.

- 1. Virus
- 2. Hoax
- ✓ 3. SPAM
- 4. Phishing email
- 5. Mother-in-law coming to visit





*Virginia Information Technologies Agency*

# Undercover Clicker Rules

1. Compete by teams.
2. Correct answers are worth a maximum of 15 points.
3. Incorrect answers score 0.
4. Score is based on the average score of the team.
5. Speed scoring in effect (i.e. the quicker you answer the more points you score).
6. First response only counts.
7. Good luck!



*Virginia Information Technologies Agency*



# Pick your team.

## What day of the month were you born on?

- 1. Team 1:** if you were born on days 1 through 15
- 2. Team 2:** if you were born on days 16 through 31





Virginia Information Technologies Agency



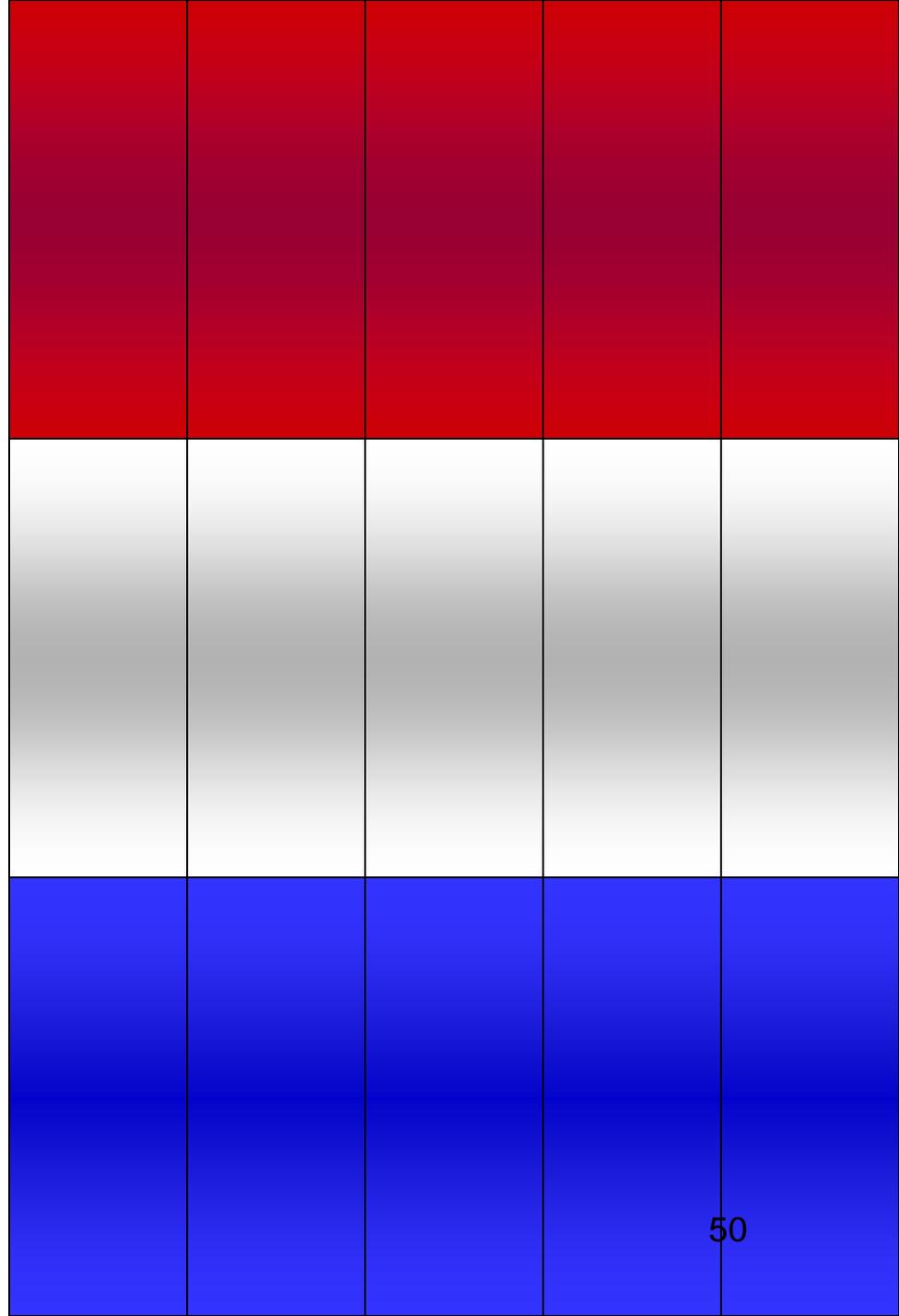
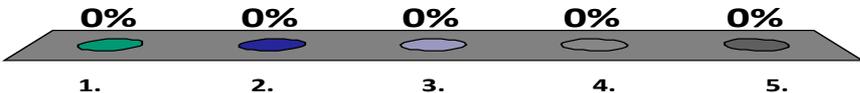






# Identify this diagram of an encryption process:

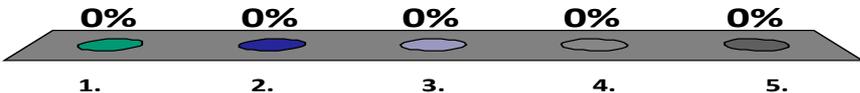
- 1. Key Escrow Administration
- 2. Crypto Key Management
- 3. Key Bit Flipper Attack
- ✓ 4. Public Key Encryption
- 5. 2-Factor Key Authentication



# What is this screenshot from?

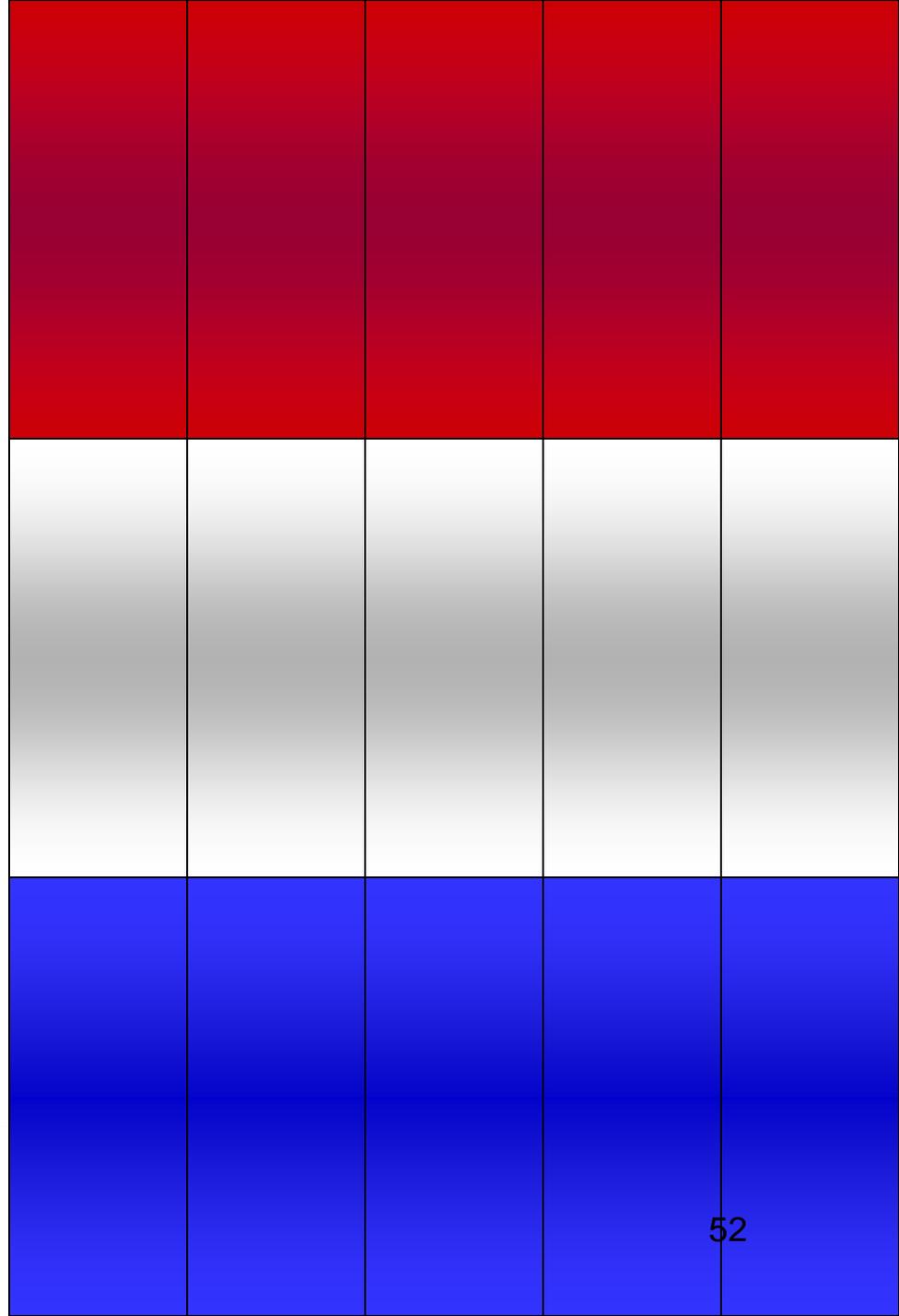
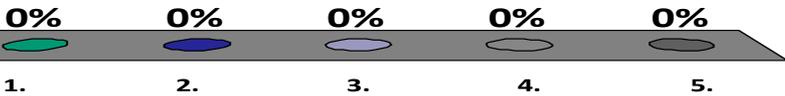


- 1. Mister McDashboard
- 2. RSA Archer eGRC
- 3. Cisco Communications Console
- 4. MS Management Console
- 5. iRisk Vulnerability View



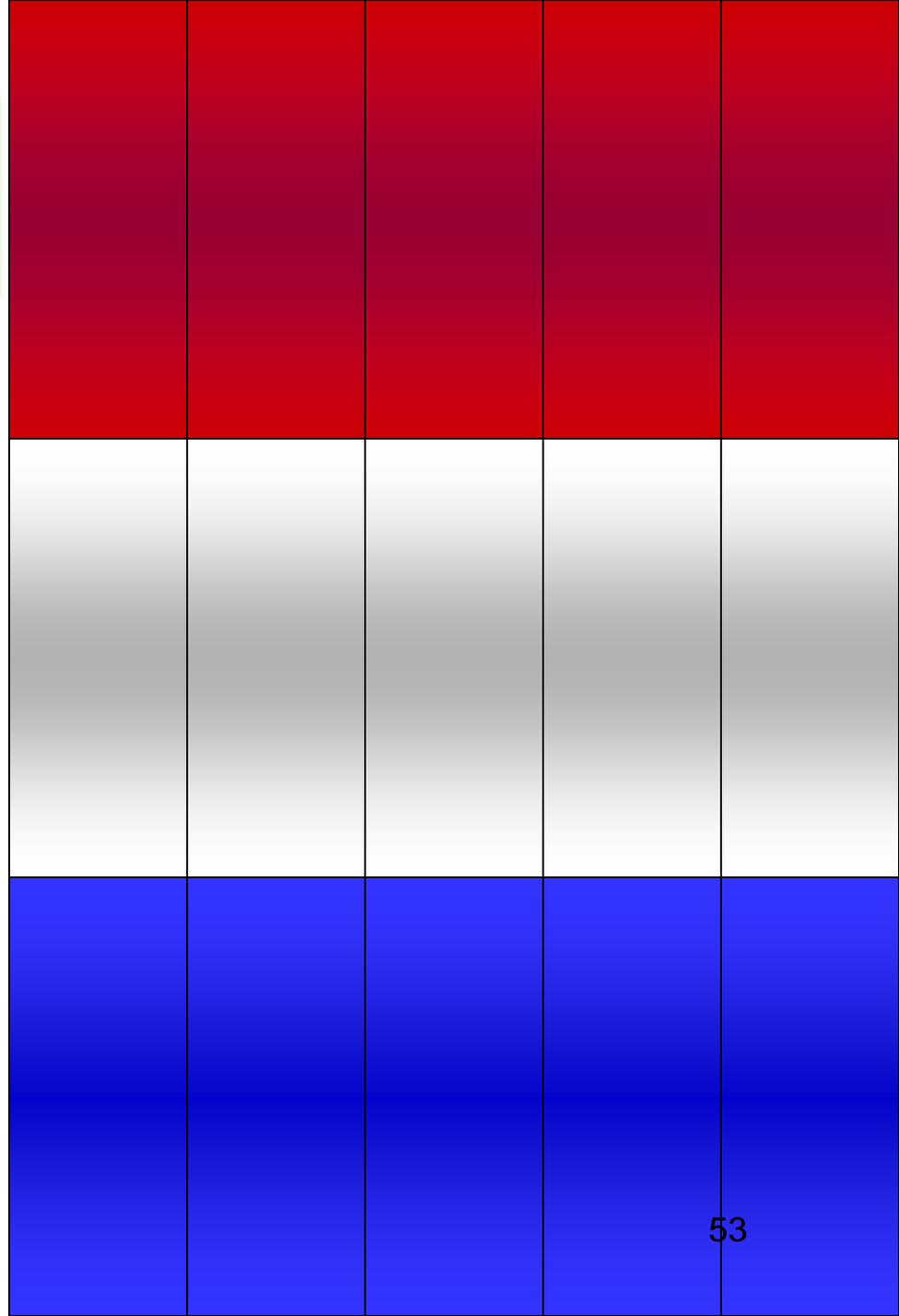
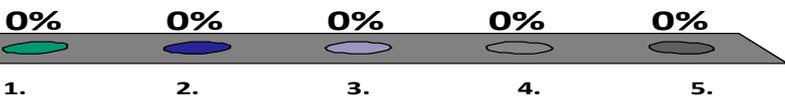

# What security framework does this represent?

- 1. System Development Life Cycle
- 2. COBIT 5.1
- ✓ 3. NIST Security Life Cycle
- 4. PCI-Data Security Standards
- 5. Mauri Shaw Risk Management Framework



This 1991 malware coincidentally shared the same name as this fictional character.

- 1. Nimda
- ✓ 2. Michelangelo
- 3. Pikachu
- 4. Sasser
- 5. Koobface



# Team Scores

**Points Team**

**Points Team**

# Participant Leaders

**Points**      **Participant**

**Points**      **Participant**

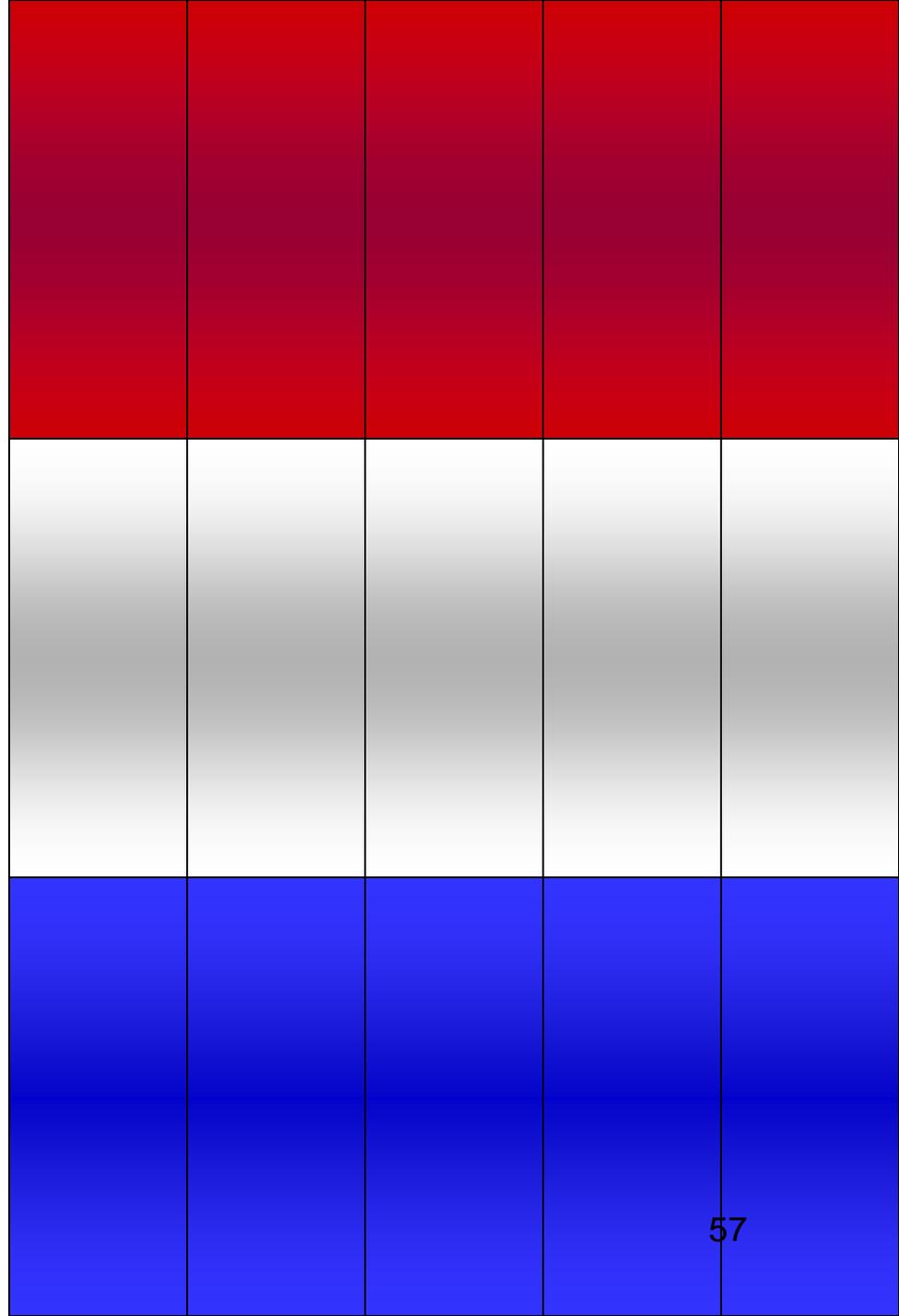
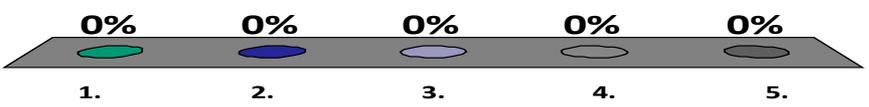


Virginia Information Technologies Agency



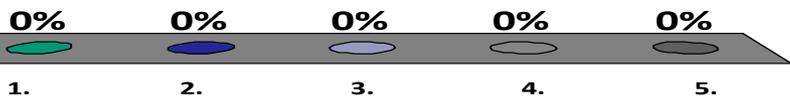
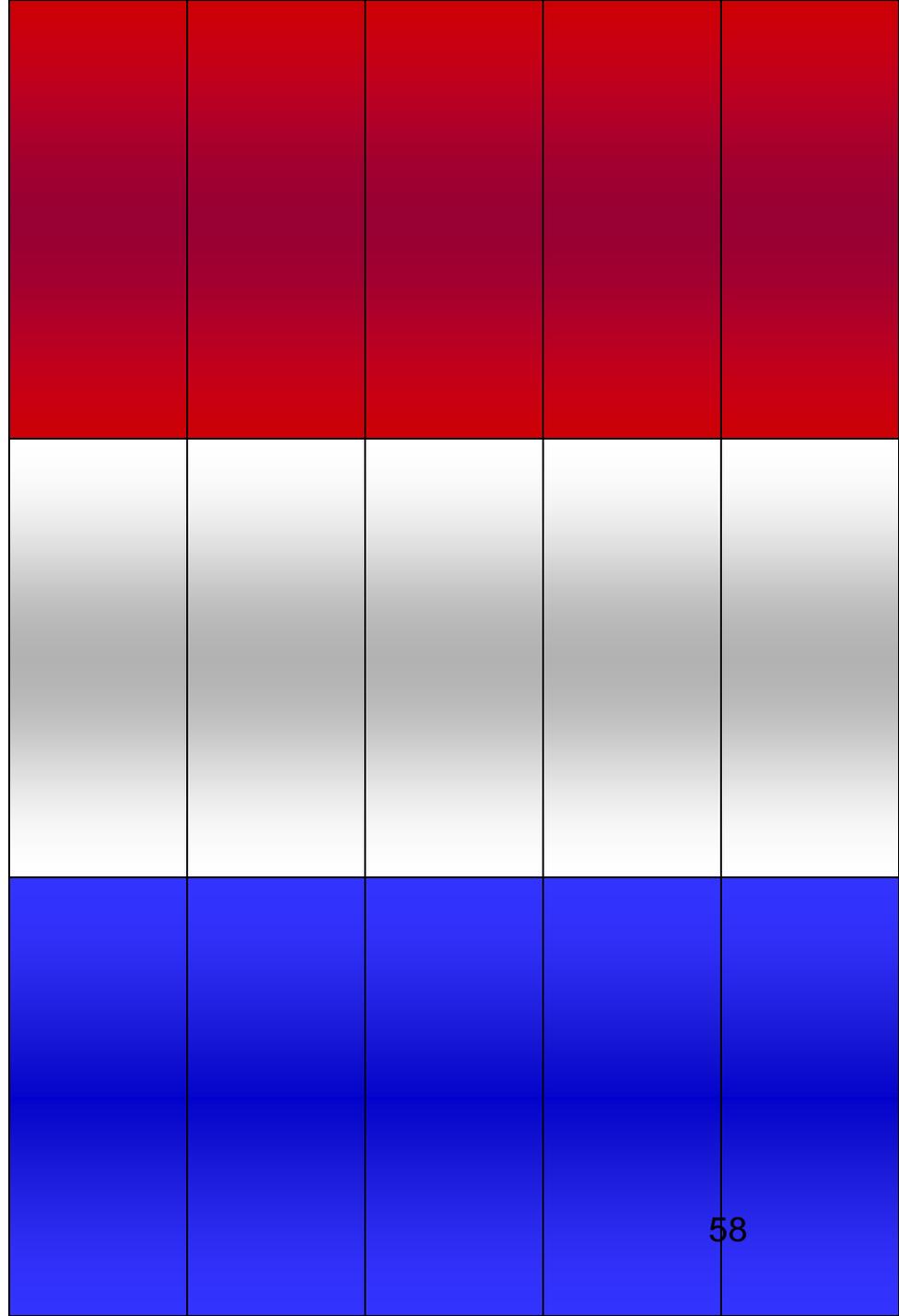
# What security concept does this graphic represent?

- 1. OSI Security Model
- ✓ 2. Defense-in-Depth
- 3. OWASP Top 10
- 4. Network Security Model
- 5. SANS Critical Controls



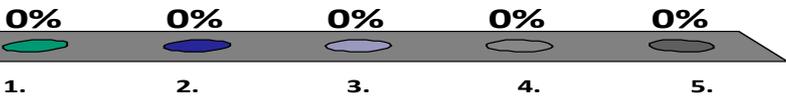
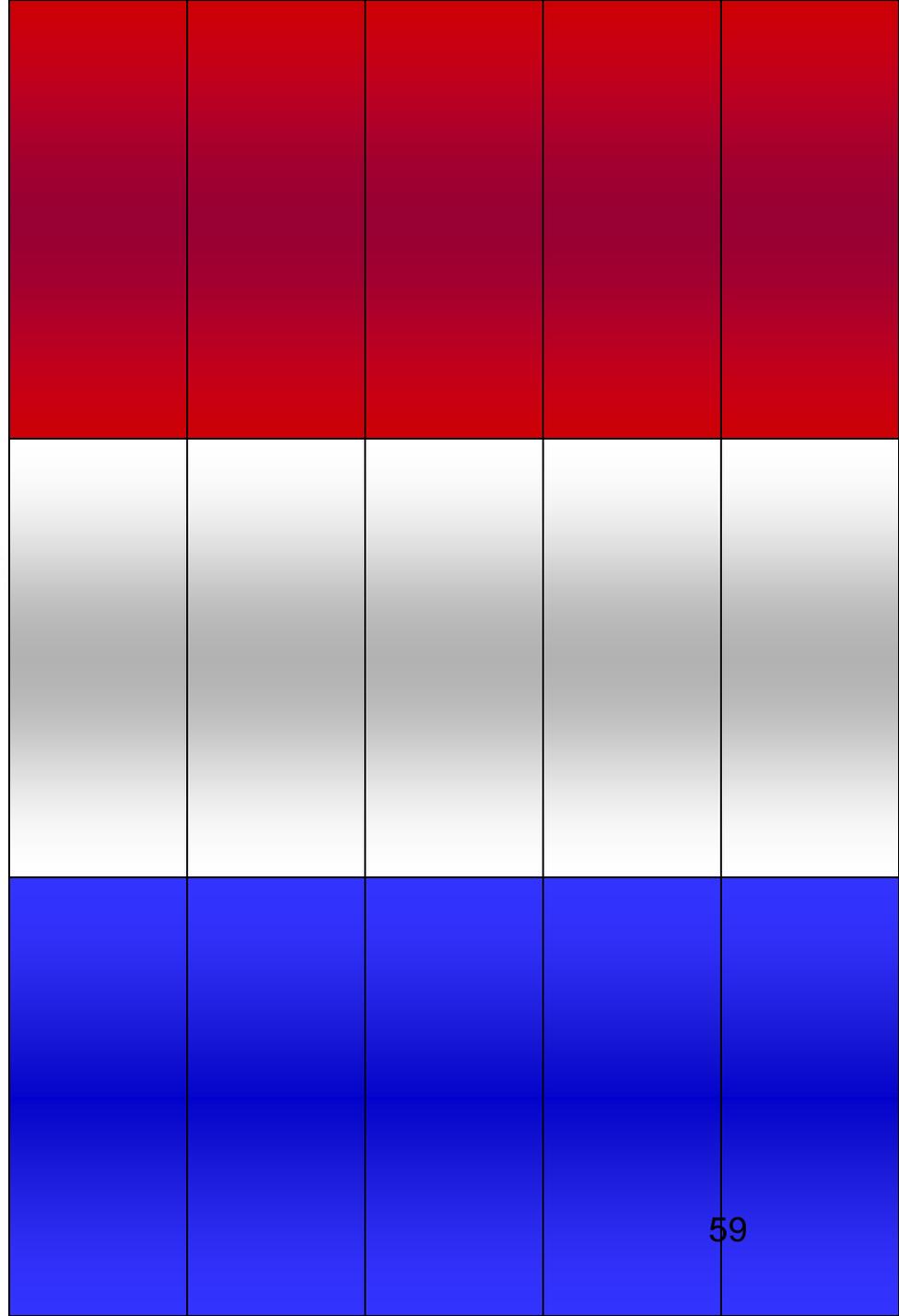
# What hacker group is represented?

1. Syrian Electronic Army
2. Legion of Doom
3. Chaos Computer Club
- ✓ 4. Anonymous
5. Level Seven



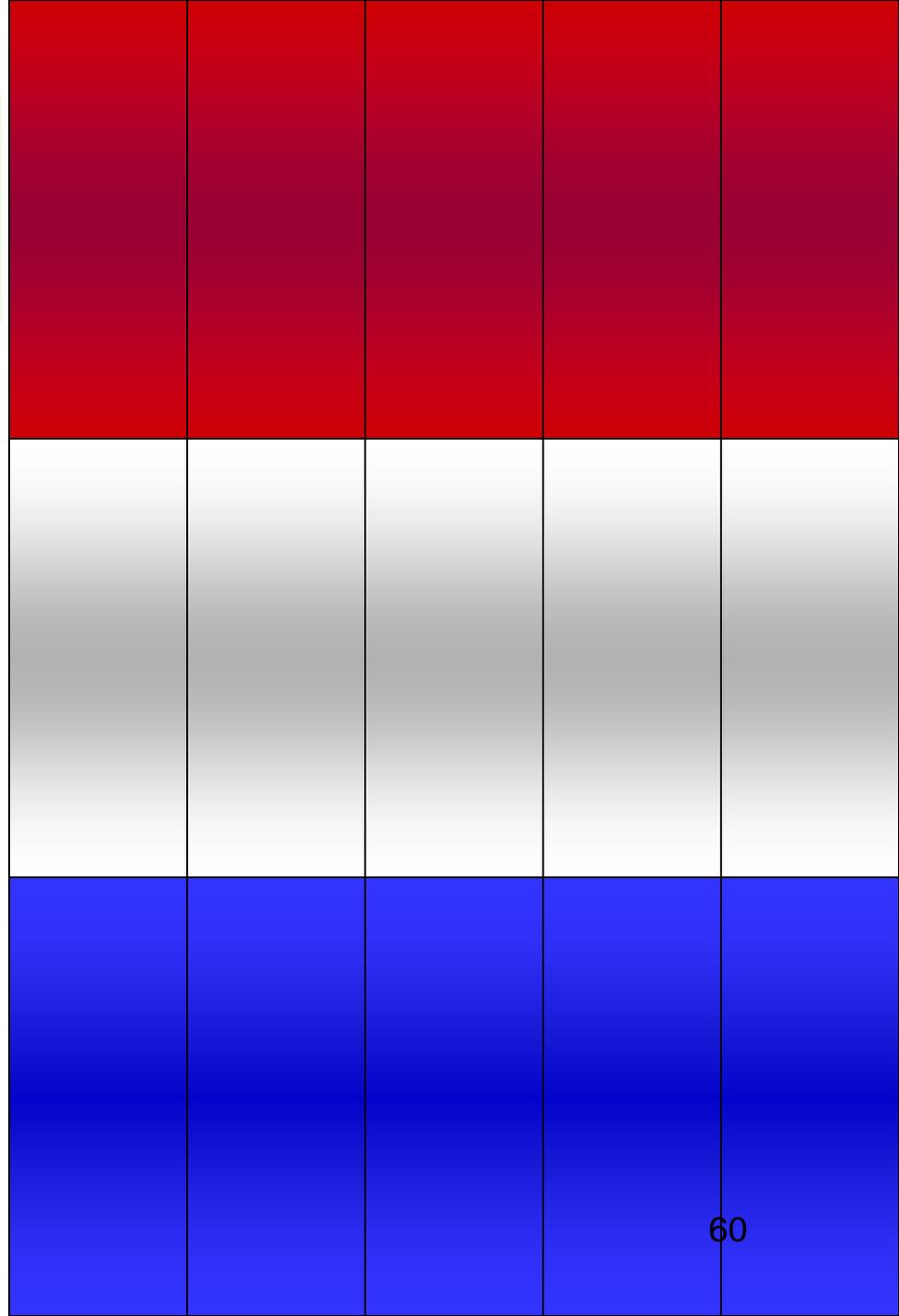
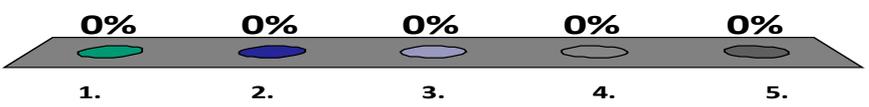
# What hacker group is represented here?

1. NCPH
2. UGNazi
3. Cult of the Dead Cow
4. Honker Union
- ✓ 5. LulzSec



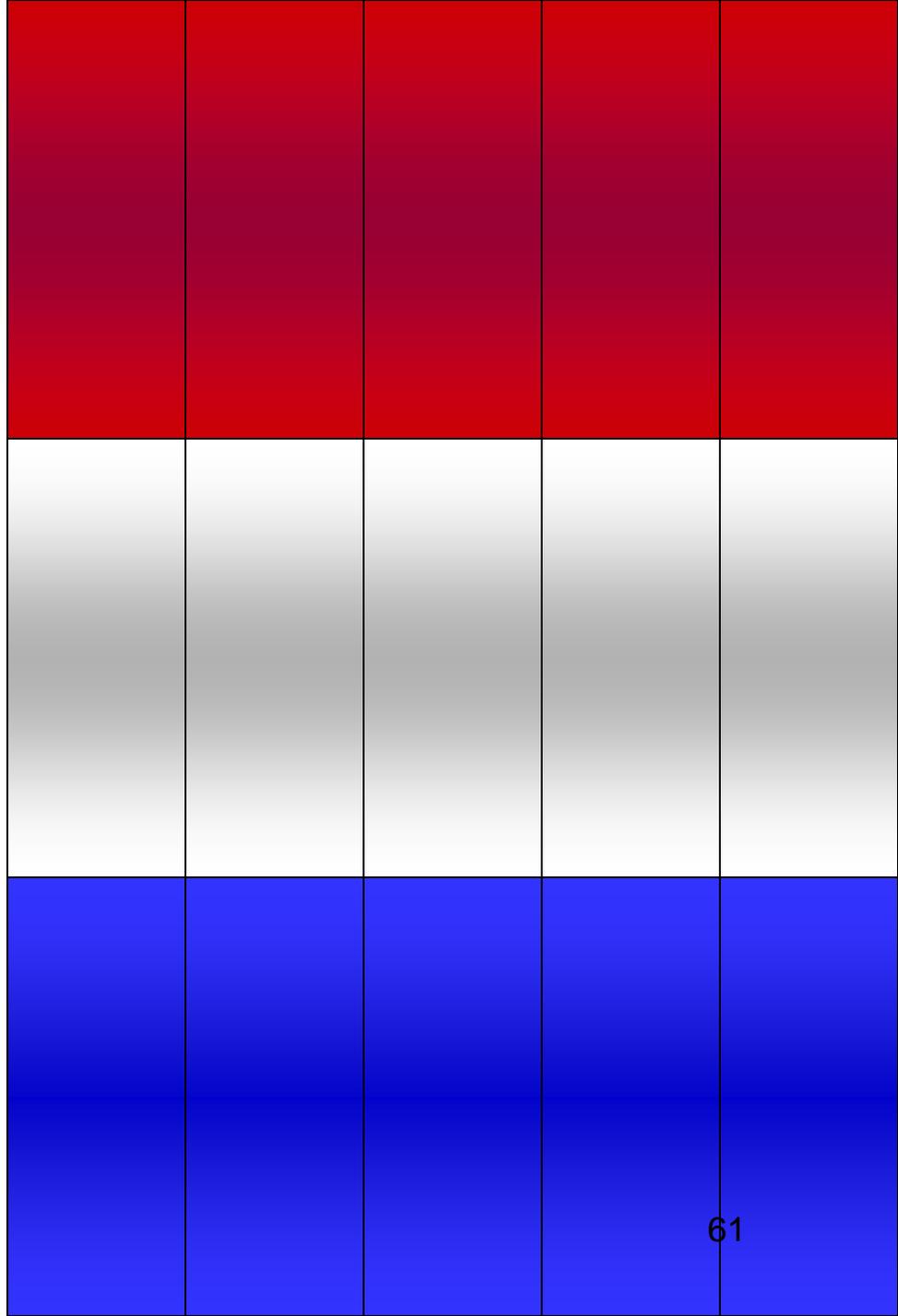
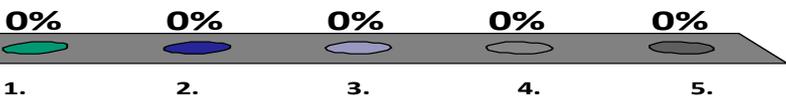
# What does this security graphic represent?

- 1. Multi-Factor Authentication
- 2. Public Key Infrastructure
- ✓ 3. OSI Model
- 4. Intrusion Layers
- 5. Network Segmentation



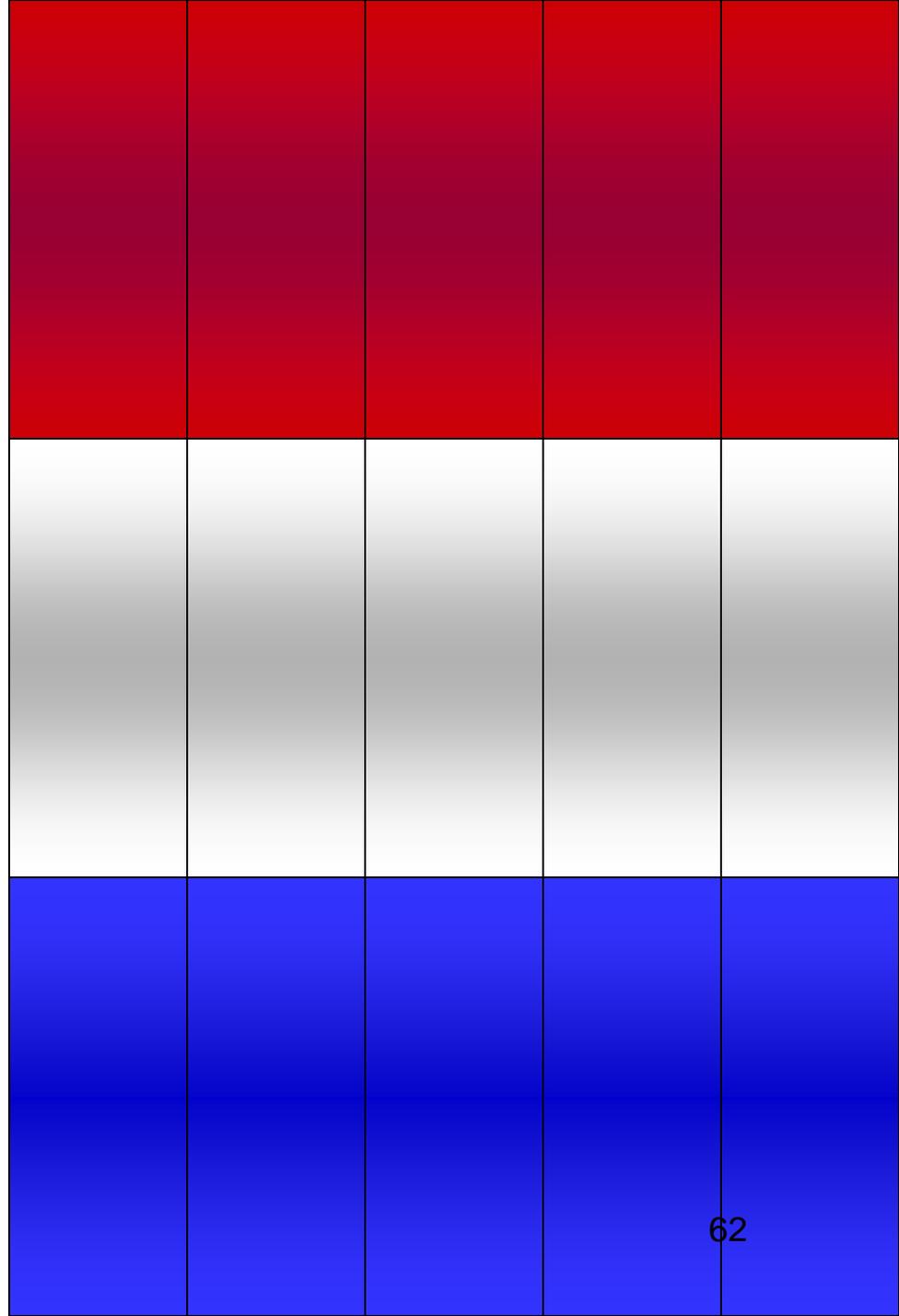
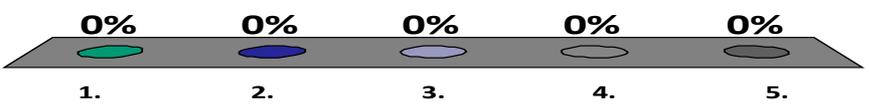
# What best describes this risk management tool?

- 1. Data Sensitivity Analysis
- 2. Threat-Vulnerability Dashboard
- 3. Mission Essential Functions Matrix
- ✓ 4. Risk Heat Map
- 5. Commonwealth Essential Functions



# What backup strategy is represented here?

- 1. Incremental
- 2. Differential
- 3. Full
- ✓ 4. Towers of Hanoi
- 5. Sequential



# Team Scores

**Points**

**Team**

**Points**

**Team**

# Participant Leaders

**Points**

**Participant**

**Points**

**Participant**



Virginia Information Technologies Agency


# In contingency planning, what is represented here?

1. Business Impact Analysis
- ✓ 2. VDEM Continuity Functions
3. Business Process Analysis
4. Mission Essential Functions
5. Risk Assessment Workflow

0%

1.

0%

2.

0%

3.

0%

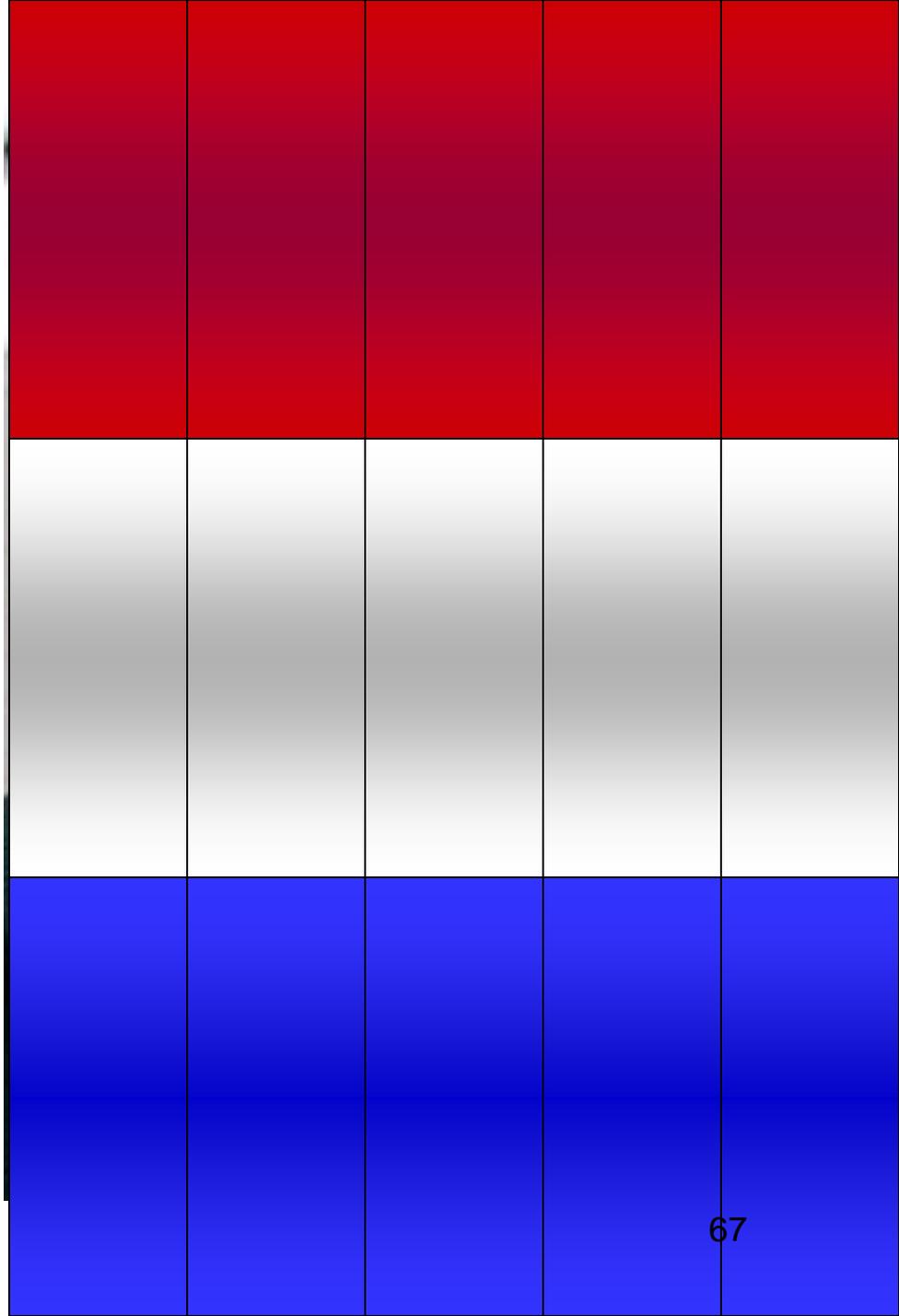
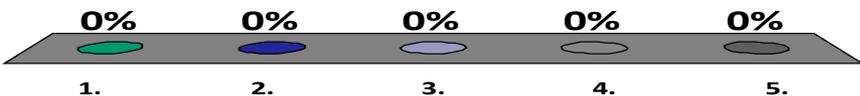
4.

0%

5.


Who said: “We know where you are. We know where you've been. We can more or less know what you're thinking about.”

- 1. Mark Zuckerberg/Facebook
- 2. Reid Hoffman/LinkedIn
- 3. Will Ferrell/SNL
- ✓ 4. Eric Schmidt/Google
- 5. Edward Snowden/NSA



# What does this pop-up represent?

- ✓ 1. Virus Warning
- 2. Data Overwrite Warning
- 3. Patch Notification
- 4. Critical Updates Available
- 5. Encryption Enabled

0%



1.

0%



2.

0%



3.

0%

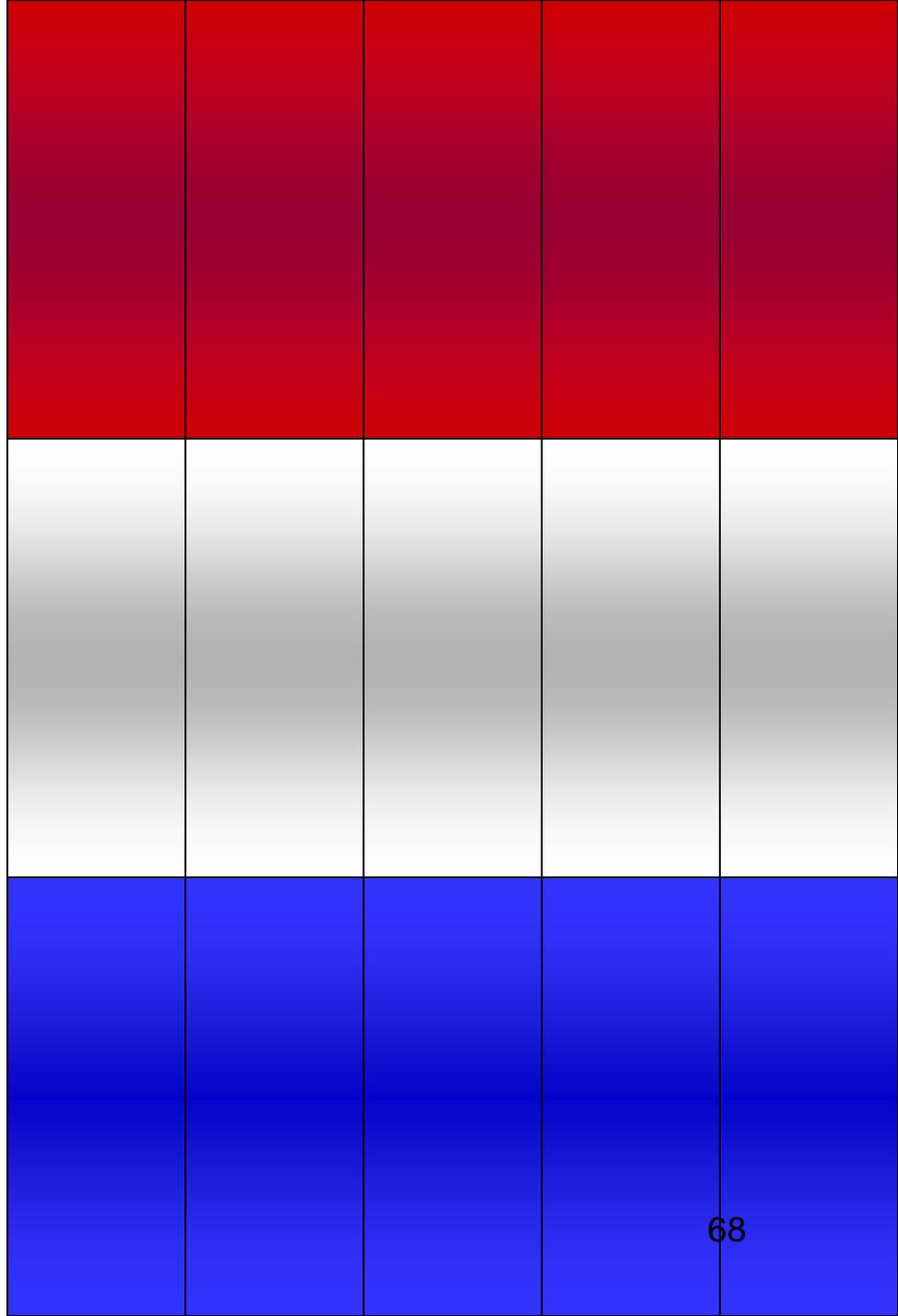


4.

0%



5.



# Who is this famous IT security guy?

1. Peter Norton
2. Brian Krebs
3. Will Ferrell
- ✓ 4. John McAfee
5. Bruce Schneier

0%

0%

0%

0%

0%

1.

2.

3.

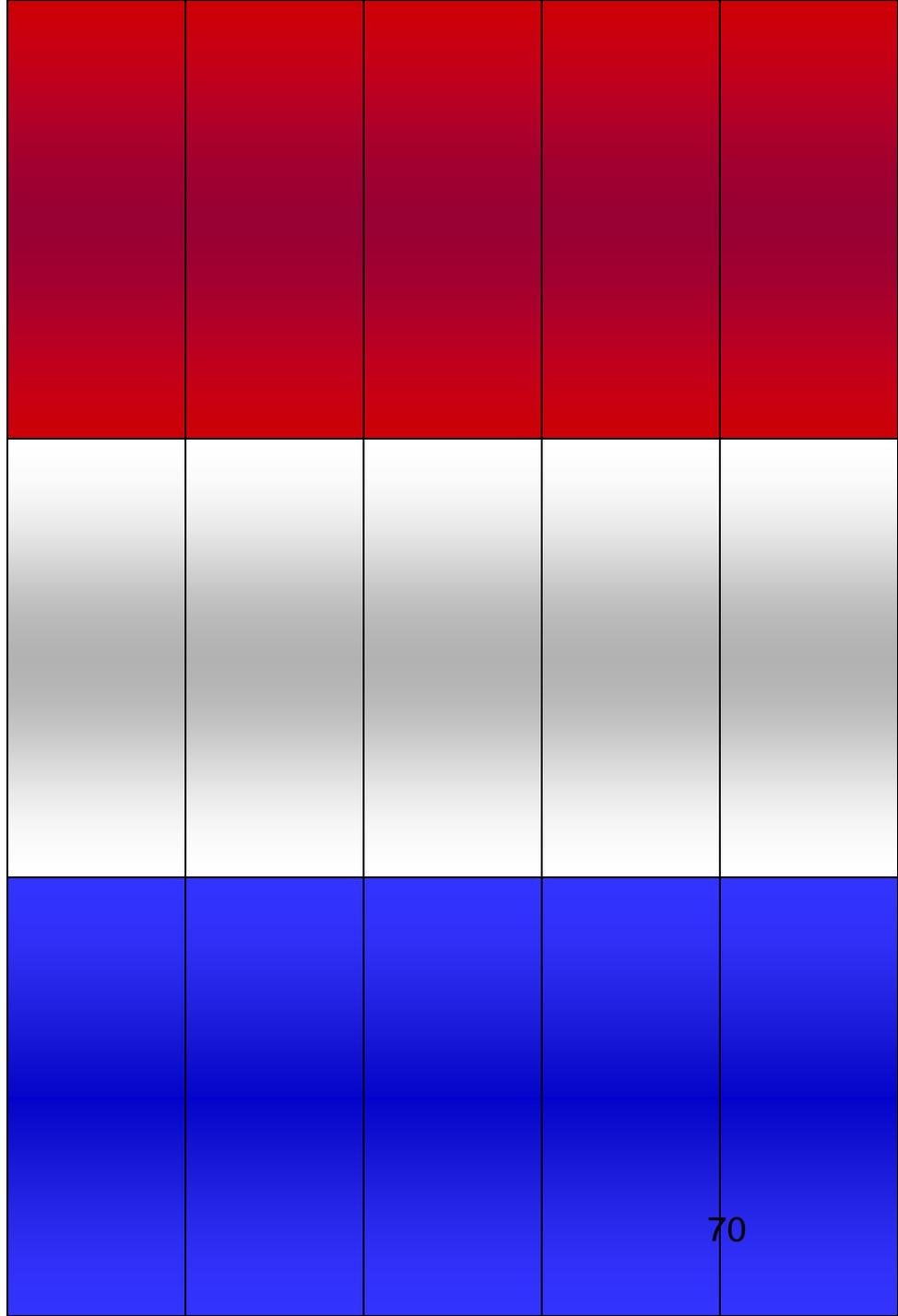
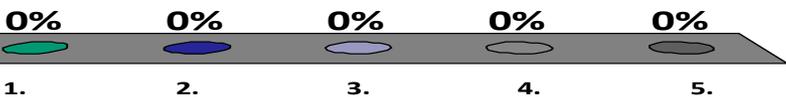
4.

5.

69

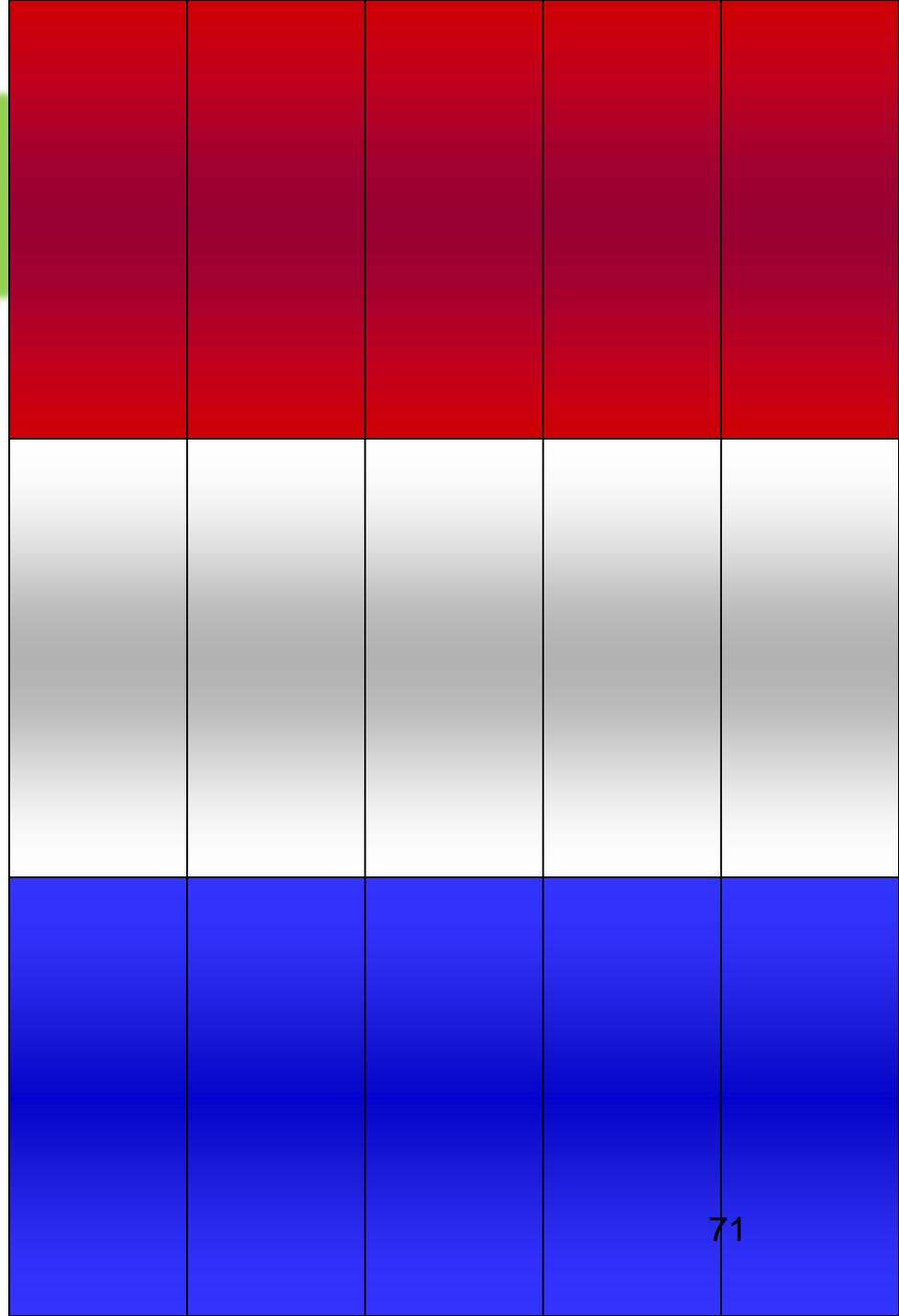
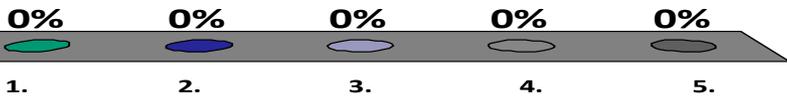
# What kind of controls are these?

1. System Specific Controls
2. Common Controls
- ✓ 3. NIST Control Families
4. Hybrid Security Controls
5. Control Domain Attributes



In this movie, a programmer was trapped inside a computer.

- ✓ 1. Tron
- 2. Swordfish
- 3. WarGames
- 4. Terminator
- 5. Hackers



# Team Scores

**Points Team**

**Points Team**



Virginia Information Technologies Agency

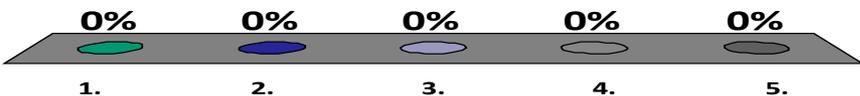
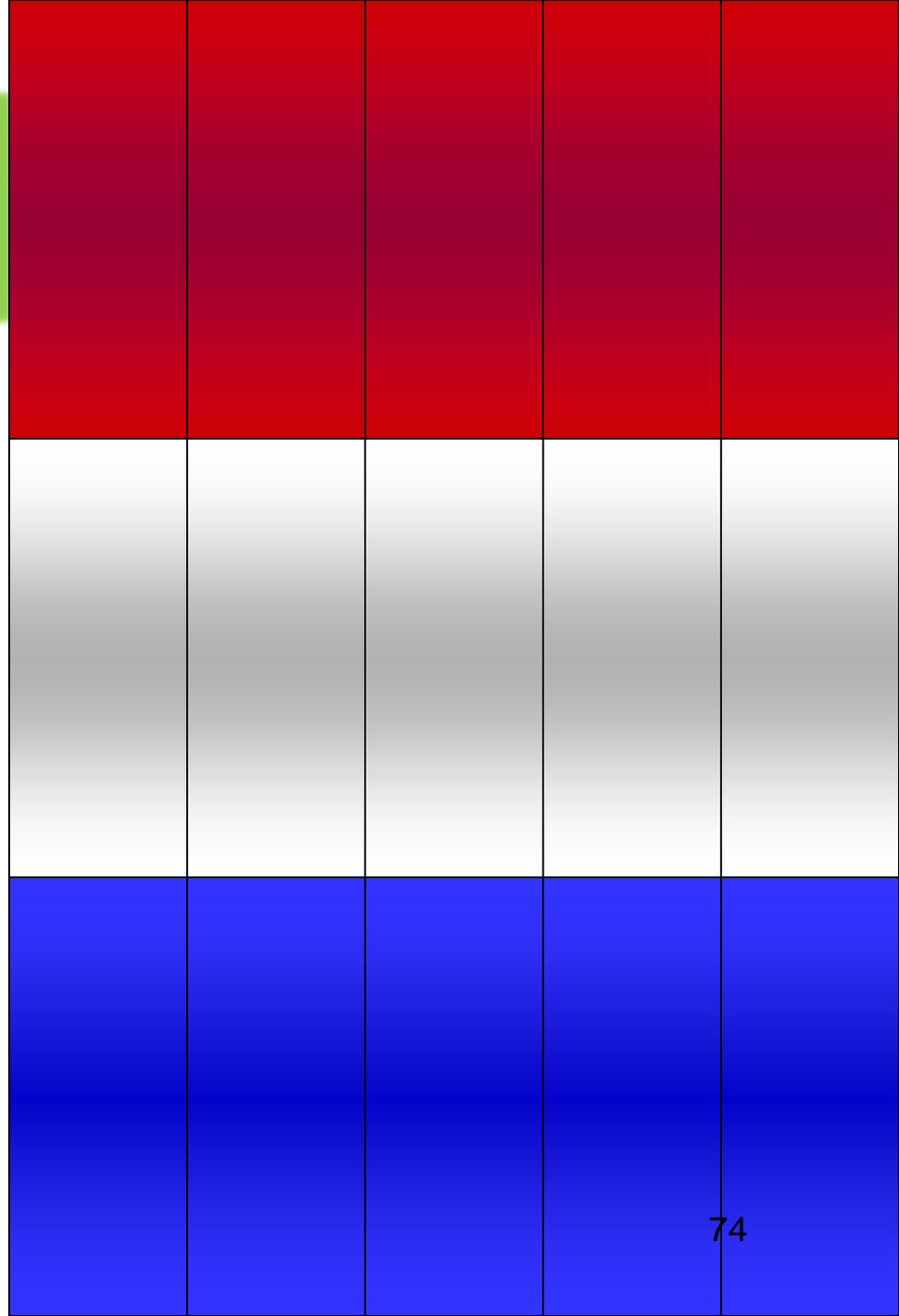


# Bonus Question

## 25 points!

What Will Ferrell character said:  
“I don’t know how to put this, but  
I’m kind of a big deal.” ?

1. Steve Butabi
2. Ricky Bobby
- ✓ 3. Ron Burgundy
4. Chazz Michael Michaels
5. Cam Brady





Game over!

# Team Racing Scores

# Team Scores

**Points Team**

**Points Team**

# Participant Leaders

**Points**

**Participant**

**Points**

**Participant**



*Thanks for playing*  
**Undercover Clicker!**



# UAC and DEP: Protection Mechanisms for Windows

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Historical Need for UAC

- Prior to User Account Control (UAC) an end-user logged on to a system as an administrator was automatically granted full access to all system resources.
- While utilizing an administrator account the end-user could unintentionally or intentionally install a malicious program.



## User Account Control - Basics

- UAC is a system facility used to inform the end user when an application requests a system change that requires administrator-level permission.
- UAC provides the ability to adjust the permission level of current user account to match the requirement of the executing application.



## User Account Control - Basics

- UAC can be configured to “dump” privileges if tasks such as reading e-mail or creating documents are performed using an account with administrator privileges.



## User Account Control - Basics

- UAC provides a facility to temporarily provide the needed administrative rights to complete the requested task and then reduce privilege levels back to that of a standard user.
- This facility can prevent unintended and unannounced changes to the system.



## User Account Control - Prompts

- UAC utilizes one of four types of dialog boxes to notify the user of an administrative-level change.
- Each dialog box will provide guidance on how to respond to the request.



## User Account Control - Prompts

- Native Windows Settings or Features
- This type of update will have a valid digital signature that verifies that Microsoft is the publisher.
- Microsoft recommends that it is safe to proceed.



## User Account Control - Prompts

- A Program that not supplied by Microsoft
- This type of update will have a valid digital signature from the software vendor.
- Microsoft recommends verifying that the software should be implemented as well as that the software vendor is trusted by the organization.



## User Account Control - Prompts

- A Program from an unknown publisher
- This type of update does not have a valid digital signature. Many legacy software packages are not signed by the software vendor.
- Microsoft recommends that extra caution be used and the software should only be permitted if from a trusted source.



## User Account Control - Prompts

- Software update blocked by administrator
- This type of update has been determined to be not trustworthy.
- Microsoft recommends that the user contact the system administrator.



## Permission Level Recommendations

- The standard user account should be used for everyday activities such as browsing the Internet, sending e-mails, or utilizing an office suite.
- The standard user account can also be used when installing a new program or changing a system setting since the system will prompt for permission to perform the task.



## UAC Decision Factors

- Things to consider when the UAC box pops up (software installation/configuration change):
  - Check the name of the program, the publisher information, and the certificate information.
  - Is the software from a trusted source such as the original CD or a publisher's website.
  - Research the software to determine if it's a known program or malicious software.



## UAC Changes for Windows 7

- Increased the number of tasks that the standard user can perform that do not prompt for administrator approval.
- Allow a user with administrator privileges to configure the UAC experience in the Control Panel.



## UAC Changes for Windows 7

- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for local administrators in Admin Approval Mode.
- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for standard users.



## UAC Changes for Windows 7

- By default, standard users and administrators access resources and run applications in the security context of standard users.
- The system will create an access token for the standard user. The access token contains information about the level of access granted, including specific security identifiers (SIDs) and Windows privileges.



## UAC Changes for Windows 7

- The system will create two separate access tokens when an administrator logs into the system: a standard user access token and an administrator access token.
- The standard user access token contains the same user-specific information as the administrator access token, but the administrative Windows privileges and SIDs have been removed.



## UAC Changes for Windows 7

- The standard user access token is used to start applications that do not perform administrative tasks.
- When the application must perform an administrative task the user must change or "elevate" the security context to an administrator (called Admin Approval Mode).



## UAC Events

- Any tasks that require administrator privileges will generate a UAC prompt
- The event are marked by a security shield icon with the 4 colors of the Windows logo for Vista and Windows Server 2008 or with two panels yellow and two blue for Windows 7 and Server 2008 R2.



## UAC Events

- Executing the application as an Administrator
- Changes to system-wide settings or to files in %SystemRoot% or %ProgramFiles%
- Installing and uninstalling applications



## UAC Events

- Installing device drivers
- Installing ActiveX controls
- Changing settings for Windows Firewall
- Changing UAC settings
- Configuring Windows Update



## UAC Events

- Adding or removing user accounts
- Changing a user's account type
- Configuring Parental Controls
- Running Task Scheduler
- Restoring backed-up system files



## UAC Events

- Viewing or changing another user's folders and files
- Running Disk Defragmenter
- Changing the system time itself since the system time is commonly used in security protocols such as Kerberos.

## Data Execution Prevention

- DEP is a security feature included in most modern operating systems including Microsoft Windows, Linux, Mac OS X, iOS, and Android.
- DEP is designed to prevent an application or service from executing code from a non-executable memory region, thus preventing exploits that store code in that region via a buffer overflow.



## Data Execution Prevention

- DEP is based on the Linux Write XOR Execute memory protection facility.
- Marks areas of memory as either writeable or executable, but not both.
- DEP is designed to prevent code execution of code loaded onto the process stack or the function's heap area.



## Data Execution Prevention

- Executable code should only be loaded into pages explicitly marked for code execution such as the code segment.
- Any attempt to run code from a page marked non-executable will generate an exception and the process will terminate.



## Memory Basics – The Heap

- Program code is loaded into an area of memory known as the Heap.
- The Heap contains four memory segments:
  - Code Segment
  - Data Segment
  - BSS Segment
  - Heap Segment



## Memory Basics – The Code Segment

- The Code segment holds the executable instructions for a program.
- The Code segment is often loaded into a lower memory location than the other segments.
- Since the Code segment holds executable code it should be non-writable.

## Memory Basics – The Data Segment

- The Data segment holds the initialized global variables used by the program.
- This segment holds initialized variables:
  - `int y = 1;`
  - `char *MyString = "Hello World";`
- Since the Data segment holds variables it should be non-executable.

## Memory Basics – The BSS Segment

- The BSS segment holds the uninitialized for the program such as:
  - `int Y;`
  - `char *OpenString;`
- Since the BSS segment holds variables it should be non-executable.
- So what does BSS stand for???



## Memory Basics – The Heap Segment

- The Heap segment is a very dynamic area of memory.
- Used to hold user data or feature-rich application content
- Since the Heap segment holds variables and other application content it should be non-executable.

# Data Execution Prevention Modes

- DEP supports two modes:
  - Hardware mode enforces DEP via registers in the CPU that mark memory pages as not executable
  - Software mode enforces DEP on those systems that do not provide hardware support in the CPU.
  - Software mode does not protect against execution of code in data pages but instead counters SEH overwrite



## DEP Hardware Enforcement

- Hardware mode DEP enables the NX (No Execute) bit on AMD processors and the XD (Execute Disable) bit on Intel processors.
- Hardware mode DEP requires the use of the PAE kernel for 32-bit Windows and is supported natively on 64-bit kernels.



## DEP Software Enforcement

- The function must be compiled with Software DEP/SafeSEH enabled.
- The vast majority of Microsoft Windows DLLs and Microsoft programs have been compiled to support Software DEP/SafeSEH.
- To fully secure a program all related files must be compiled to support SafeSEH.

## DEP Software Enforcement

- Software DEP is also known as SafeSEH in the Microsoft Windows world.
- Software DEP/SafeSEH builds a table of trusted exception handling routines during code compilation and then verifies that any exception raised by the running function is registered in that function's exception table.

## DEP Software Enforcement

- If a function generates an exception only the trusted exception handling routines will be allowed to execute.
- If a trusted exception handler cannot be found for the raised exception, the “Unhandled” exception handler will be invoked to terminate the process.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



Virginia Information Technologies Agency

# Upcoming Events





## COVITS 2013

*COVITS is a forum to discuss technology requirements, share valuable lessons from actual case studies, and glimpse the future of government interaction with its customers.*

***September 9 & 10***

***Richmond Marriott***

500 East Broad Street, Richmond, VA 23219

***Register Here:*** <http://www.govtech.com/events/COVITS-2013.html>



## IS Orientation

**When: Thursday, Sept 5, 2013**

**Time: 10:00 am to Noon**

**Where: CESC , Room 1221**

**Register here:**

**<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>**

Next IS Orientation will be held on Dec 5, 2013



## Future ISOAG Dates

**Aug 7**                    **1:00 – 4:00 pm @ CESC**  
**Keynote Speaker: Bennie Moore, Fed Reserve Bank**  
**on “Crisis Management in Incident Response”**

**Sep 4**                    **1:00 – 4:00 pm @ CESC**  
**Keynote Speaker: Dr. Larry Wortzel, Asia Strategies & Risk, LLC**  
**on “Chinese Cyber-Security Threat”**

**Oct 2**                    **1:00 – 4:00 pm @ CESC**  
**Keynote Speaker: Hank Leininger, Kore Logic**  
**on “Passwords & Password Cracking”**

**ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2013**



## SANS 2013 Aggregate Buy Reminder

- 2013 Pricing through the SANS “Government Partnership” Aggregate Buy. Now thru 07/31/2013

The program offers two opportunities, *SANS Security Awareness Training* and *SANS OnDemand* classes via the SANS group flex pass method.

- **\*\*This is a good opportunity, but agencies need to follow the Virginia Public Procurement Act (VPPA) and their agencies' procurement rules.**
- For more information please contact:
  - [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



## Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

10 July, 2013



**NORTHROP GRUMMAN**



# ADJOURN

