

osisoft.
USERS 2013
CONFERENCE
The **Power of Data**
E M E A

THRIVING IN A WORLD OF CHANGE



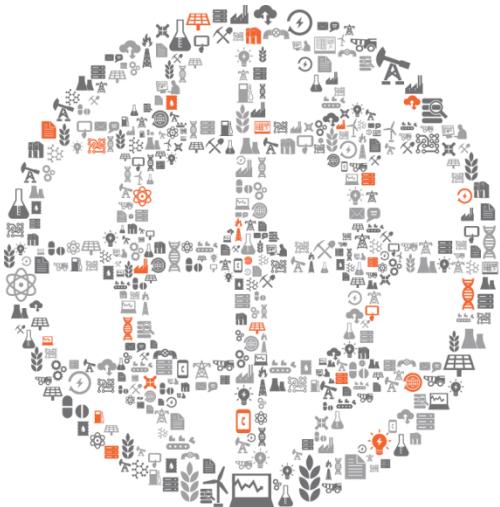


New Technologies for Cyber Security

Presented by

Bryan Owen
bryan@osisoft.com
Cyber Security Manager
OSIsoft, LLC

Jim Davidson
jdavidson@osisoft.com
Security Products Manager
OSIsoft, LLC



OSIsoft®

USERS CONFERENCE 2013

The Power of Data

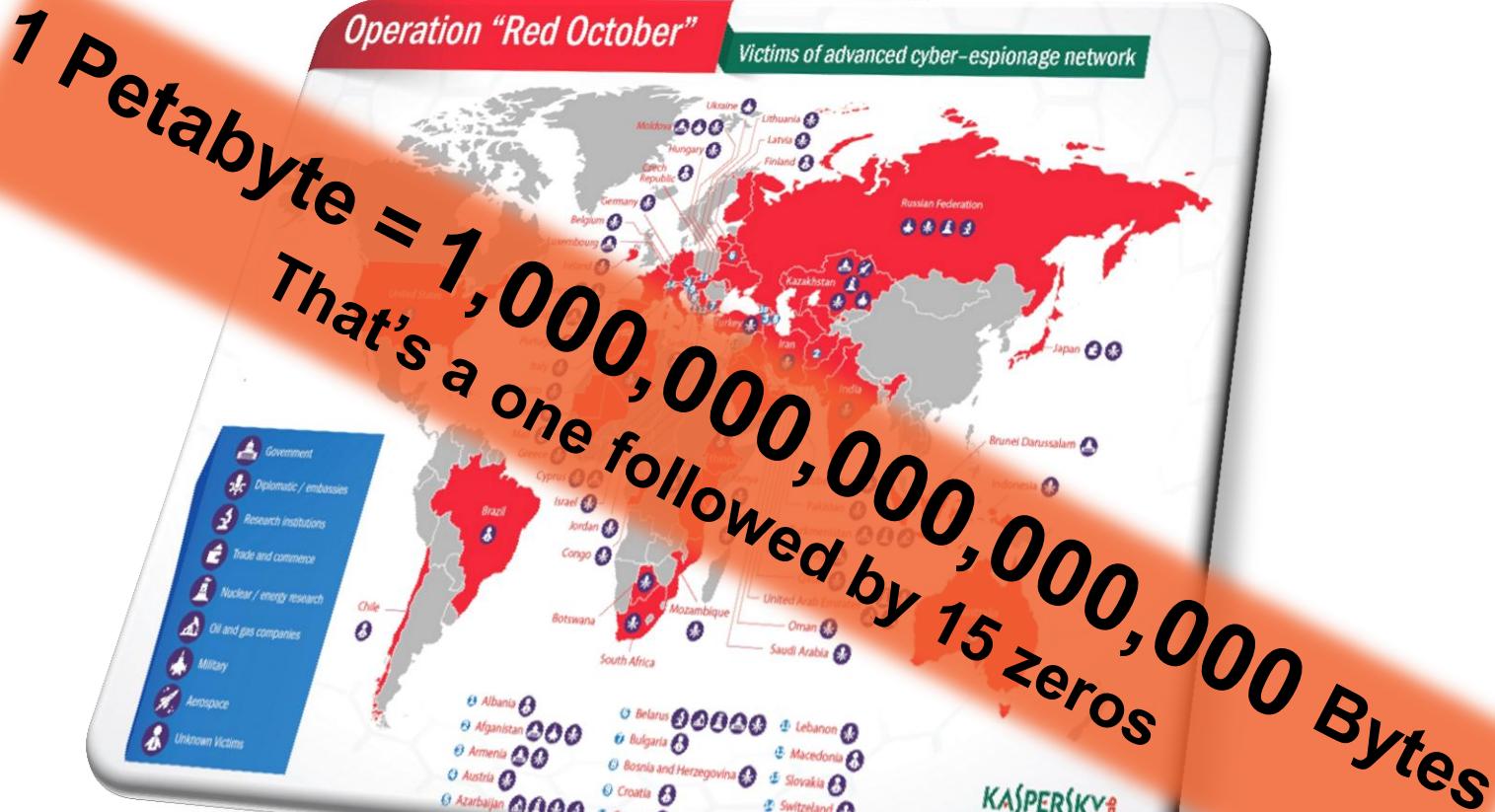
THRIVING
IN A
WORLD OF
CHANGE

E

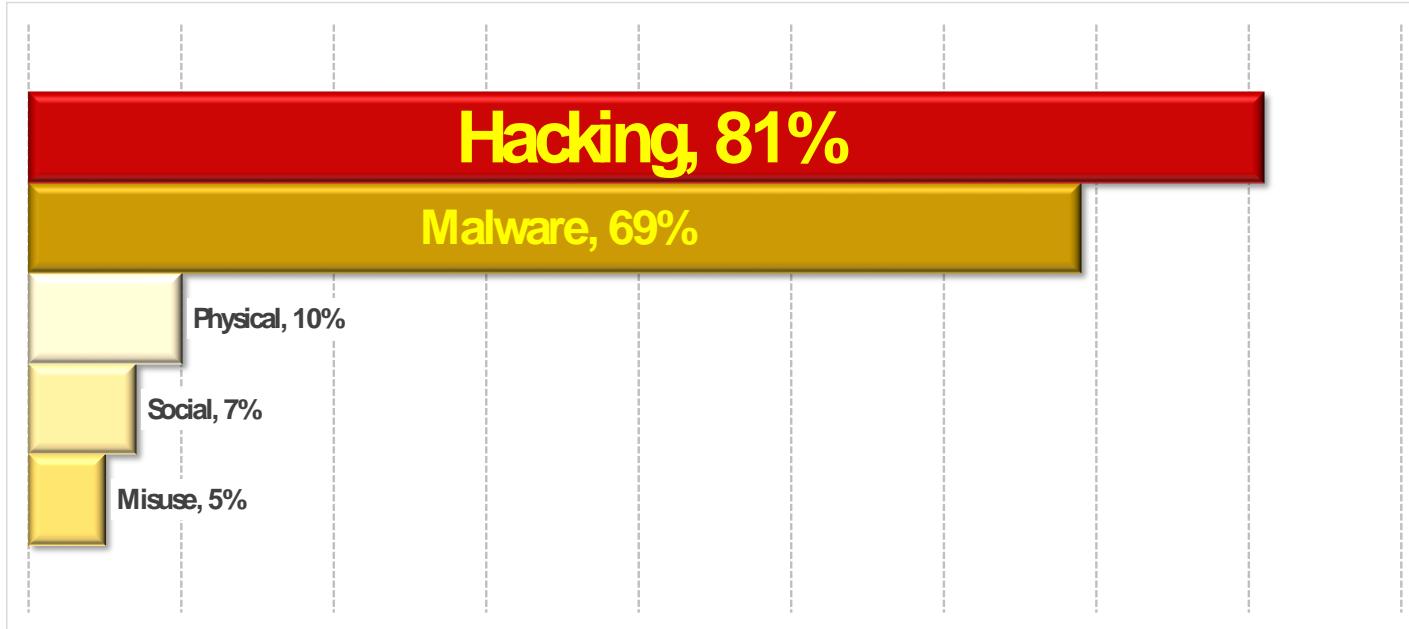
M

E

A



How Do Breaches Occur?



2012 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service.



Strategies to Mitigate Targeted Cyber Intrusions

Australia Becomes First Nation To Discover Reliable Method of Stopping Targeted Attacks (October 30 & 31, 2012)

.... implementing just the top four strategies can block 85% of targeted cyber attacks

<http://www.dsdc.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm>

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
1	Application whitelisting of permitted/trusted programs. To prevent executing malicious and unknown programs	Essential	Medium	High	Medium	Both	Yes	Yes	Yes
2	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate high risk vulnerabilities within two days of Adobe Reader prior to X.	Essential	Low	High	High	Prevent	Yes	Possible	No
3	Patch operating system vulnerabilities. Patch or mitigate high risk vulnerabilities in desktops running Windows XP or earlier	Essential	Low	Medium	Medium	Prevent	Yes	Possible	Possible
4	Minimise the number of users with domain or local administrative privileges. All users should have a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Medium	Prevent	Yes	Possible	

1- APPLICATION WHITELISTING

2- PATCH APPLICATIONS

3- PATCH OPERATING SYSTEM

4- LEAST PRIVILEGES

Whitelisting

Applications

Microsoft's Applocker

Windows 2008 & 2012

Windows 8 Pro

Communications

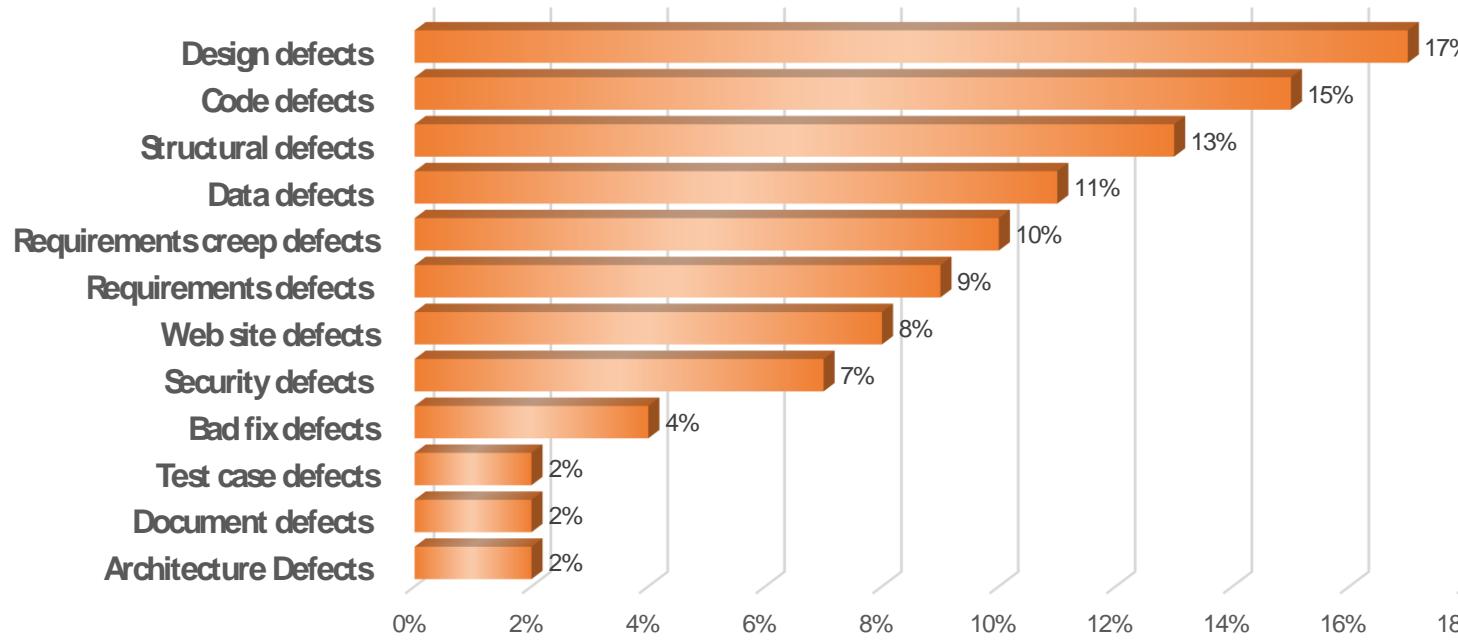
Windows Firewall

All Current Versions of
Windows

Enable Output Rules

All Software Has Bugs

Origins of High Severity Software Defects



Source: SOFTWARE QUALITY IN 2011: A SURVEY OF THE STATE OF THE ART (Capers Jones)

Security Development Lifecycle

Essential Processes and Practices for:

Reducing the Number of Vulnerabilities

Reducing the Severity of Vulnerabilities

Increasing the Resiliency of the Software

Increasing the Reliability of the Software



OSIsoft's Responsibility

Example: PI Server 2012

19 New Security Bugs Found and Fixed

Reduced exploitability (software resilience)

Buffer Overrun Detection

SEH - Safe Exception Handling Protection

SEHOP – Structured Exception Handling Protection

DEP/NX – Data Execution Prevention and No eXecute

ASLR – Address Space Layout Randomization

Heap Metadata Protection



Continuous Improvement



Patch/Upgrade PI Software

- Each Revision Reduces Bugs
- 64 Bit Versions are more Secure
- PI Server 2012 Certified on Windows Core
- PI AF Server 2012 Tested on Windows Core
- MSSQL Server 2012 Certified on Windows Core

Patch/Upgrade OS

Servers (Running on Windows Core where possible)

- Windows 2012 or
- Windows 2008 R2

Clients

- Windows 8 or
- Windows 7



Windows OS retirement coming

(No further security updates from Microsoft)

- Windows XP support ends in April 2014
- Window Server 2003 support ends in July 2015

Windows Core

- No Graphical User Interface (GUI)
- No Graphic Based Applications
- Smaller Faster Code Base
- More Resources Available
- Fewer Patches Needed
- Less Maintenance
- Lower Total Cost of Ownership

Least Privileges

Do not use piadmin account

Use Windows Integrated Security (WIS)

Enable Windows User Account Control (UAC)

Create Users and Trusts based on Least Privileges

The Top 4

1: Use Whitelisting Techniques

2: Upgrade your PI Software

3: Upgrade your Operating System

Use Windows Server Core for Servers

4: Least Privileges

Additional Information

OSIsoft Links

- Whitelisting guidance
- For the latest in PI security use Search string “PI Security Best Practices”
<http://techsearch.osisoft.com/Pages/results.aspx?k=pi%20security%20best%20practices>
- Product documentation on core
- For Windows Security Requirements look at this technical article:
<http://techsupport.osisoft.com/Support+Solution/8/KB00354.htm>
- OS support

External links

Verizon - 2012 Data Breach Investigations Report:
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?_ct_return=1

Australian Defence Signals Directorate - Strategies to Mitigate Targeted Cyber Intrusions:

<http://www.dsdc.gov.au/infosec/top35mitigationstrategies.htm>

Honeywell Whitepaper on Application Whitelisting:

http://www.controleng.com/fileadmin/content_files/ce/honeywell-iits-wp-application-whitelisting.pdf

EA Customers

Contact Your EPM or CoE to Learn More about Best Practice Availability

Please don't forget to.....

Complete the Online Survey
for this session



Eventmobi.com/emeauc13

Share what you saw with
friends on Twitter, Facebook
or LinkedIn!

#UC2013





THANK
YOU

Brought to you by



vCampus Live! 2013 - OSIsoft Annual Technical Conference



DECEMBER 3 - 6, GRAND HYATT SAN FRANCISCO

vCampus Live! 2013

WHERE PI GEEKS MEET



S A V E T H E D A T E

