The PMC Group LLC

Engineering a better tomorrow today

Cybersecurity: Protecting Your Buildings - and Your Company

Michael Chipley, PhD GICSP PMP LEED AP
President

April 23, 2015

mchipley@pmcgroup.biz

Agenda

Cyber attacks on Building Control Systems and IT
New federal Acquisition and Procurement Language
Overview of Building Control Systems
Exploiting Building Control Systems
Protecting Building Control Systems

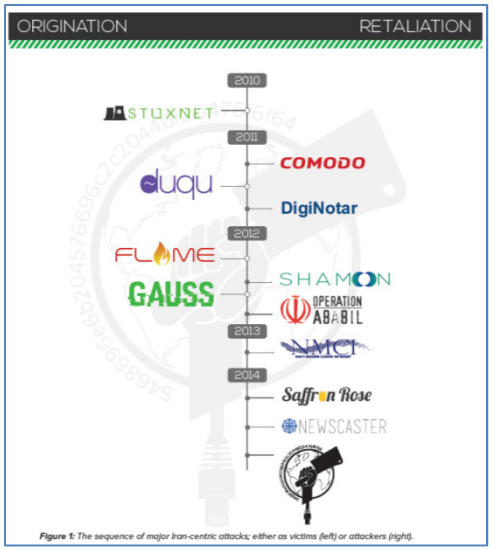
Operation Cleaver - Iran

- Iranian team dubbed Tarh Andishan
- Believed to consist of at least 20 hackers and developers, collaborating on projects and missions to support Iranian interests
- Evolved skillset and uses a complex infrastructure to perform attacks of espionage, theft, and the ***potential destruction of control systems and networks***
- Over 50 victims, distributed around the globe
- 10 victims are headquartered in the US and include a major airline, a medical university, an energy company specializing in natural gas production, an automobile manufacturer, ***a large defense contractor, and a major military installation***.

WHY THE NAME CLEAVER?

The string cleaver is found several times in a variety of custom software used in Operation Cleaver, including inside the namespaces of their custom bot code TinyZBot, e:\projects\cleaver\trunk\zhoupin_**cleaver**\obj\x86\release\netscp.pdb

Targets and Access



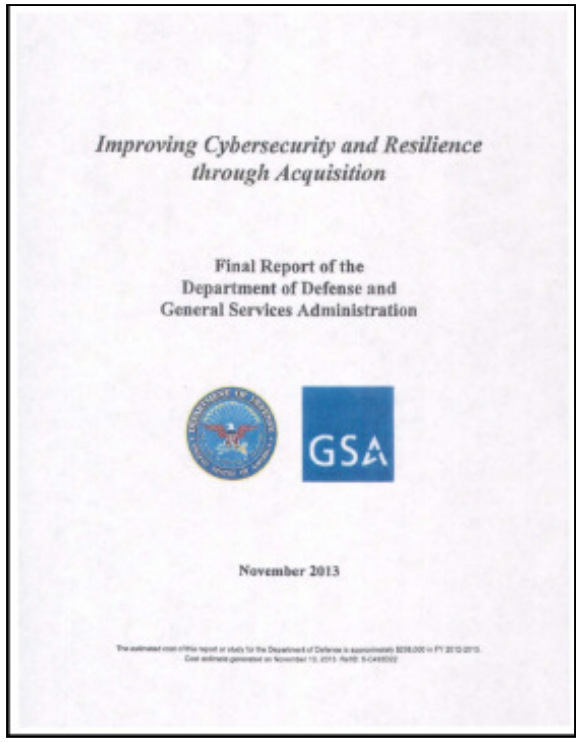
- Targeting and compromise of transportation networks and systems
- Level of access seemed ubiquitous: Active Directory domains were fully compromised, along with entire Cisco Edge switches, routers, and internal networking infrastructure
- Fully compromised VPN credentials meant their ***entire remote access infrastructure and supply chain*** was under the control of the Cleaver team, allowing ***permanent persistence*** under compromised credentials
- Achieved ***complete access to airport gates and their security control systems***
- Gained access to PayPal and Go Daddy credentials allowing them to make fraudulent purchases and allowed ***unfettered access to the victim's domains***

What's At Stake?

- Persian hacker names are used throughout the campaign including: Salman Ghazikhani, Bahman Mohebbi, Kaj, Parviz, Alireza, and numerous others.
- Numerous domains used in the campaign were registered in Iran
- Spearfishing using resumes, multiple domains were registered in order to make the download sites seem more realistic (Teledyne-Jobs.com, Doosan-Job.com, NorthropGrumman.net)
- ***To date it has successfully evaded detection by existing security technologies***
- ***Confirmed hacking into unclassified U.S. Navy computers in San Diego's NMCI (Navy Marine Corp Intranet)***
- Iran is no longer content to retaliate against the US and Israel alone, position themselves to impact critical infrastructure globally

Mitigation: identify their presence in your network, prevent them from expanding the scope of the compromise, and remove their access **immediately**.

GSA-DoD Acquisition Reform

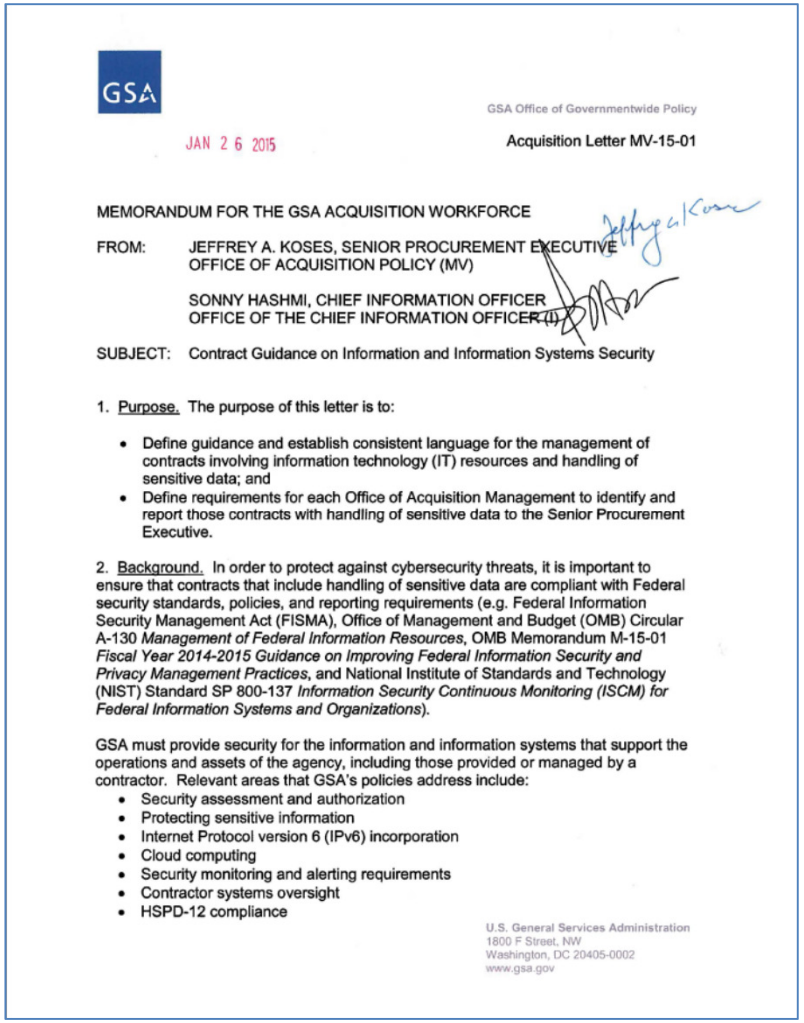


Six reform recommendations:

1. Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions
2. Include cybersecurity in acquisition training
3. Develop common cybersecurity definitions for federal acquisitions
4. Institute a federal acquisition cyber risk management strategy
5. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other trusted sources
6. Increase government accountability for cyber risk management

http://www.gsa.gov/portal/content/176547

GSA IT Acquisition Memo Jan 2015



GSA

GSA Office of Governmentwide Policy

JAN 2 6 2015

Acquisition Letter MV-15-01

MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE

FROM: JEFFREY A. KOSES, SENIOR PROCUREMENT EXECUTIVE
OFFICE OF ACQUISITION POLICY (MV)

SONNY HASHMI, CHIEF INFORMATION OFFICER
OFFICE OF THE CHIEF INFORMATION OFFICER (I)

SUBJECT: Contract Guidance on Information and Information Systems Security

1. Purpose. The purpose of this letter is to:

- Define guidance and establish consistent language for the management of contracts involving information technology (IT) resources and handling of sensitive data; and
- Define requirements for each Office of Acquisition Management to identify and report those contracts with handling of sensitive data to the Senior Procurement Executive.

2. Background. In order to protect against cybersecurity threats, it is important to ensure that contracts that include handling of sensitive data are compliant with Federal security standards, policies, and reporting requirements (e.g. Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130 *Management of Federal Information Resources*, OMB Memorandum M-15-01 *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, and National Institute of Standards and Technology (NIST) Standard SP 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*).

GSA must provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by a contractor. Relevant areas that GSA's policies address include:

- Security assessment and authorization
- Protecting sensitive information
- Internet Protocol version 6 (IPv6) incorporation
- Cloud computing
- Security monitoring and alerting requirements
- Contractor systems oversight
- HSPD-12 compliance

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Appendix D

New Contract Language

The following language shall be included in the Statement of Work, or equivalent, for all procurements where contractors may require access to sensitive data, or use information technology (IT) resources.

[Begin Paragraph]

Safeguarding Sensitive Data and Information Technology Resources

In accordance with FAR 39.105, this section is included in the contract.

This section applies to all users of sensitive data and information technology (IT) resources, including awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

Contract Cyber Risk Management Plan

(e) Order Cybersecurity Risk Management Plan (OCRMP) Submittal, Review, and Acceptance
(1) Submittal.
(i) When submitting a proposal in response to any task order solicitation, Contractor shall **submit its approved CCRMP** to the ordering contracting officer **as an addendum to the proposal**.
(ii) If required by the task order solicitation, Contractor shall also provide an Order Cybersecurity Risk Management Plan (OCRMP) that includes additional information to address the specific security requirements of the task order solicitation.

(f) Order Cybersecurity Risk Management Plan Update, Review, and Acceptance
(1) Updates.
(i) Contractor may update its OCRMP at any time after order award to ensure the Government is adequately assured of Contractor's continuous ability to provide appropriate cybersecurity in the deliverables it provides under the contract.

CCRMP based on NIST SP 800-53 R4

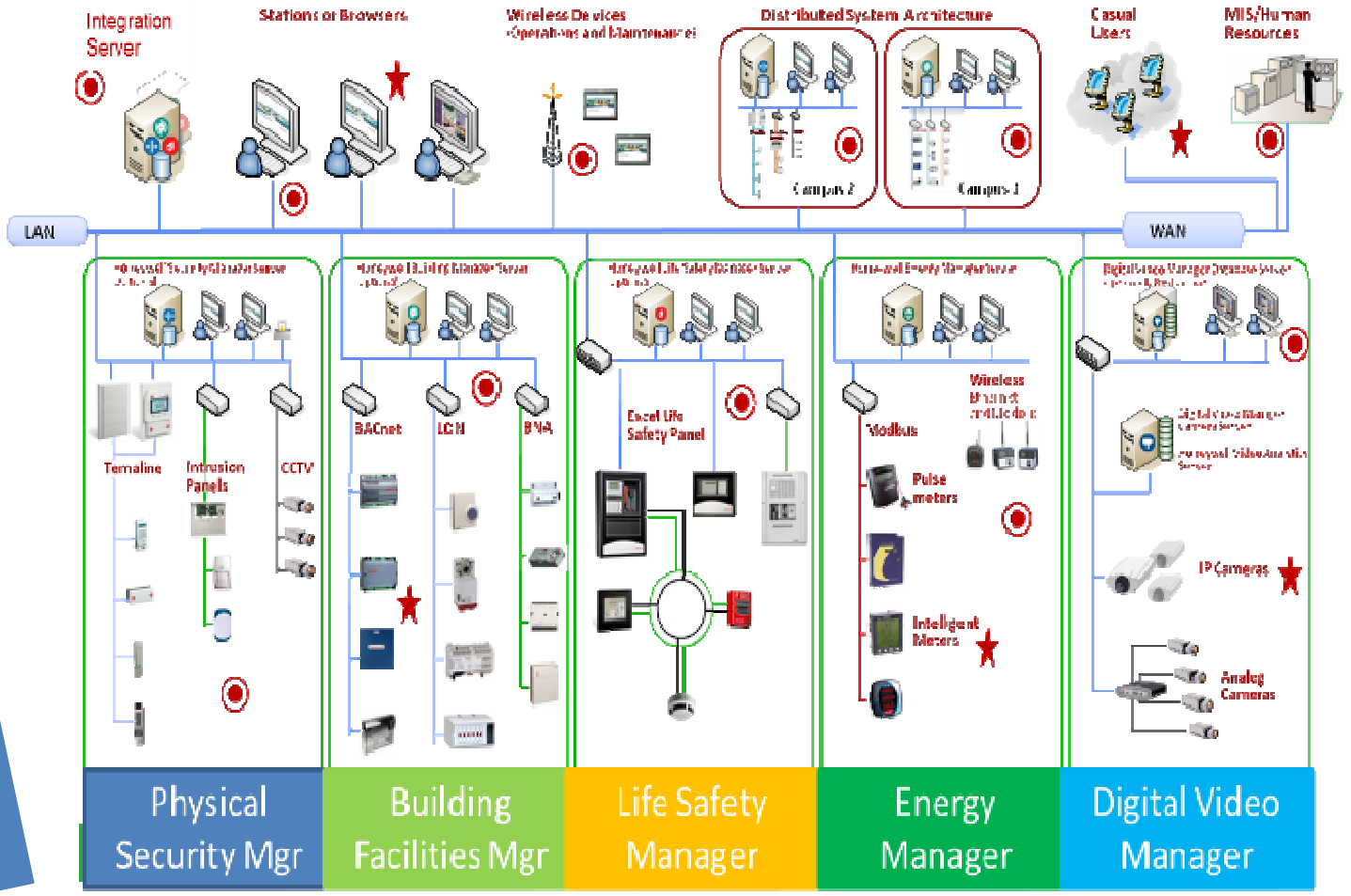
Arlington Workshops: "How To" Workshop: Develop a Contract Cybersecurity Risk Management Plan

DoD Building ICS

DoD Real Property Portfolio

- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- $847 B value

What's in Your Building?

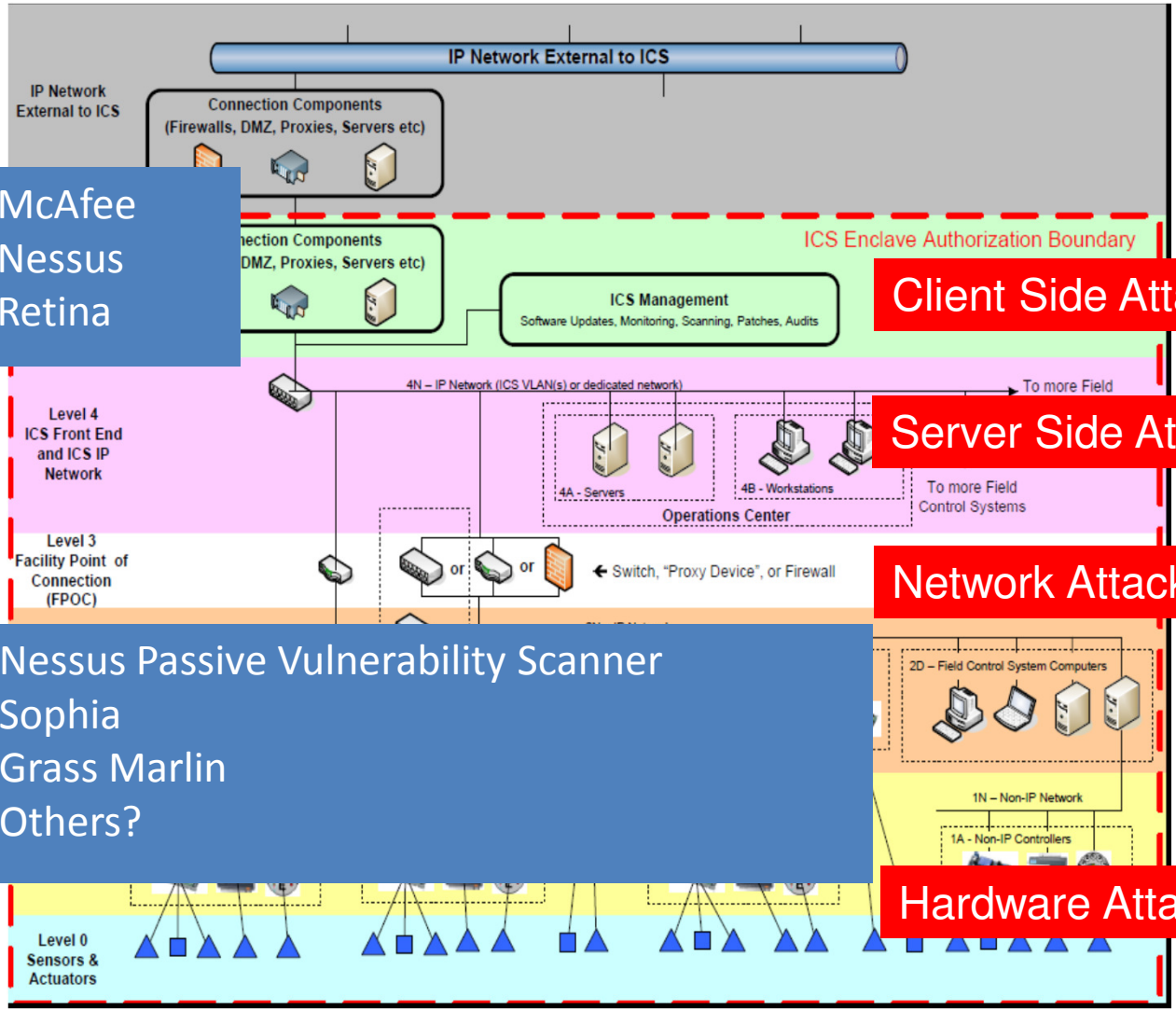


Continuous Monitoring and Attack Surfaces

Host Based
Security Systems
Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

Intrusion Detection
Systems (Passive)
PLC, RTU, Sensor
Modbus, LonTalk,
BACnet, DNP3



McAfee
Nessus
Retina

Nessus Passive Vulnerability Scanner
Sophia
Grass Marlin
Others?

Client Side Attacks

Server Side Attacks

Network Attacks

Hardware Attacks

System & Terminal Unit Controllers, Actuators

JACE

Field Server

iLon Smart Server

VAV

L-switch

BAS Remote Server

Valve Actuator

Valve Actuator

Pressure Sensor

Temperature Sensor

Analog voltage, resistance, current signal is converted to digital and then IP

ICS Protocols

Internet Protocols

- IPv4 and IPv6
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP) - Port 80
- Hypertext Transfer Protocol Secure (HTTPS) - Port 443

Open Control Systems Protocols

- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1679
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- Zigbee - Peer to Peer
- Bluetooth – Master/Slave

Proprietary Control Systems Protocols

- Tridium NiagraAX/Fox
- Johnson Metasys N2
- OSISoft Pi System
- Many others…

Building Control System Protocols

Control systems are fundamentally different than IT

- Can be based on Master and Slaves or Peer to Peer
- Slaves have Registers and Coils
- Devices use several different programming languages to perform operations
- Not originally designed for security or encryption

Master = Client : sends requests for values in the address
Slave = Server : replies with data
Registers and Coils = memory locations

Typical file extensions:

*.ACD
*.CXP
*.ESD
*.ESX
*.LDA
*.LCD
*.LDO
*.LCX
*.plcproject
*.PRJ
*.PRT
*.RSP
*.QXD
*.SCD

Tools

Information Gathering

- **Google Search and Hacking**
- Google Earth
- The Harvester
- Recon-NG
- **Shodan**
- Costar

Network Discovery and Monitoring

- Nmap
- Snort
- Kismet
- Nessus
- McAfee
- **Sophia**
- Bandolier

Attack and Defend Tools

- Kali Linux (Backtrack)
- **SamuraiSTFU**
- **Wireshark**
- Gleg
- Windows PowerShell
- Windows Management Information Console
- Windows Enhanced Mitigation Tools
- Windows Sysinternals

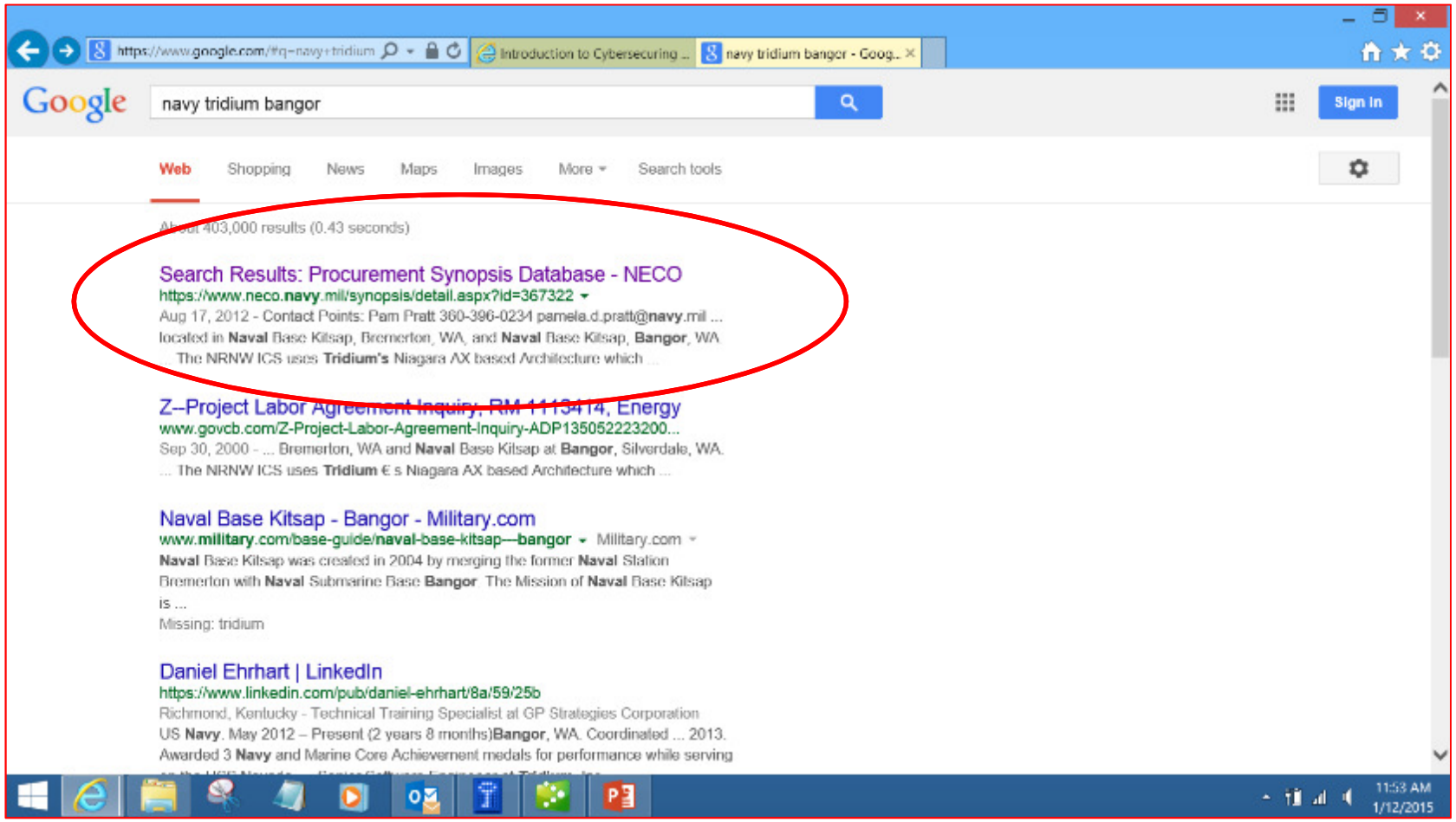
Assessment Tools

- **DHS ICS-CERT Cyber Security Evaluation Tool (CSET)**

Virtual Machines

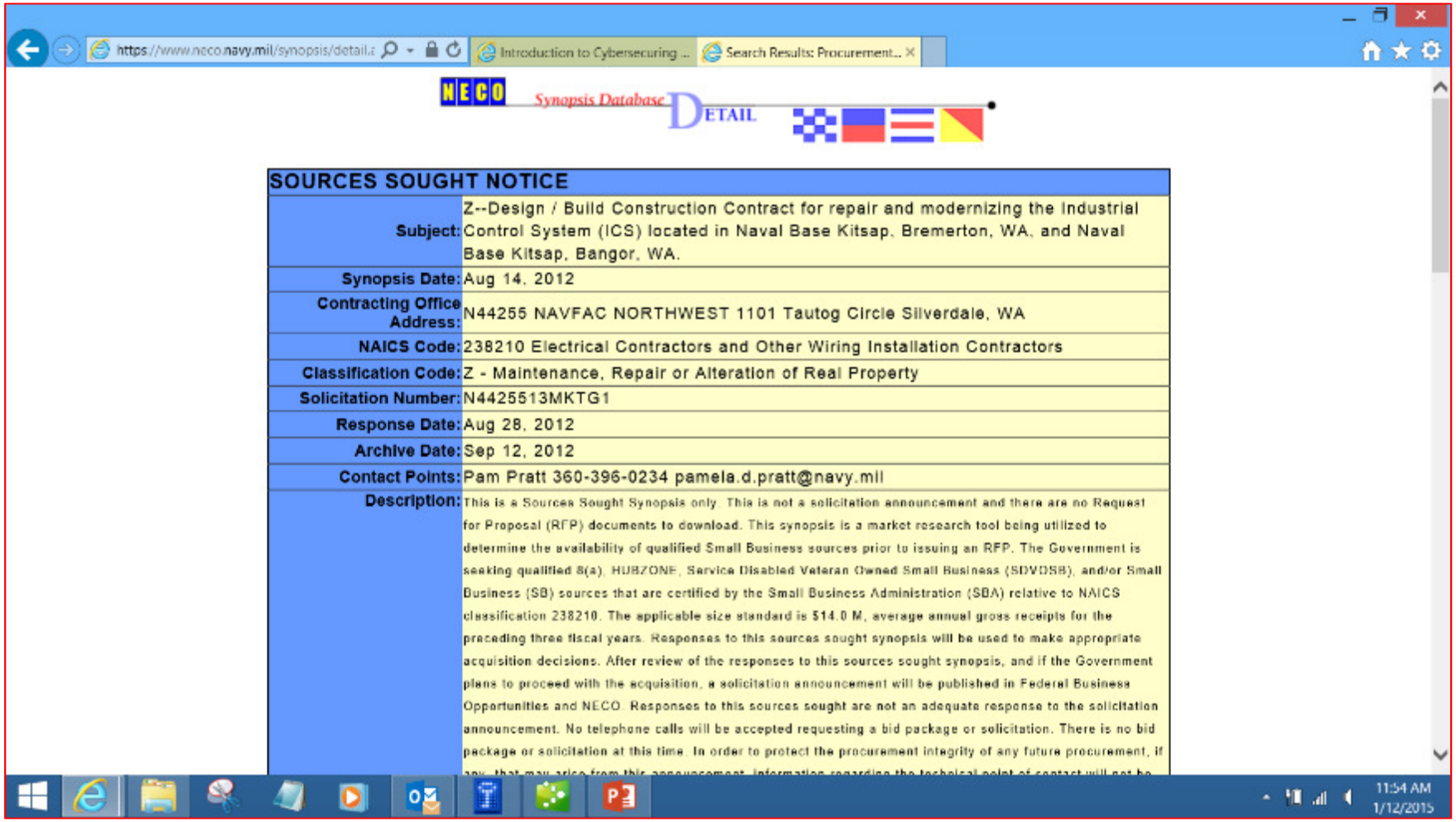
- VM Player
- Windows Hypervisor

Google Hacking



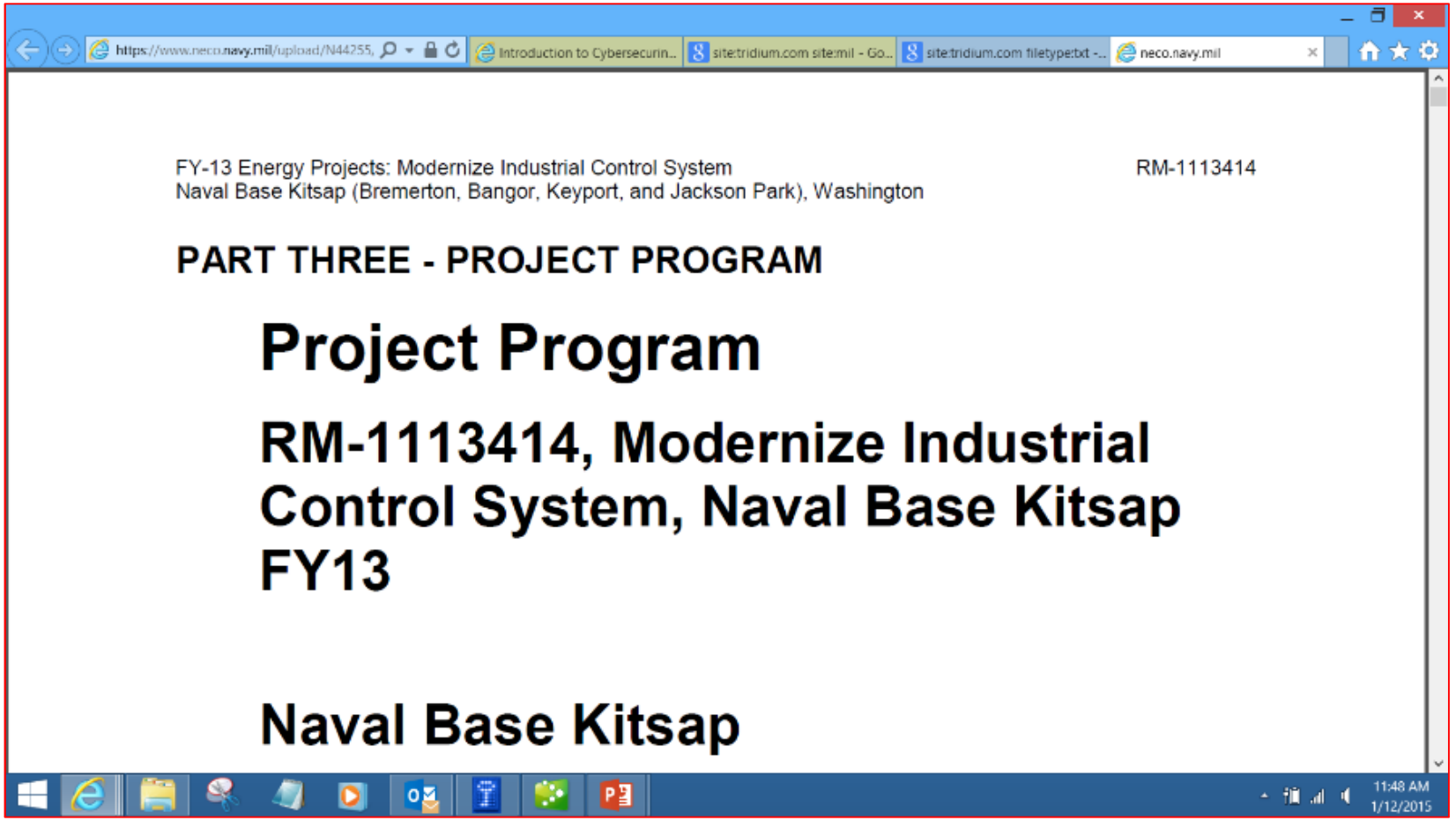
https://www.google.com/#q=navy+tridium+bangor

Google Hacking



https://www.neco.navy.mil/synopsis/detail.aspx?id=367322

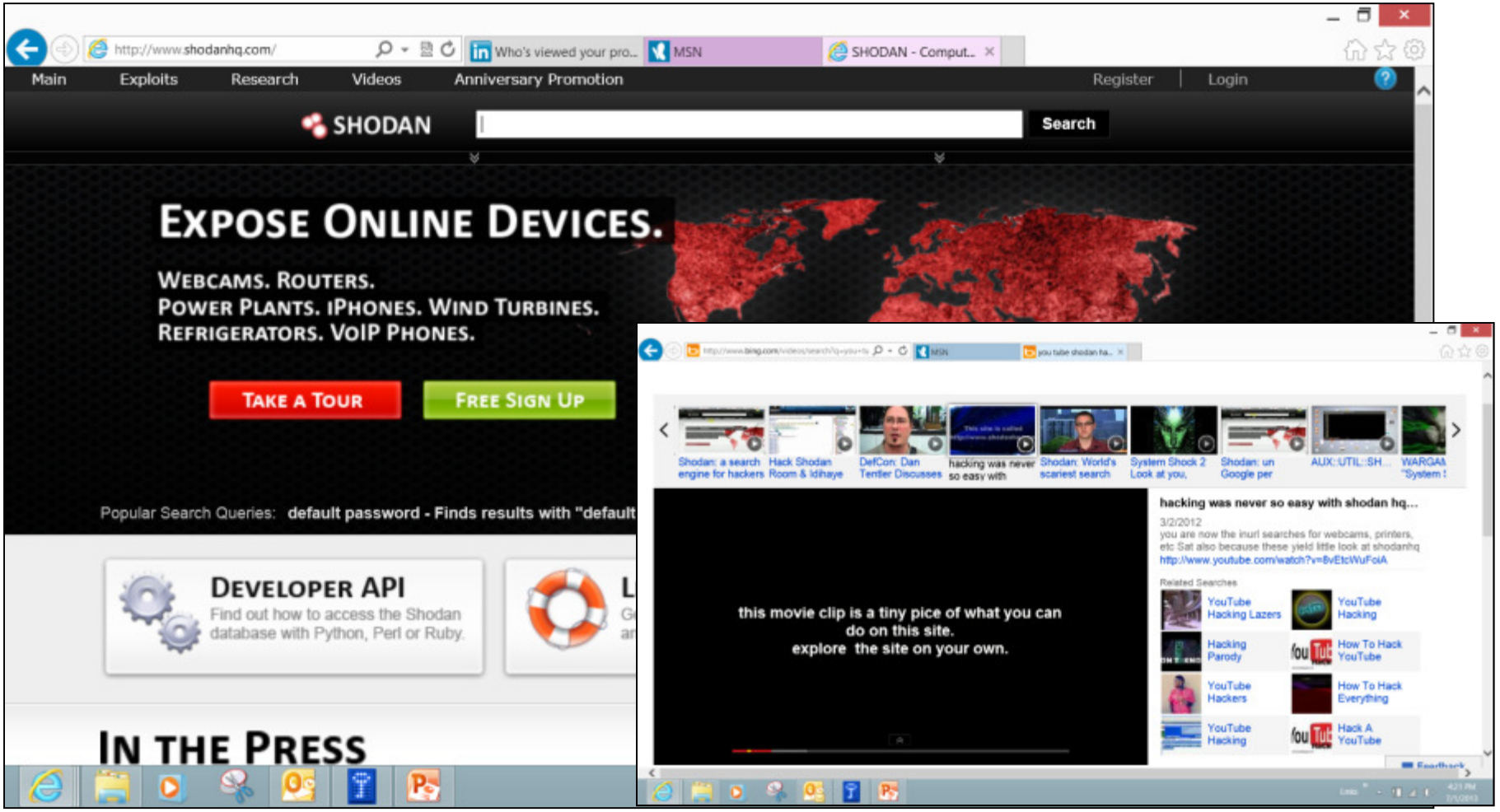
Google Hacking



filetype:pdf -site:tridium.com site:mil

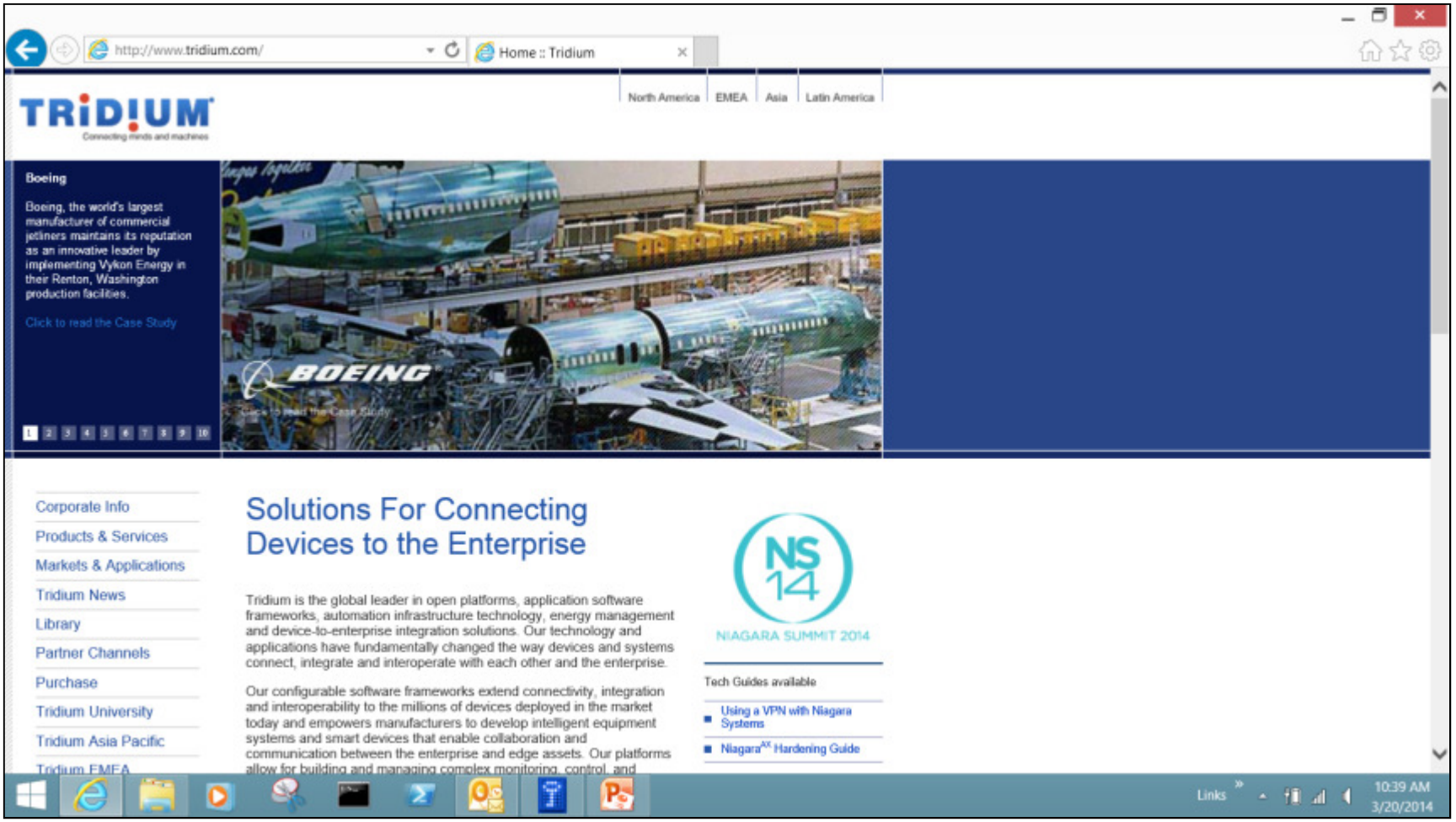
https://www.neco.navy.mil/upload/N44255/N4425513R40020005N4425513R40020005N44255-13-R-4002_Part_3_Draft.pdf

Shodan

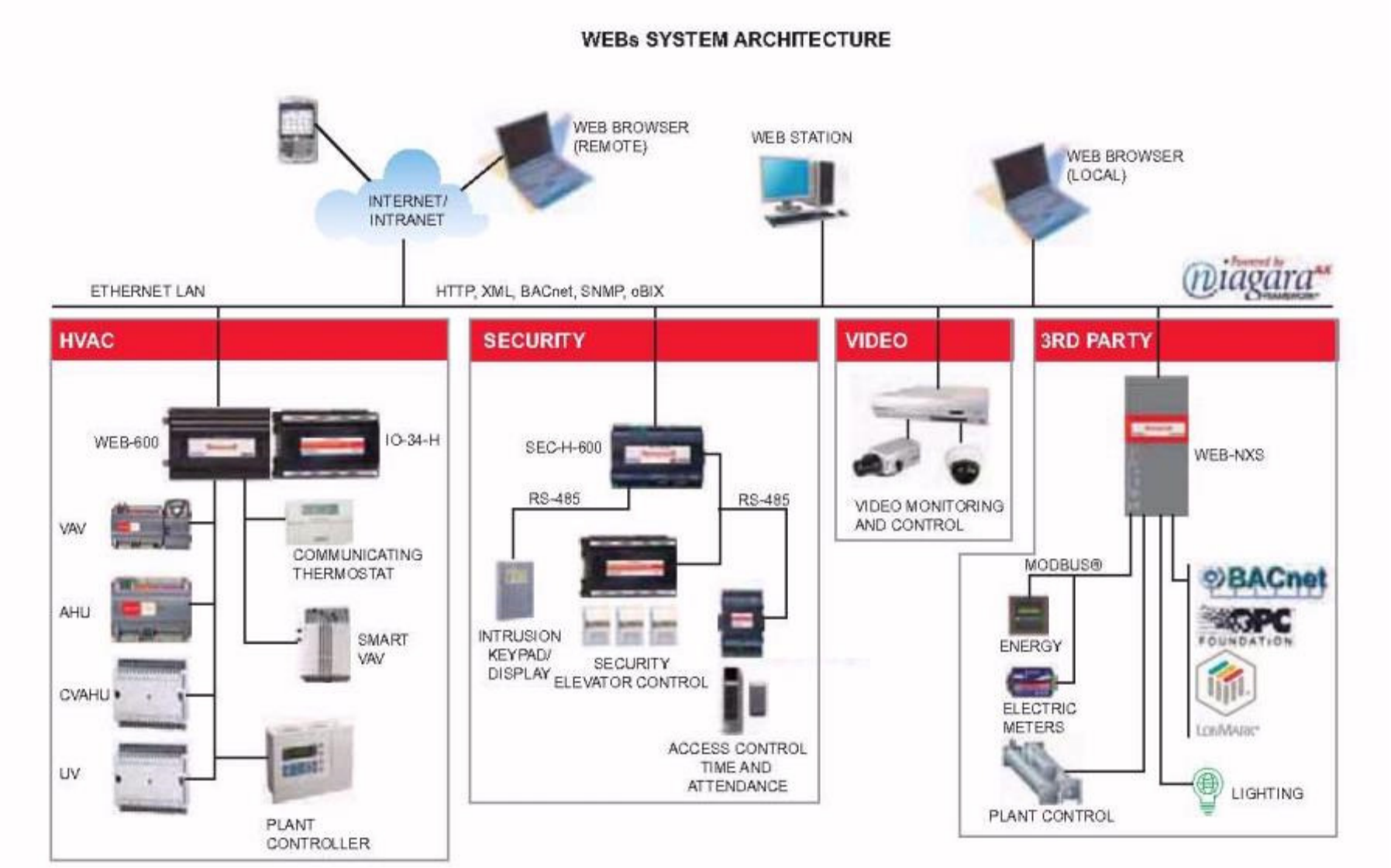


Shodan is to OT IP addresses as is Google is to text search

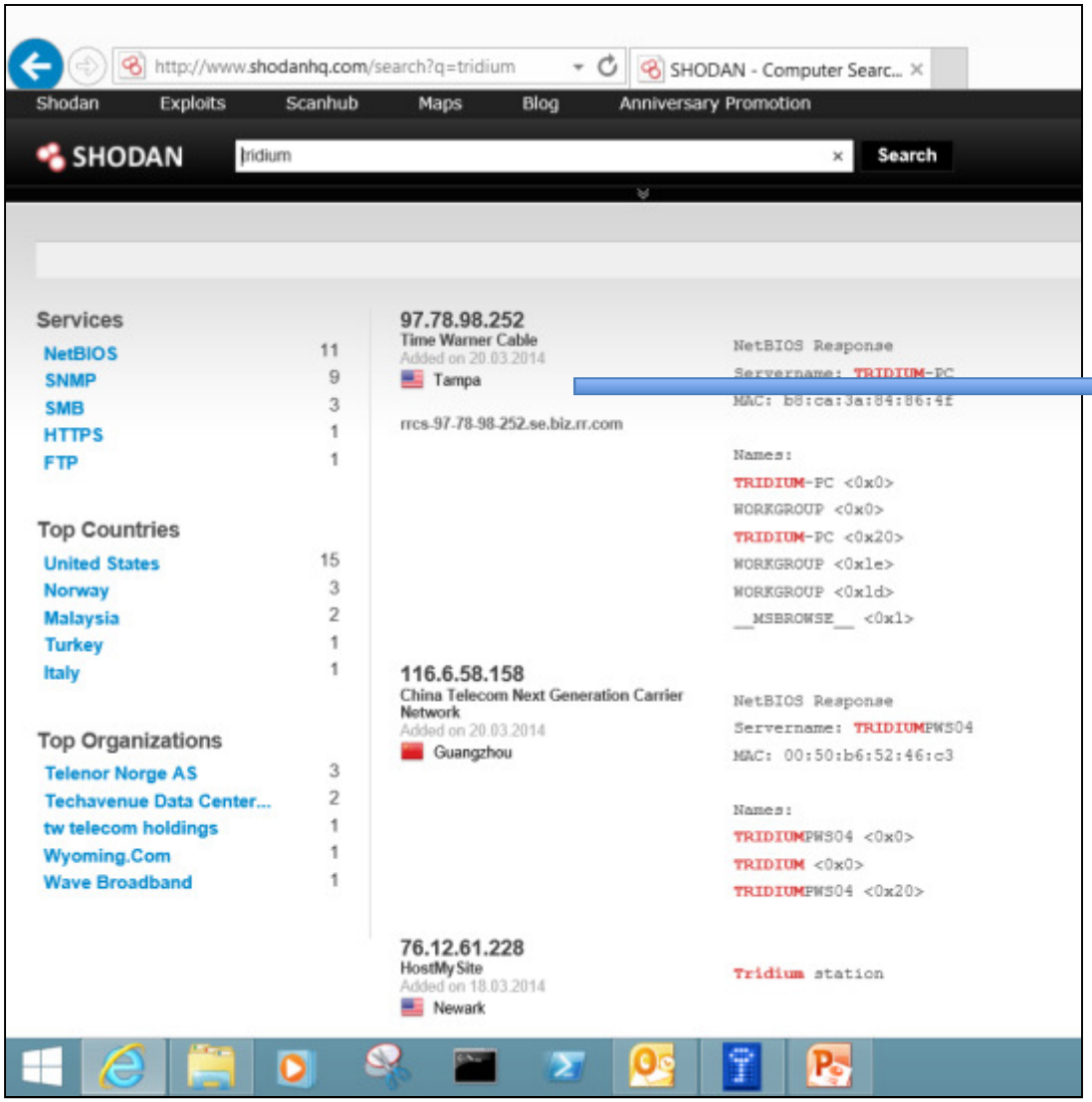
Tridium

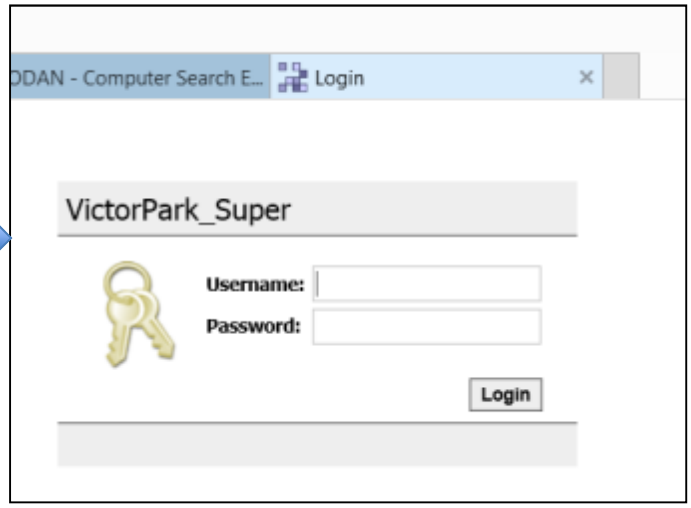

http://www.tridium.com/
Home :: Tridium
TRIDIUM
Connecting minds and machines
North America
EMEA
Asia
Latin America
Boeing
Boeing, the world's largest manufacturer of commercial jetliners maintains its reputation as an innovative leader by implementing Vykon Energy in their Renton, Washington production facilities.
Click to read the Case Study
BOEING
Corporate Info
Products & Services
Markets & Applications
Tridium News
Library
Partner Channels
Purchase
Tridium University
Tridium Asia Pacific
Tridium EMEA
Solutions For Connecting Devices to the Enterprise
Tridium is the global leader in open platforms, application software frameworks, automation infrastructure technology, energy management and device-to-enterprise integration solutions. Our technology and applications have fundamentally changed the way devices and systems connect, integrate and interoperate with each other and the enterprise.
Our configurable software frameworks extend connectivity, integration and interoperability to the millions of devices deployed in the market today and empowers manufacturers to develop intelligent equipment systems and smart devices that enable collaboration and communication between the enterprise and edge assets. Our platforms allow for building and managing complex monitoring, control, and
NS 14
NIAGARA SUMMIT 2014
Tech Guides available
Using a VPN with Niagara Systems
Niagara^AX Hardening Guide
Links
10:39 AM
3/20/2014

Tridium Architecture



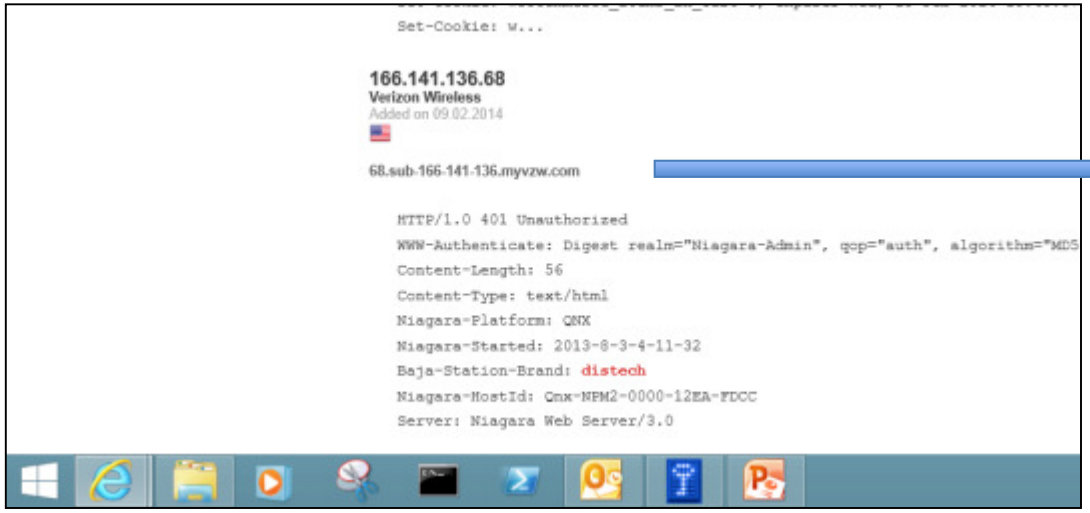
Shodan – Tridium Search





Distech Controls

Shodan – Distech Search

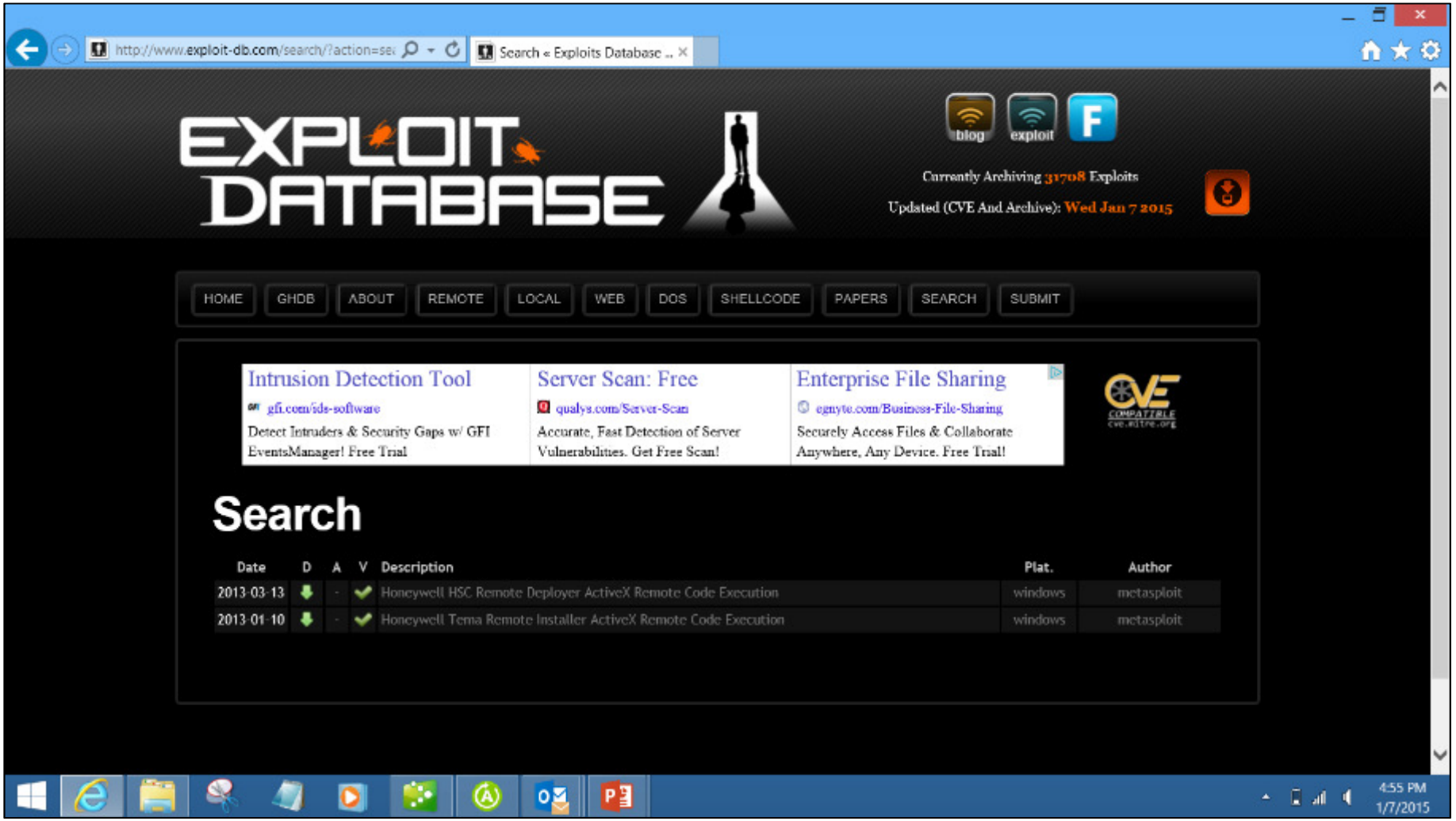


HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="**Niagara-Admin**", qop="auth", algorithm="**MD5**", nonce="UvdraWNmNDAwNjE1ODc4NzBhYTc5NjMyYzlkYTk3NTg1ZDQy"
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32
Baja-Station-Brand: **distech**
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC
Server: **Niagara Web Server/3.0**

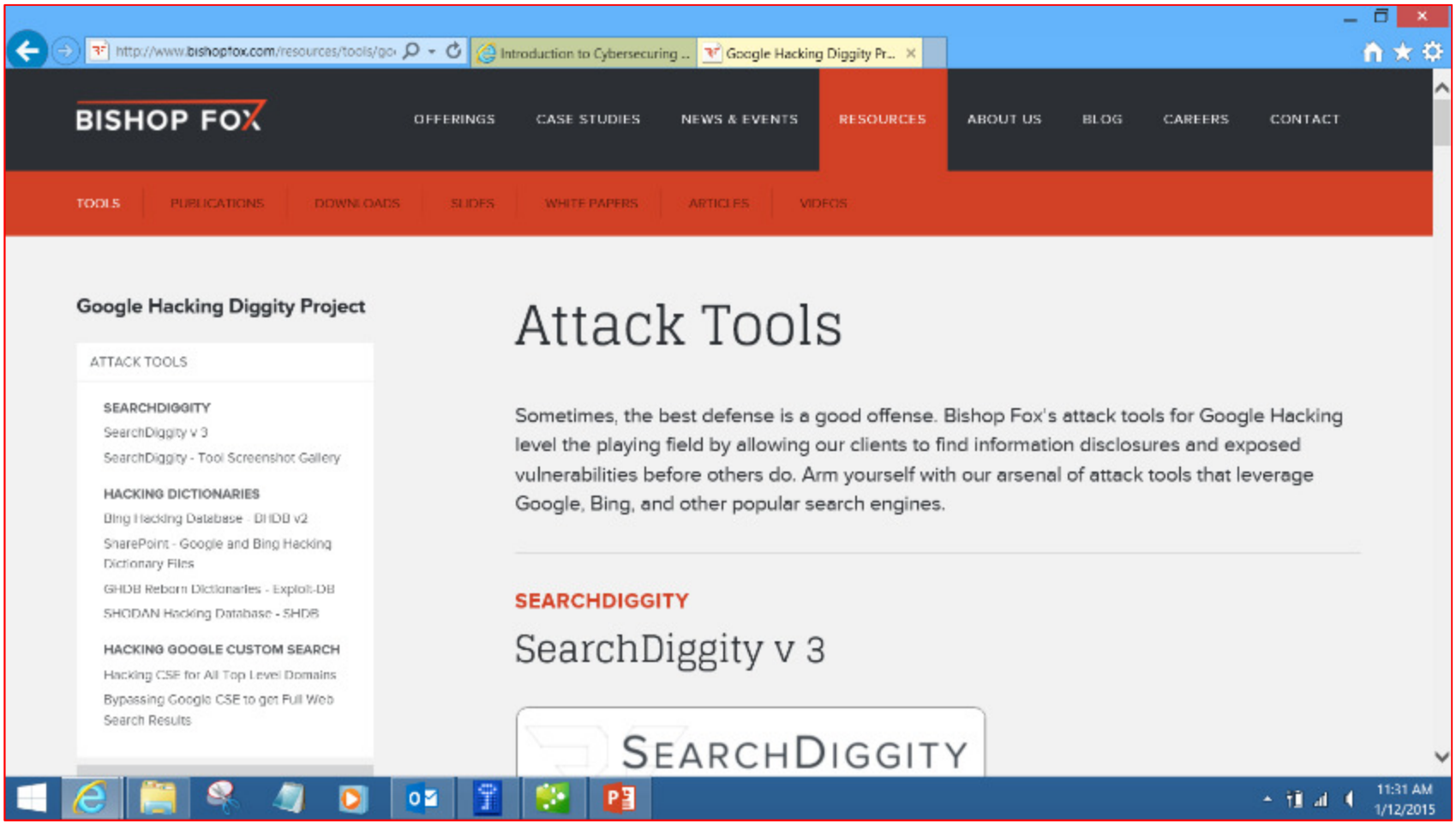
Google Hacking-Database

http://www.exploit-db.com/google-dorks/

Google Hacking DB Search

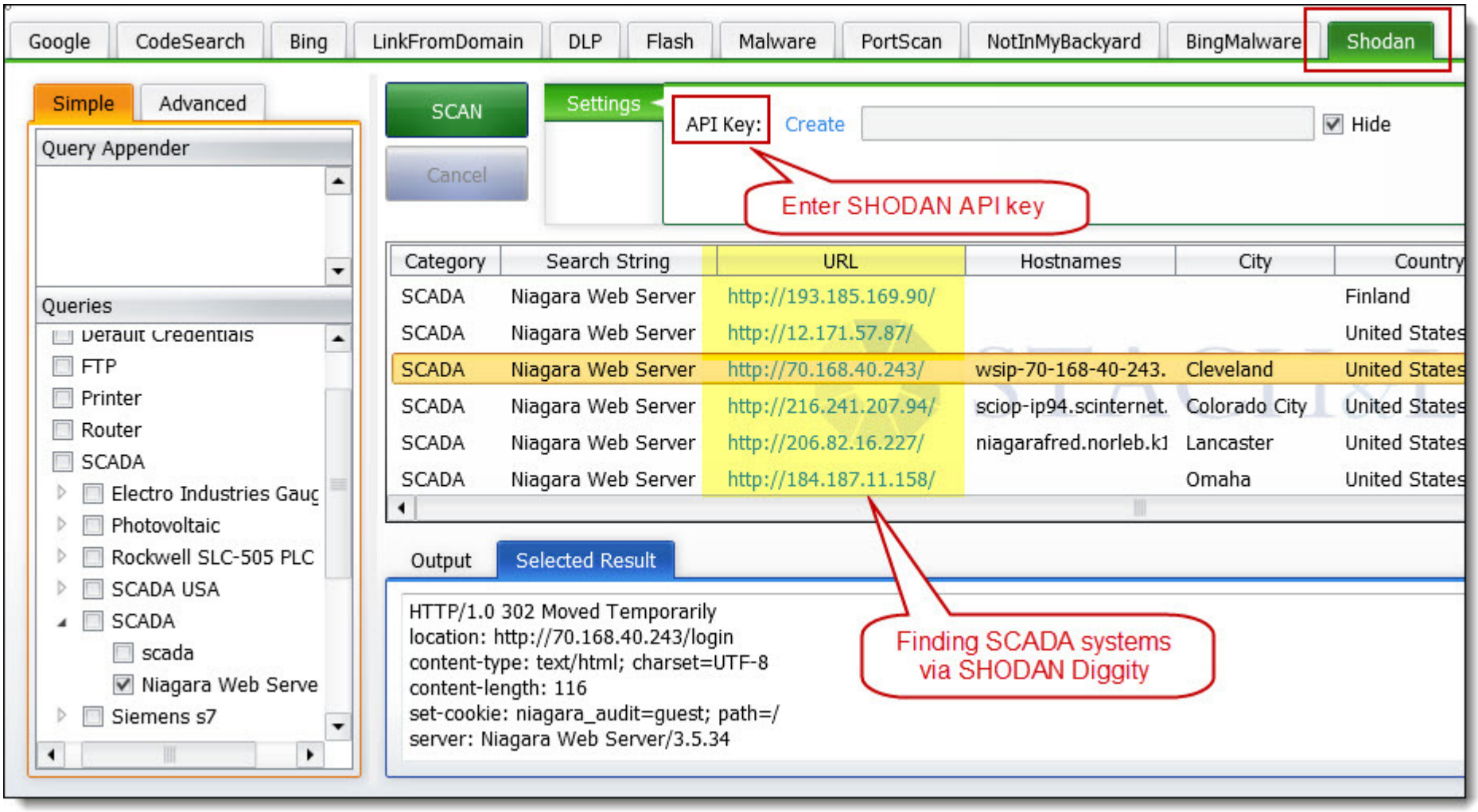


Google Hacking Diggity Project



http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/#searchdiggity

Google Hacking Diggity Project

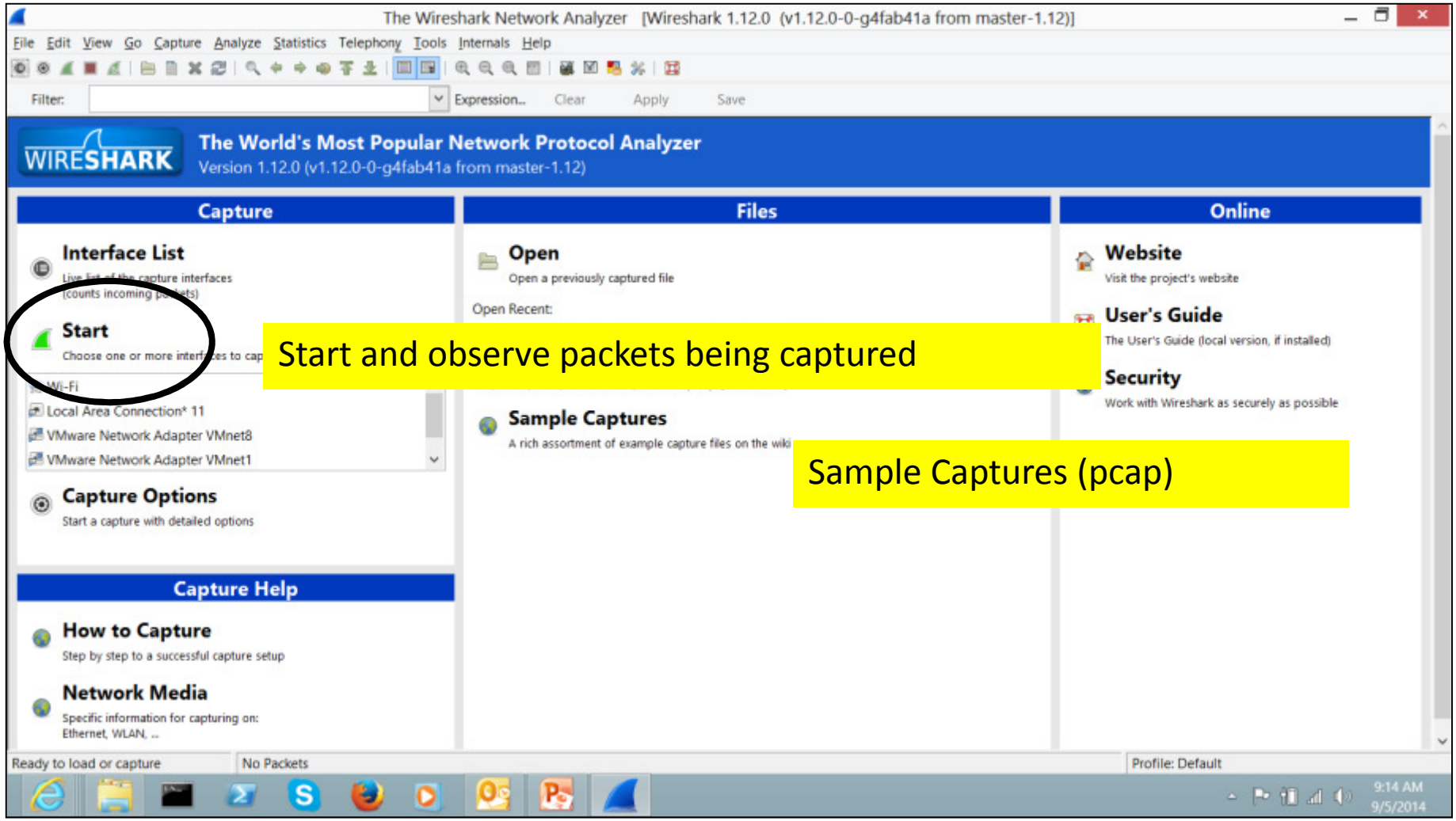


Kali Linux

http://www.kali.org/

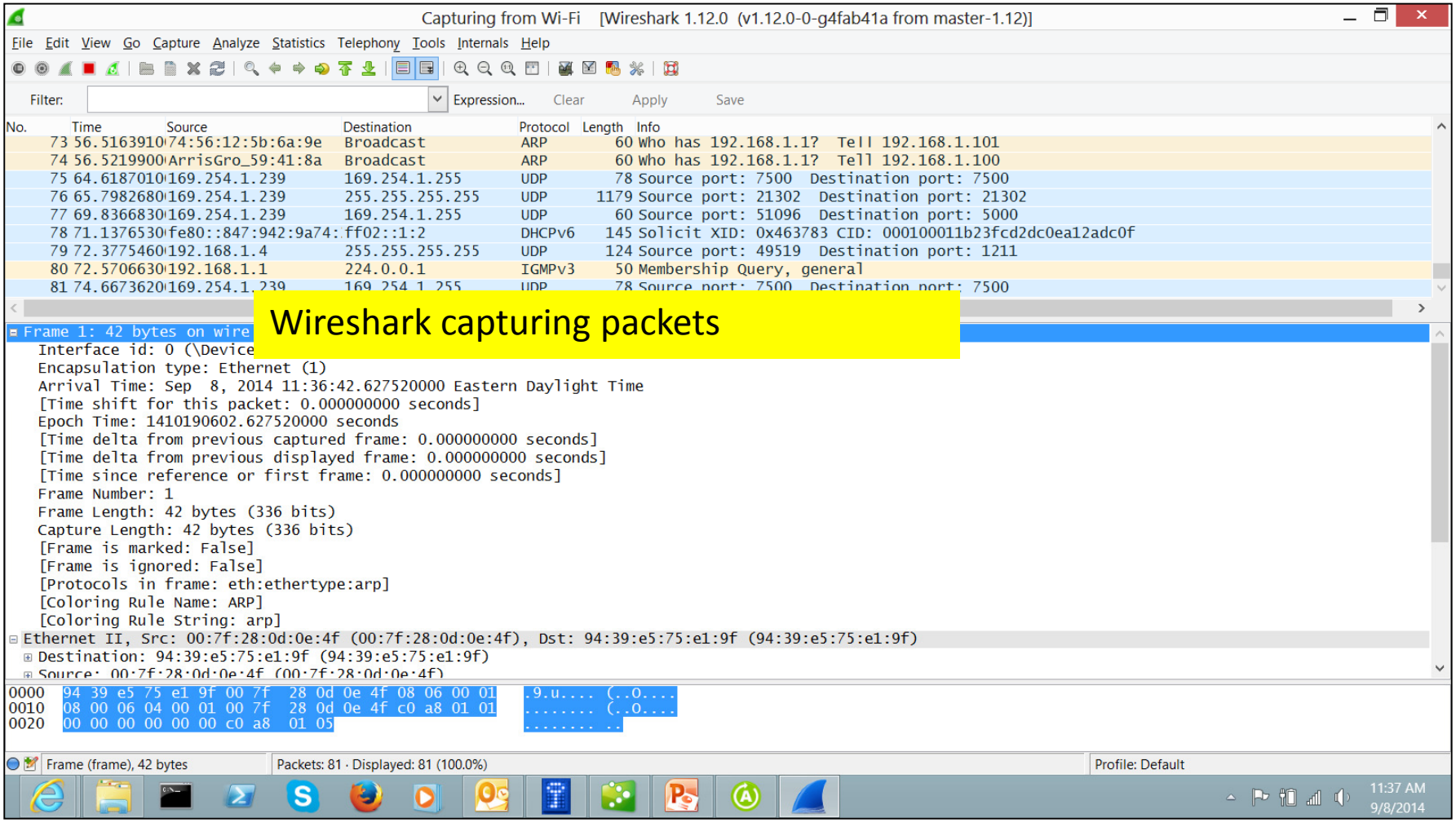
SamuraiSTFU Applications

Wireshark Home

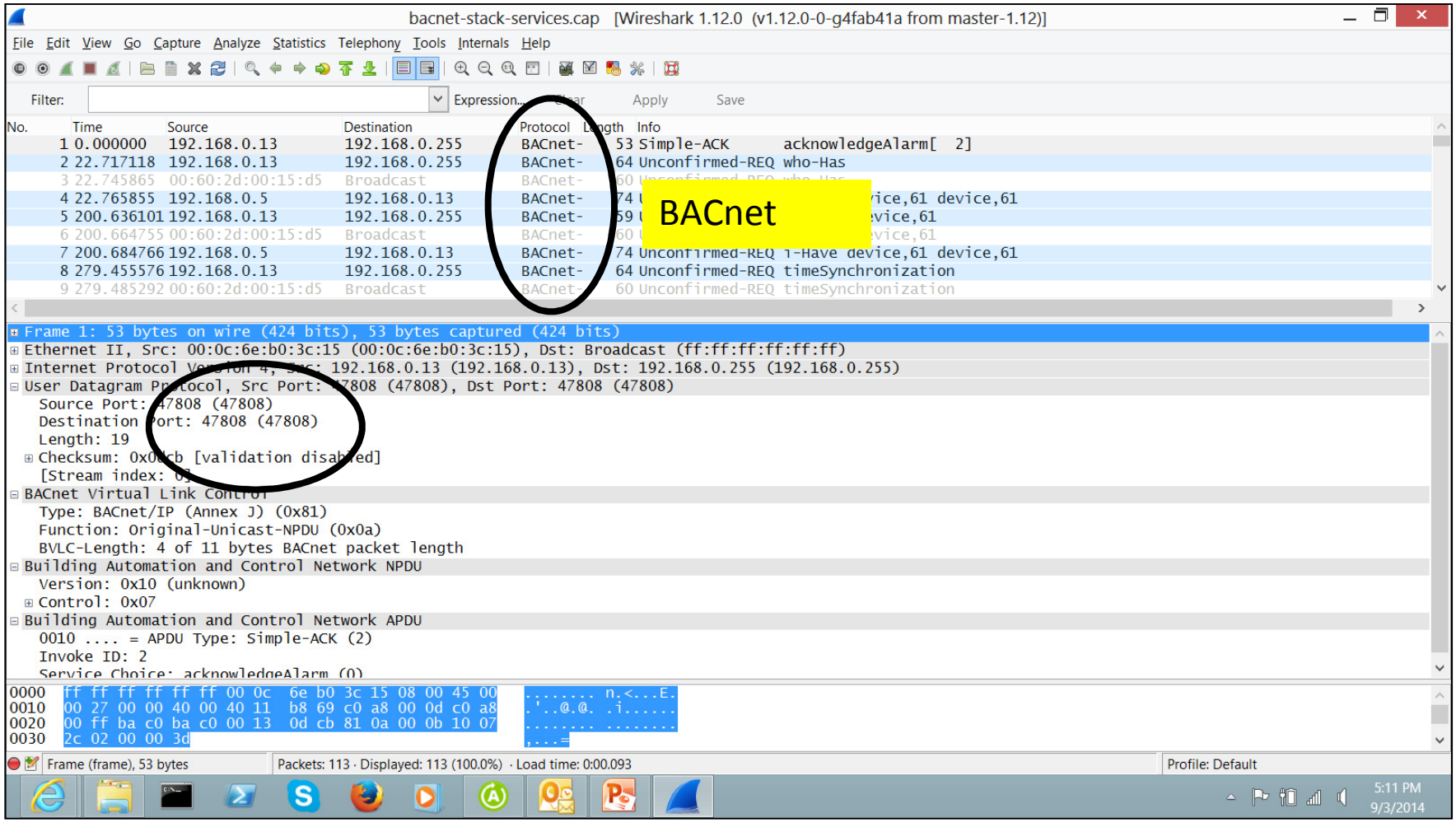


https://www.wireshark.org/about.html

Wireshark Active Packet Capture



Wireshark BACnet pcap



NIST SP 800-82 R2

Section 2.5 added per DoD request to address 'other-than-industrial' control systems

Standards – NIST SP 800-82 R2

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

- **800-82 Rev 1 was released May 2013 - has 800-53 Rev 3 Appendix I and 600+ controls**
- 800-82 Rev 2 is scheduled for Final release spring 2015 – has 800-53 Rev 4 800+ controls, **Appendix G ICS Overlay**

NIST SP 800-82 R2 Key Security Controls

Inventory
- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

Central Monitoring
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

Critical Infrastructure
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection, Outbound Detection

DHS CSET

- Stand-alone Software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:

www.ics-cert.us-cert.gov/Downloading-and-Installing-CSET

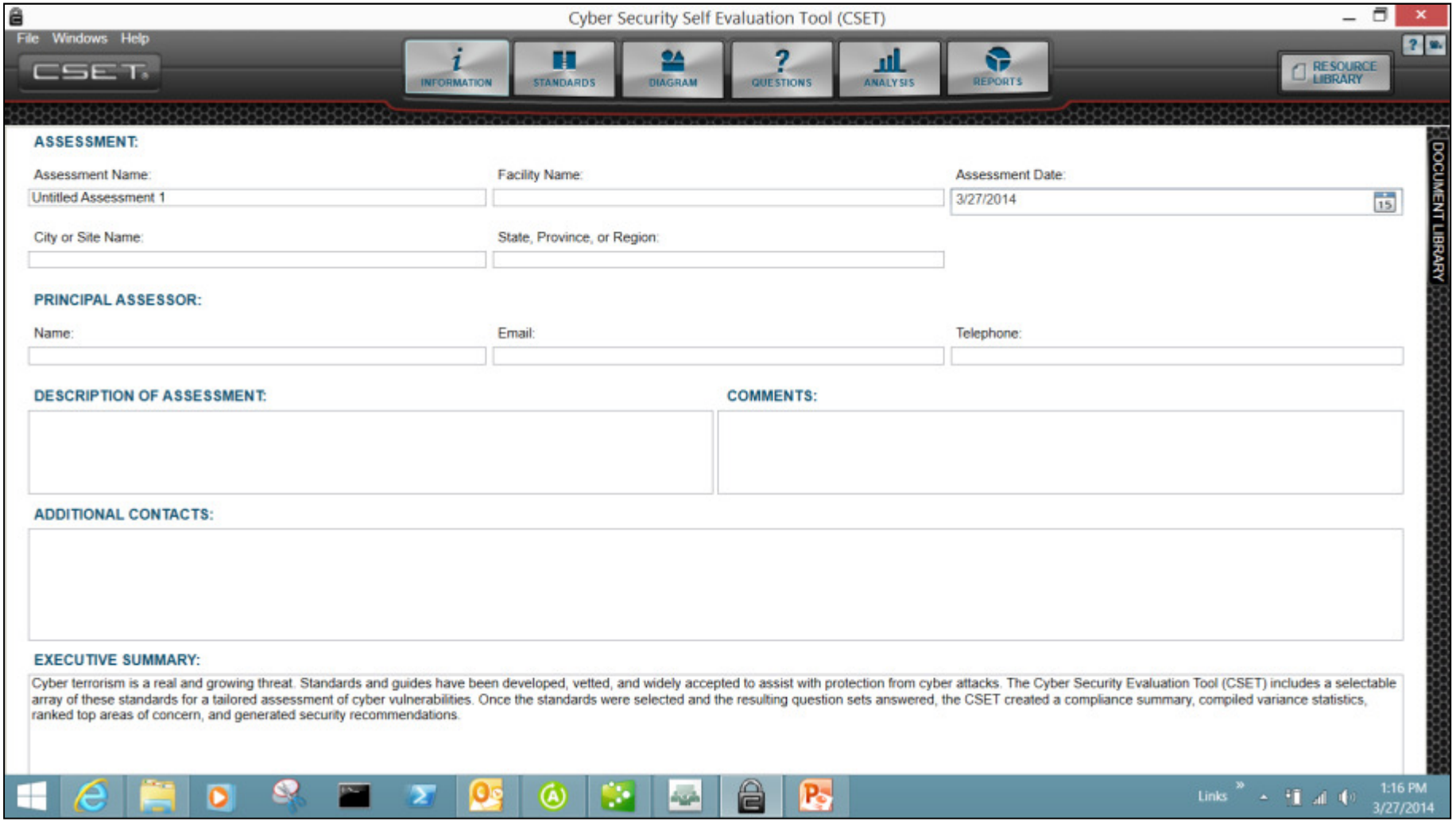
DHS NCCIC and ICS-CERT CSET

National Cybersecurity and Communications Integration Center
http://www.us-cert.gov/nccic/

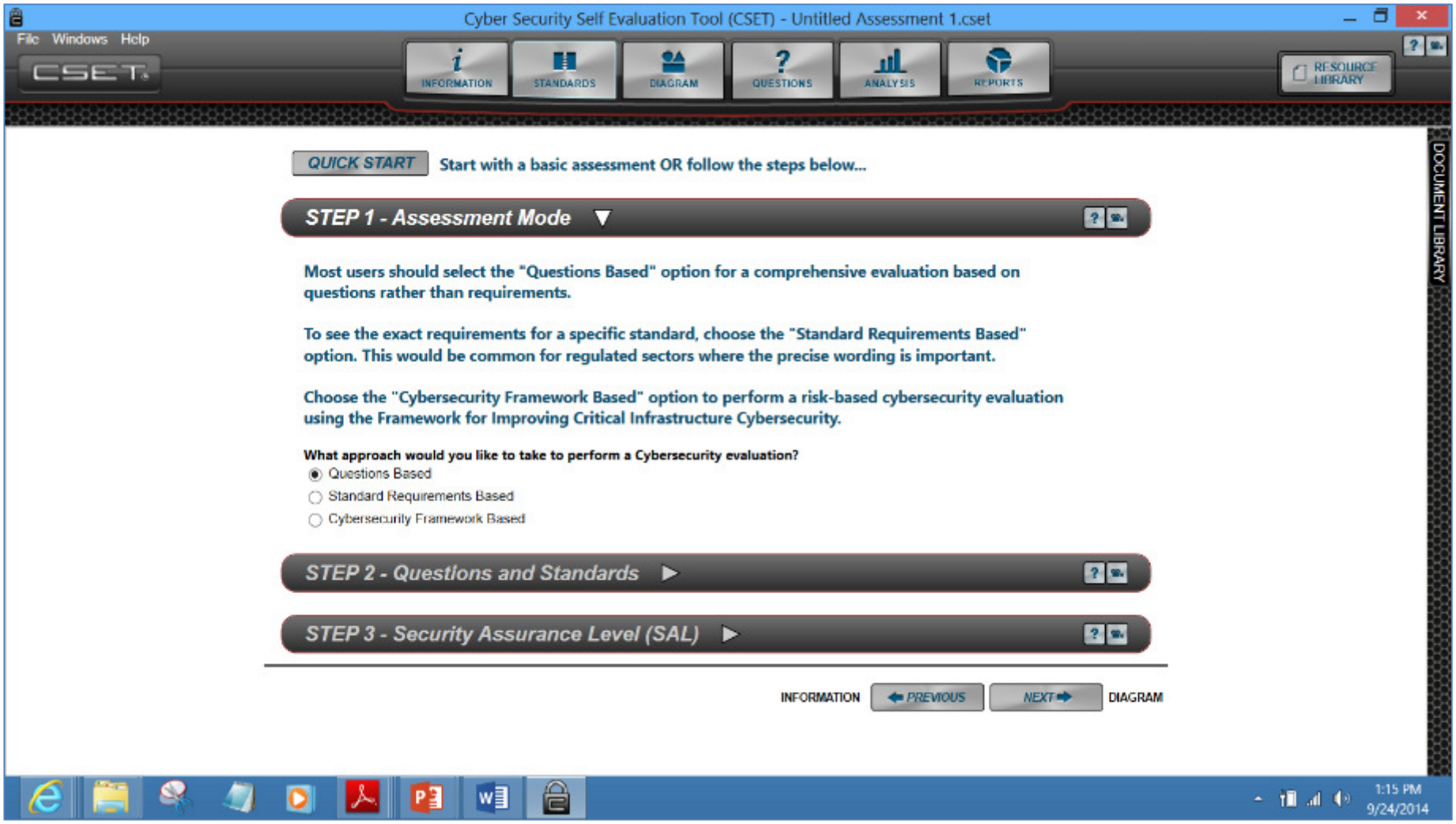
DHS CSET 6.2 Tool

- NIST Cybersecurity Framework
- NIST 800-30
- NIST 800-53 Rev 3
- NIST 800-53 Rev 4
- NIST 800-82 Rev 1
- NIST 800-82 Rev 2
- NIST 1108
- NISTR 7628
- NERC CIP

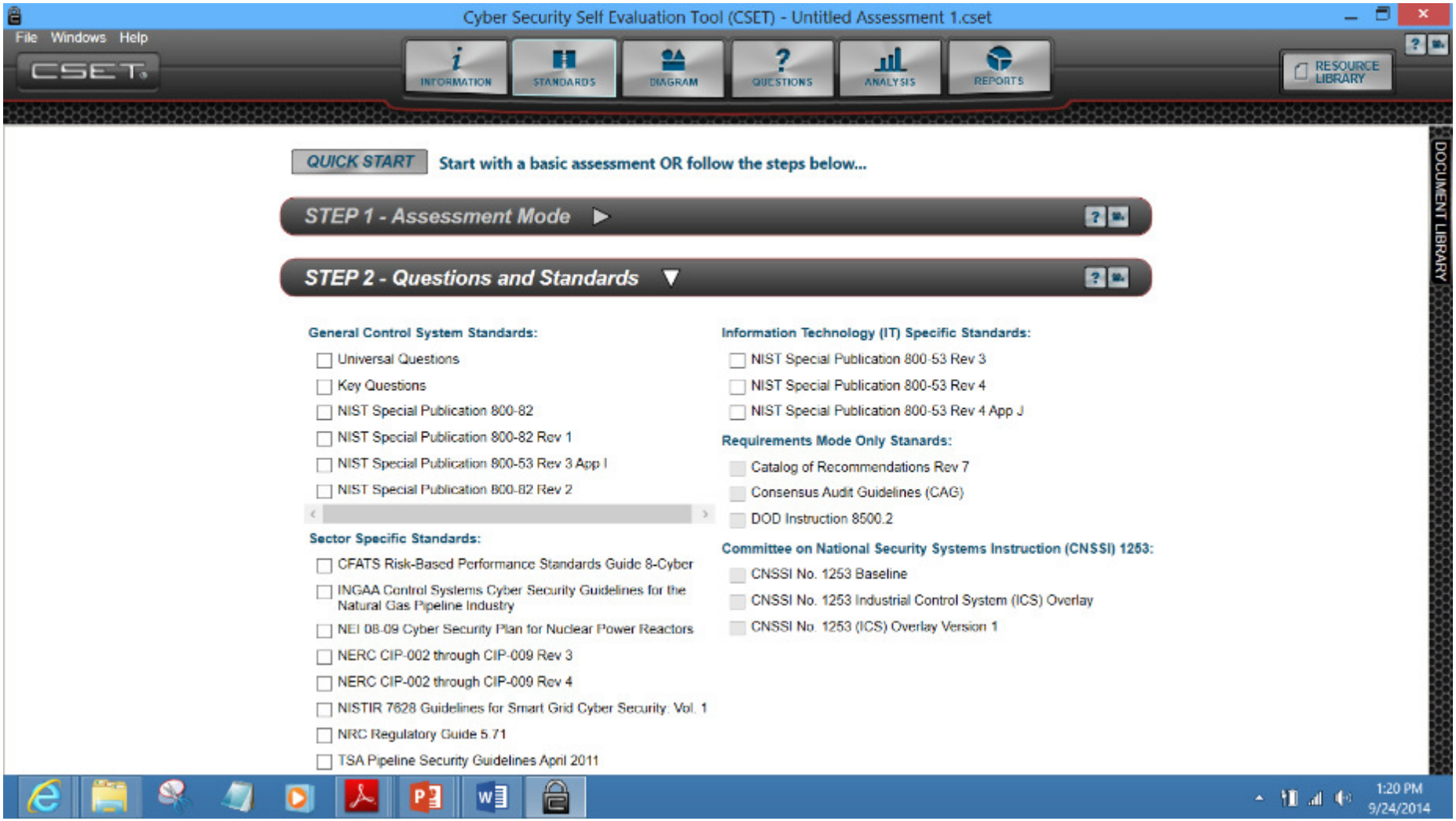
New Assessment Form



Standards Home - Step 1 Assessment Mode

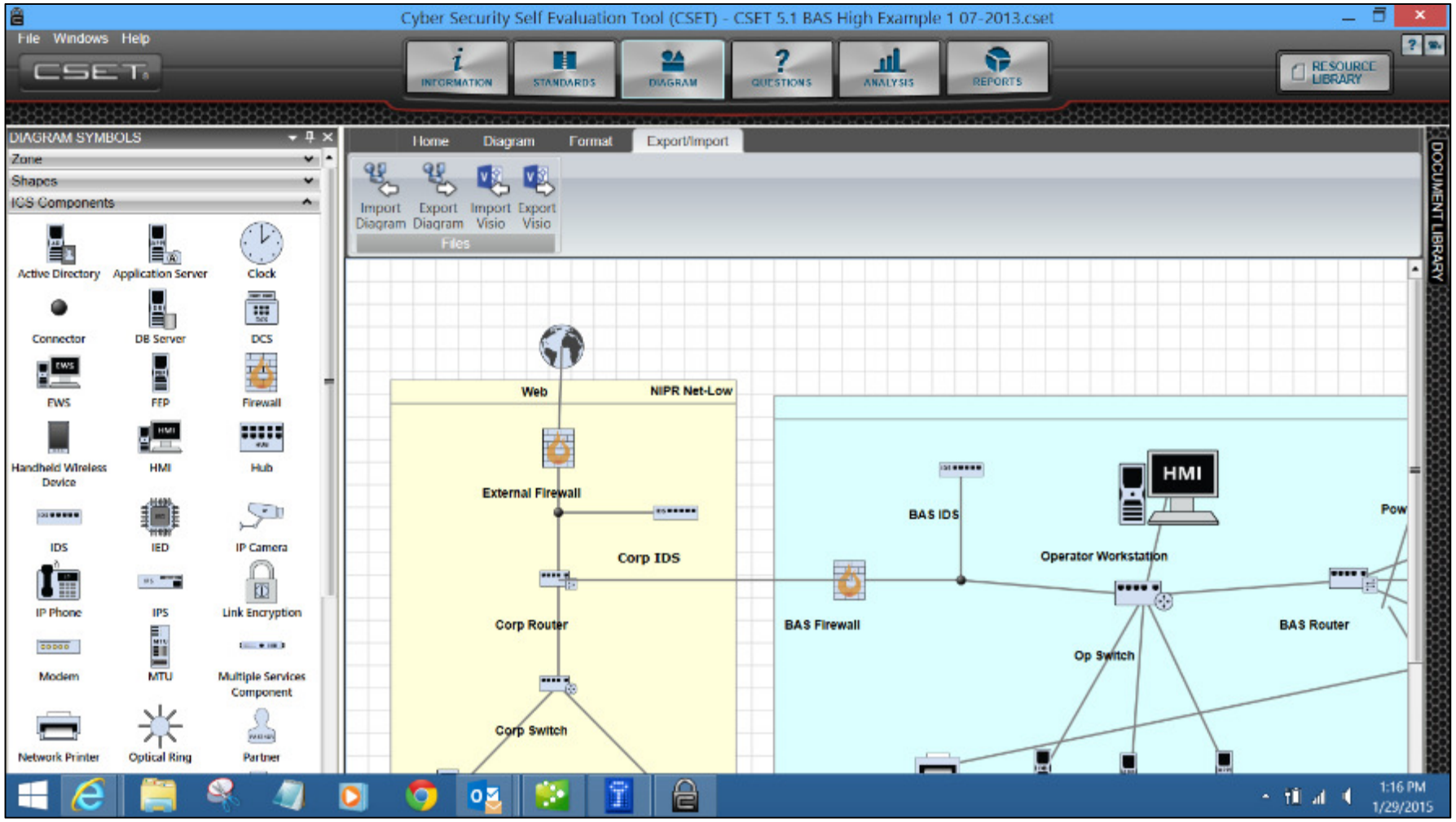


Step 2 - Questions and Standards

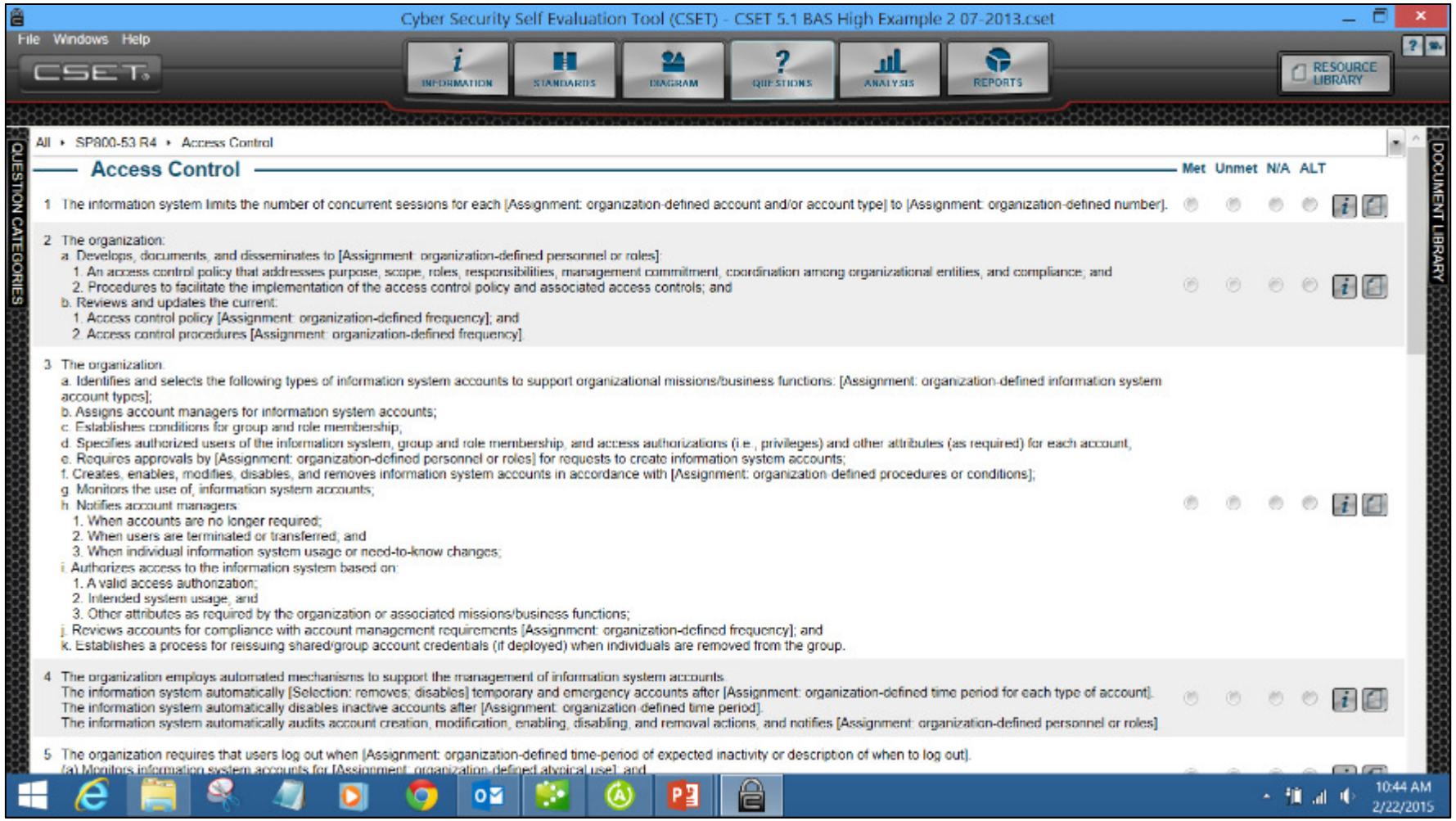


Step 3 Questions

Diagram – Tools, Templates, Inventory



Questions – Family, Detail, Info



Analysis - Dashboard

Reports


Cyber Security Self Evaluation Tool (CSET)
File Windows Help
CSET
INFORMATION
STANDARDS
DIAGRAM
QUESTIONS
ANALYSIS
REPORTS
RESOURCE LIBRARY
Report Builder
Select the report(s) you want to create and the file type then click the 'Create' button to create reports for your assessment.
The 'Detail Options' button will allow you to determine what sections to include in the Detail Report before you create it.
EXECUTIVE SUMMARY
SITE SUMMARY
DETAIL OPTIONS
SECURITY PLAN
PDF
DOC
DOCX
CREATE
Select All
Detail Report Options
Assessment Information
Executive Summary
Document Library
Evaluation Of Selected Standards
Standards Compliance
Component Diagram
Network Component Analysis
Component Compliance
Findings & Recommendations
Security Assurance Level
Ranked Subject Areas
Summary of Ranked Questions
Questions Marked For Review
Questions with Alternate Justification
Select All
Detail Report Standards Options
Network Components
DOCUMENT LIBRARY
Links
2:03 PM
3/27/2014

System Security Plan

SITE CYBER SECURITY PLAN

CONTROL SYSTEMS CYBER SECURITY EVALUATION

Homeland Security

Untitled Assessment 1

3/27/2014

Assessor:

3. Risk Analysis

A good security plan will require that a risk evaluation is performed to determine the level of necessary rigor and cost benefit analysis for the level of controls selected. If not yet performed yet it is recommended that the general risk analysis be performed. A good risk assessment should include an evaluation of the value of the protected assets and information, an examination of the consequences to the organization in the event of a successful attack, an examination of the threat if possible, and the cost of implementing mitigating controls.

threats × vulnerability × asset value = total risk

total risk – countermeasures = residual risk

Consequence

The examination of the consequences of an attack should include

if control systems were maliciously accessed and manipulated to cause harm in a worst case scenario

- *How many people could sustain injuries requiring a hospital stay?*
- *How many people could be killed?*
- *Estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)*
- *Estimate the potential cost in terms of economic impact to both the site and surrounding communities. (Consider any losses to community structures and use and any costs associated with displacement.)*
- *Estimate the potential cost of environmental cleanup to the site and surrounding communities. (Consider the cost for cleanup, fines, litigation, long term monitoring, etc.)*

Threat

The threat portion of the equation can be deduced from the recommended implementation priorities list. The priorities are set based on incident data collected at the ICS-CERT watch floor and subject matter experts as of the time of publication of CSET. Top priorities are controls that mitigate the most actively exploited vulnerabilities with the most significant consequences.

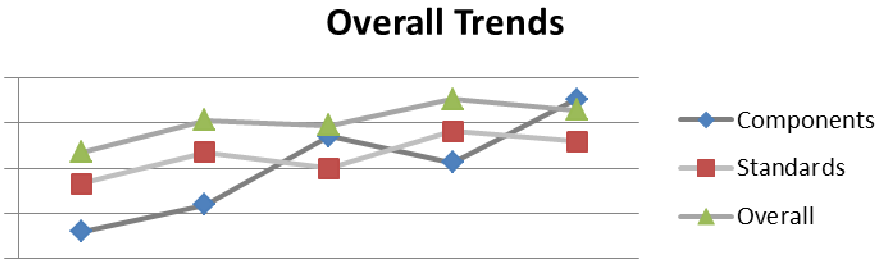
Cost Benefit Analysis

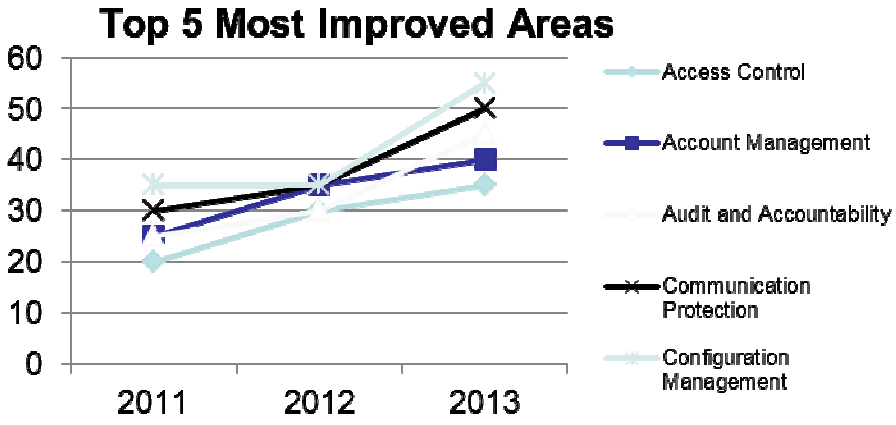
The cost of implementing controls with respect to the additional security provided is the final step in selecting the controls to implement.

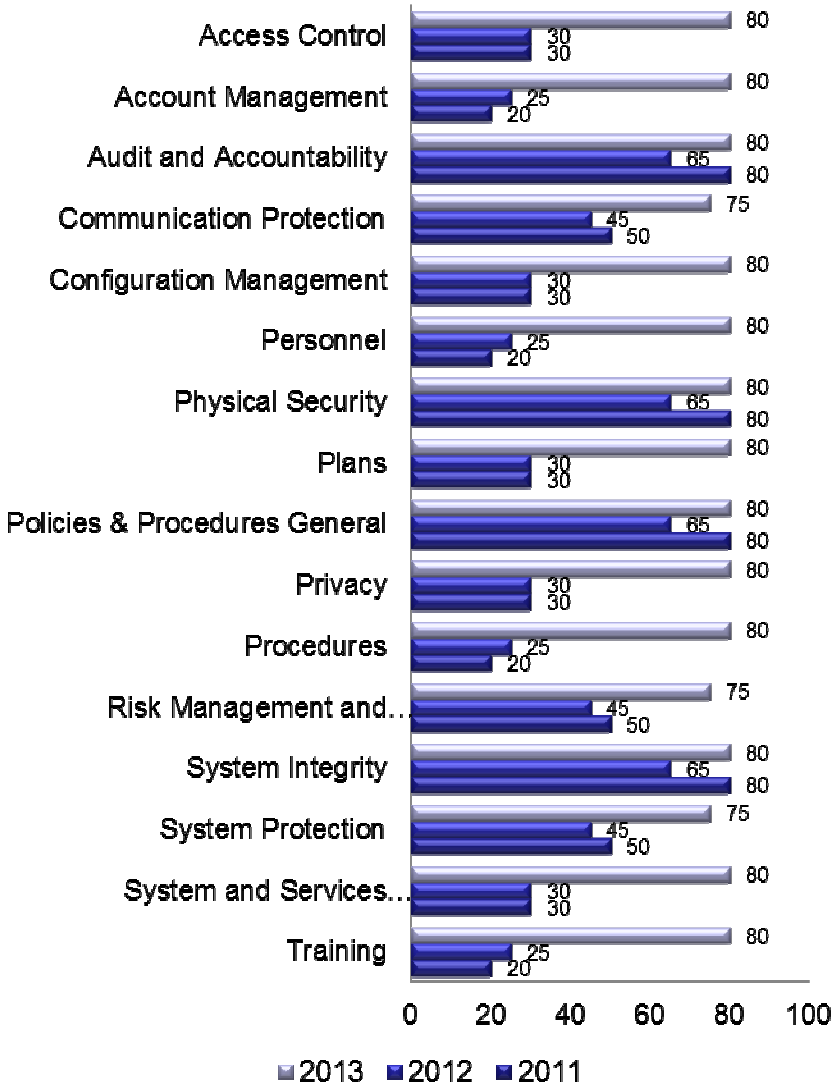
3.1. Basic Model

Traditional security models define three areas of consideration Confidentiality, Integrity, and Availability. The security plan should address the each of these areas with respect to data and systems.

Trending

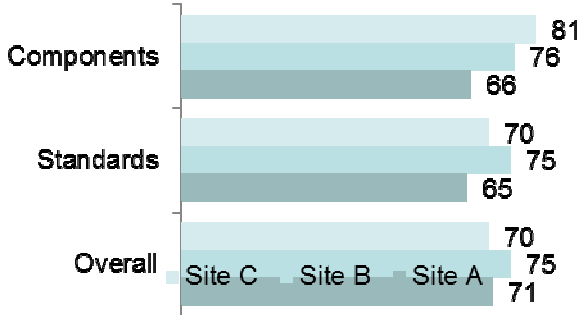

Overall Trends
Components
Standards
Overall

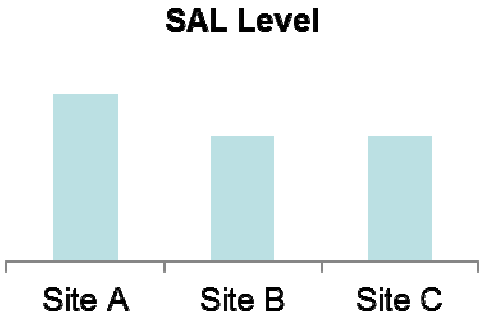

Top 5 Most Improved Areas
60
50
40
30
20
10
0
2011
2012
2013
Access Control
Account Management
Audit and Accountability
Communication Protection
Configuration Management

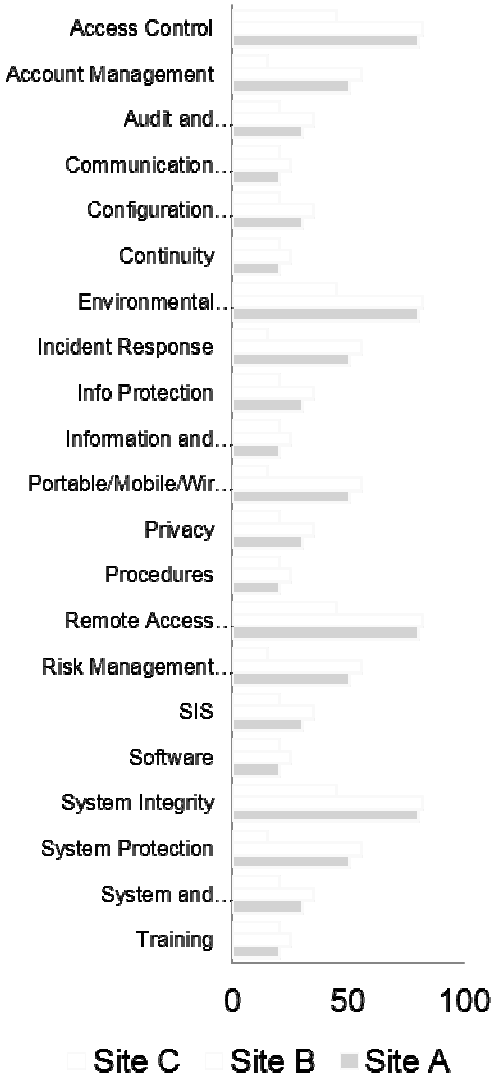

Access Control
Account Management
Audit and Accountability
Communication Protection
Configuration Management
Personnel
Physical Security
Plans
Policies & Procedures General
Privacy
Procedures
Risk Management and...
System Integrity
System Protection
System and Services...
Training
0
20
40
60
80
100
2013
2012
2011

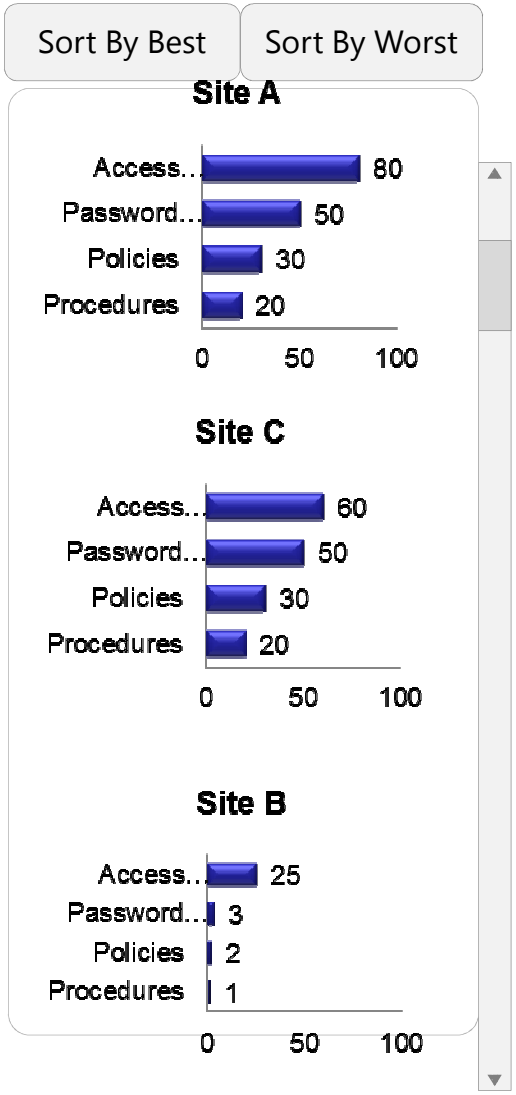
Compare

Site	Total Questions Answered	Yes	No
Site A	560	300	260
Site B	342	300	42
Site C	268	152	116







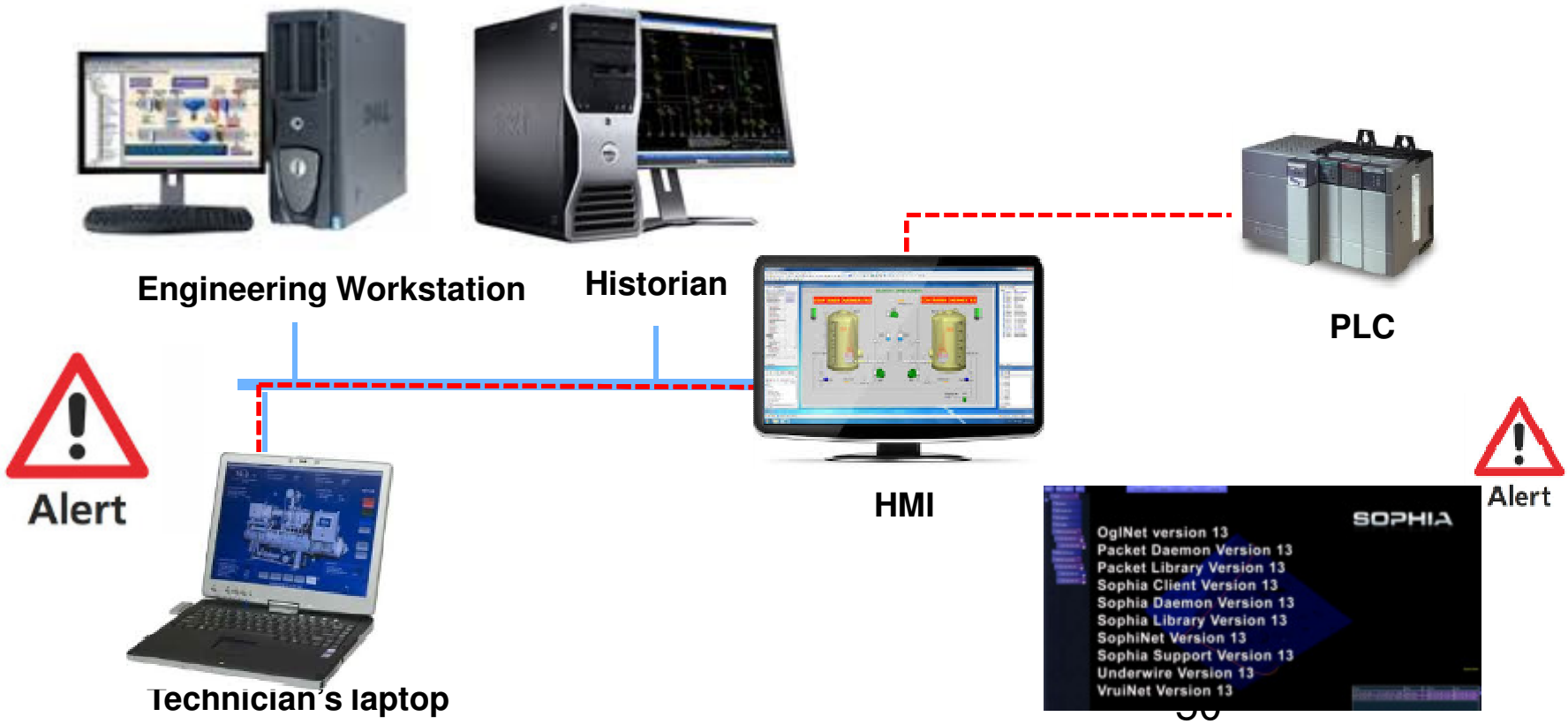


SOPHIA

http://nexdefense.com/?ao=1

SOPHIA

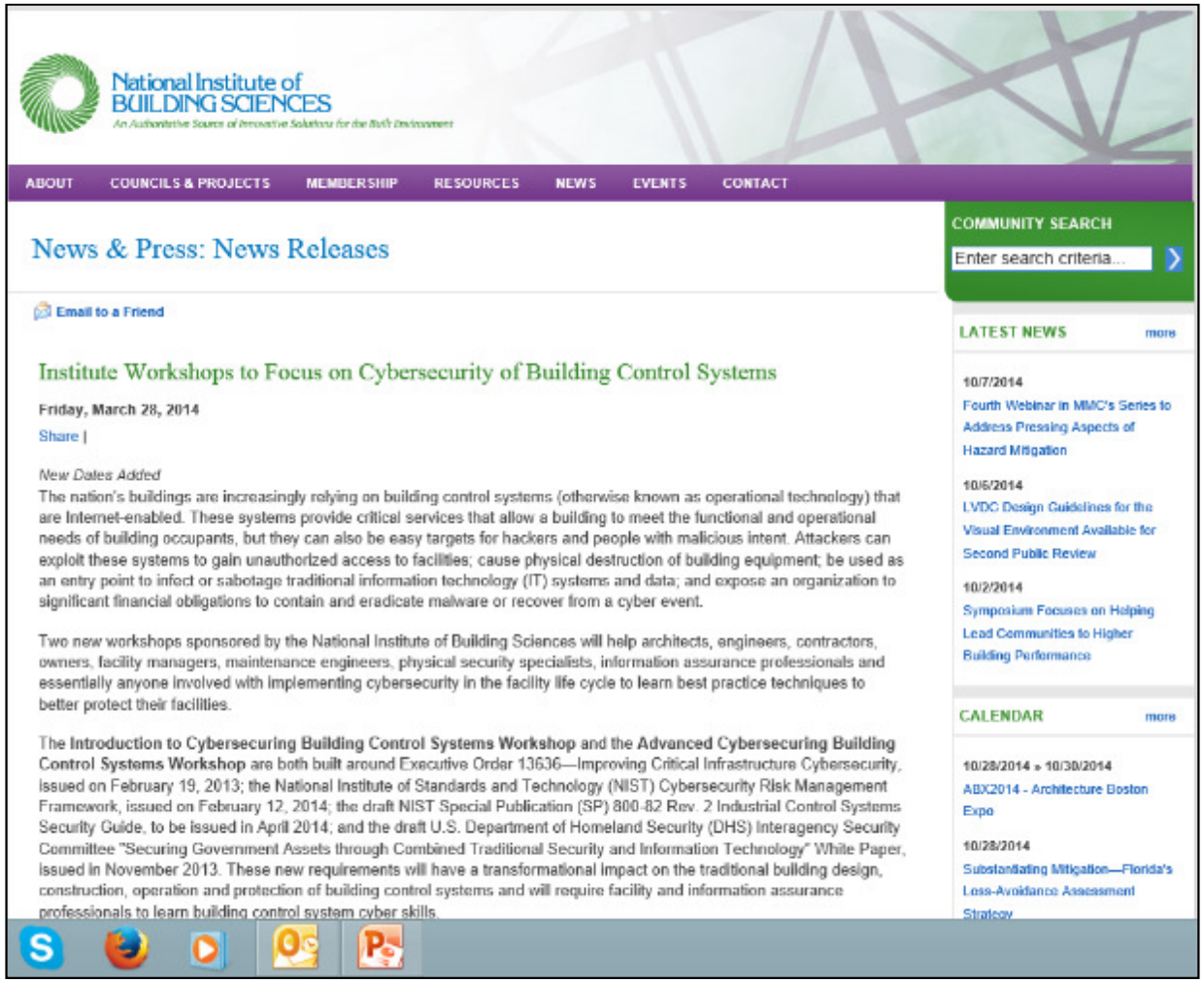
- Sophia can baseline approved/expected communication behavior
- Alert on communication sessions that are suspect/unexpected
- Example: DB Technician laptop should never send a Modbus command to the PLC



WBDG Cybersecurity Resource Page

http://www.wbdg.org/resources/cybersecurity.php

Cybersecuring Buildings Workshops



http://www.nibs.org/news/166752/Institute-Workshops-to-Focus-on-Cybersecurity-of-Building-Control-Systems.htm

QUESTIONS

Michael Chipley
President, The PMC Group LLC
Cell: 571-232-3890
E-mail: mchipley@pmcgroup.biz