AUTOMATING THE 20 CRITICAL SECURITY CONTROLS

Wolfgang Kandek, CTO
Qualys
2012 – the Year of Data Breaches

Lax Security at LinkedIn Is Laid Bare

SAN FRANCISCO — LinkedIn is a data company that did not protect its data.

Last week, hackers breached the site and stole more than six million of its customers’ passwords, which had been only lightly encrypted. They were posted to a Russian hacker forum for all to see.

That LinkedIn was attacked did not surprise anyone. Companies’ computer systems are attacked every day. Indeed, the CBS music site Last.fm and the dating site eHarmony confirmed last week that millions of user passwords were stolen.
2013 – continued in a similar Way
Background

- Open System Administration Channels
- Default and Weak Passwords
- End-user has Administrator Privileges
- Outdated Software Versions
- Non-hardened Configurations

➤ Flaws in System Administration
Solution

- 20 Critical Controls
- Owned by SANS
  - with widespread industry expert input
Solution

20 Critical Controls

Owned by SANS with widespread industry input.

- US National Security Agency Red Team and Blue Team
- US DoD Computer Network Defense Architecture Group
- US DoD Defense Cyber Crime Center (DC3)
- US Department of State, Office of the CISO
- US Air Force
- US Army Research Laboratory
- US Department of Transportation, Office of the CIO
- US Department of Health and Human Services, Office of the CISO
- US Government Accountability Office (GAO)
- MITRE Corporation
- The SANS Institute
- Plus commercial penetration testing and forensics experts at InGuardians and Mandiant.
Solution

• 20 Critical Controls
• Owned by SANS
  • with widespread industry expert input
  • International participation
Solution

CPNI Critical controls

Centre for the Protection of National Infrastructure

Top 20 critical security controls for cyber defence

The top 20 critical security controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence. CPNI is participating in an international government-industry effort to promote the top 20 critical controls for computer and network security. The development of these controls is being coordinated by the SANS Institute.
## Solution

<table>
<thead>
<tr>
<th>Mitigation Strategy Effectiveness Ranking</th>
<th>Mitigation Strategy</th>
<th>Overall Security Effectiveness</th>
<th>User Resistance</th>
<th>Upfront Cost (Staff, Equipment, Technical Complexity)</th>
<th>Maintenance Cost (Mainly Staff)</th>
<th>Designed to Prevent or Detect an Intrusion</th>
<th>Helps Mitigate Intrusion Stage 1: Code Execution</th>
<th>Helps Mitigate Intrusion Stage 2: Network Propagation</th>
<th>Helps Mitigate Intrusion Stage 3: Data Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications.</td>
<td>Excellent</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Prevent</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.</td>
<td>Excellent</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Prevent</td>
<td>Yes</td>
<td>Possible</td>
<td>Possible</td>
</tr>
</tbody>
</table>
Solution

- 20 Critical Controls
- Owned by SANS
  - with widespread industry input
  - International participation
- Prioritized
<table>
<thead>
<tr>
<th>Critical Control</th>
<th>Effect on Attack Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory of Authorized and Unauthorized Devices</td>
<td>Very High</td>
</tr>
<tr>
<td>2. Inventory of Authorized and Unauthorized Software</td>
<td>Very High</td>
</tr>
<tr>
<td>3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers</td>
<td>Very High</td>
</tr>
<tr>
<td>4. Continuous Vulnerability Assessment and Remediation</td>
<td>Very High</td>
</tr>
<tr>
<td>5. Malware Defenses</td>
<td>High</td>
</tr>
<tr>
<td>6. Application Software Security</td>
<td>High</td>
</tr>
<tr>
<td>7. Wireless Device Control</td>
<td>High</td>
</tr>
<tr>
<td>8. Data Recovery Capability</td>
<td>Moderately High to High</td>
</tr>
<tr>
<td>9. Security Skills Assessment and Appropriate Training to Fill Gaps</td>
<td>Moderately High to High</td>
</tr>
<tr>
<td>10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</td>
<td>Moderately High</td>
</tr>
<tr>
<td>11. Limitation and Control of Network Ports, Protocols, and Services</td>
<td>Moderately High</td>
</tr>
<tr>
<td>12. Controlled Use of Administrative Privileges</td>
<td>Moderate to Moderately High</td>
</tr>
<tr>
<td>13. Boundary Defense</td>
<td>Moderate</td>
</tr>
<tr>
<td>14. Maintenance, Monitoring, and Analysis of Security Audit Logs</td>
<td>Moderate</td>
</tr>
<tr>
<td>15. Controlled Access Based on the Need to Know</td>
<td>Moderate</td>
</tr>
<tr>
<td>16. Account Monitoring and Control</td>
<td>Moderate</td>
</tr>
<tr>
<td>17. Data Loss Prevention</td>
<td>Moderately Low to Moderate</td>
</tr>
<tr>
<td>18. Incident Response Capability</td>
<td>Moderately Low to Moderate</td>
</tr>
<tr>
<td>19. Secure Network Engineering</td>
<td>Low</td>
</tr>
<tr>
<td>20. Penetration Tests and Red Team Exercises</td>
<td>Low</td>
</tr>
</tbody>
</table>
Solution

- 20 Critical Controls
- Owned by SANS
  - With widespread industry expert input
  - International participation
- Prioritized
- Automation is critical to success
Results First 12 Months

Personal Computers and Servers

Domestic Sites

Foreign Sites

89% Reduction

90% Reduction
Solution

- 20 Critical Controls
- Owned by SANS
  - with widespread industry input
  - International participation
- Prioritized
- Automation is critical to success
  - 90 % Risk Reduction at US DoS
  - 85 % Incident Reduction at DSD Australia
## Solution

<table>
<thead>
<tr>
<th>Critical Control</th>
<th>Effect on Attack Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory of Authorized and Unauthorized Devices</td>
<td>Very High</td>
</tr>
<tr>
<td>2. Inventory of Authorized and Unauthorized Software</td>
<td>Very High</td>
</tr>
<tr>
<td>3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers</td>
<td>Very High</td>
</tr>
<tr>
<td>4. Continuous Vulnerability Assessment and Remediation</td>
<td>Very High</td>
</tr>
</tbody>
</table>
Qualys

- QualysGuard
  - Vulnerability Management
  - Policy Compliance
  - Web Application Scanning
  - PCI
  - Malware Detection

- SaaS Solution
  - Browser-based, Multi-tenant
  - Public and Private Cloud
  - Scanning, Reporting, Ticketing
  - Extensive API
CC1: Hardware Inventory

- Asset Visibility
  - Size of Network
  - Machine Types
  - Location
# CC1: Hardware Inventory

![Hardware Inventory screenshot](image-url)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>188.15.40</td>
<td>c-67-188-15-40.hsd1.ca.comcast.net</td>
</tr>
</tbody>
</table>
| 68.123.47.151       | adsl-68-123-47-151.dsl.ptln13.pacbell.net | Linux 2.4.2.6
| 68.124.23.73        | adsl-68-124-23-73.dsl.ptln13.pacbell.net | Linux 2.4.2.6
| 69.181.165.102      |                                  |
| 70.1.238.61         | 70-1-238-61-pools.spscdns.net     | Windows 2003/XP
| 70.96.188.21        | box21.bluehost.com                |
| 71.198.187.95       | c-71-198-187-95.hsd1.ca.comcast.net |
| 75.101.203.111      | cc2-75-101-203-111.compute-        | Linux 2.4.2.6 / by_di.pl

**Notes:**
- The screenshot shows a hardware inventory as managed by QualysGuard Enterprise Suite.
- The IP addresses listed are examples of systems being monitored.
- The system details include the hostname and operating system type.

---

**RSA Conference Europe 2013**

[@RSAC](https://twitter.com/RSAConference)
CC1: Hardware Inventory
CC1: Hardware Inventory

- Asset Visibility
  - Size of Network
  - Machine Types
  - Location
- New Equipment Detection
  - Authorized
  - Unauthorized
CC1: Hardware Inventory

Sandbox Changes

September 12, 2012

Report Summary
User Name: Wolfgang Kandek
Report Template: Host Changes
Hosts Matching Filters: 2
Map 1:
Title: Sandbox Map
Date: 2012-09-10 13:58:36
Map 2:
Title: Sandbox Map - 20120910 - 20120910
Date: 09/10/2012 at 16:47:53 (GMT-0700)
Total Hosts Found: 3

none:[192.168.100.51-192.168.100.54](2)

<table>
<thead>
<tr>
<th>IP</th>
<th>DNS</th>
<th>NetBIOS</th>
<th>Router</th>
<th>OS</th>
<th>Approved</th>
<th>Scannable</th>
<th>Live</th>
<th>Netblock</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.55</td>
<td>WKA NDEK-X PTEST3</td>
<td>Windows XP Service Pack 2-3</td>
<td>S</td>
<td>L</td>
<td>N</td>
<td>Added</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.100.57</td>
<td>Ubuntu / Linux 2.6.x</td>
<td></td>
<td>S</td>
<td>L</td>
<td>N</td>
<td>Added</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CC1: Hardware Inventory

- Automation
  - Scans are scheduled
  - Delta Reports are scheduled
  - Reports can be e-mailed
  - Alerting on newly discovered hosts
    - Via API
  - Integration into Asset Management Systems
    - Via API
  - Coming: ticket generation on newly discovered hosts
CC2: Software Inventory

- Asset Visibility
  - Operating Systems
  - Applications
  - Versions
  - Patch Levels
- Blacklisting
CC2: Software Inventory

(2.2) 2162 Current list of 'Prohibited software applications installed'
Failed

The installation of unauthorized, incorrect, or rogue applications can interfere with user workflow and delay the timely completion of company projects. As a single rogue application can bring the entire production process to a halt and even compromise multiple systems, unauthorized, incorrect versions or, or rogue applications installed on any system should identified and removed as appropriate to the needs of the business.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall registry key.

<table>
<thead>
<tr>
<th>Expected</th>
<th>does not contain regular expression list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mIRC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Updated: 09/09/2012 at 14:43:00 (GMT-0700)</td>
</tr>
<tr>
<td>123 Write All Stored Passwords</td>
</tr>
<tr>
<td>Adobe Flash Player 10 ActiveX:10.2.152.32</td>
</tr>
<tr>
<td>Look@LAN 2.50 Build 35</td>
</tr>
<tr>
<td>Microsoft Office Publisher MUI (English) 2007:12.0.4518.1014</td>
</tr>
<tr>
<td>Microsoft Office Shared MUI (English) 2007:12.0.4518.1014</td>
</tr>
<tr>
<td>Microsoft Office Shared Setup Metadata MUI (English) 2007:12.0.4518.1014</td>
</tr>
<tr>
<td>Microsoft Office Word MUI (English) 2007:12.0.4518.1014</td>
</tr>
<tr>
<td>Microsoft Software Update for Web Folders (English) 12:12.0.4518.1014</td>
</tr>
<tr>
<td>mIRC:7.19</td>
</tr>
<tr>
<td>Network Stumbler 0.4.0 (remove only)</td>
</tr>
<tr>
<td>Oracle VM VirtualBox Guest Additions 4.1.8:4.1.8.0</td>
</tr>
</tbody>
</table>
CC2: Software Inventory

- Asset Visibility
  - Operating Systems
  - Applications
  - Versions
  - Patch Levels
- Blacklisting
- Whitelisting
CC2: Software Inventory

- Asset Visibility
  - Operating Systems

(2.1) 2161 Current list of 'Required software applications installed'

The installation of the correct primary user applications, such as the 'Microsoft Office Suite' and other supporting software, are critical to the proper user workflow and smooth completion of company business. As having the right software supports these projects, while a single rogue application can bring the entire process to a halt, the applications installed on the system should match those specified as appropriate to the needs of the business.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall registry key.

<table>
<thead>
<tr>
<th>Expected</th>
<th>contains regular expression list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft Office</td>
</tr>
</tbody>
</table>

| Actual                          | Last Updated:09/09/2012 at 14:43:00 (GMT-0700) |
|                                | 123 Write All Stored Passwords |
|                                | Adobe Flash Player 10 ActiveX:10.2.152.32 |
|                                | Microsoft Office Word MUI (English) 2007:12.0.4518.1014 |
|                                | Microsoft Software Update for Web Folders (English) 12:12.0.4518.1014 |
|                                | mIRC:7.19 |
|                                | Network Stumbler 0.4.0 (remove only) |
|                                | Oracle VM VirtualBox Guest Additions 4.1.8:4.1.8.0 |
CC2: Software Inventory

- Asset Visibility
  - Operating Systems
  - Applications
  - Versions
  - Patch Levels
- Blacklisting
- Whitelisting
- Interactive Search
CC2: Software Inventory

- Asset Visibility
- Operating Systems
- Applications
- Versions
- Patch Levels
- Blacklisting
- Whitelisting
- Interactive Search

IP / DNS Hostname | Version
-------------------|--------
123 Write All Stored Passwords (1 Host) | 
192.168.100.51  
wkan dek-xpt est | 
Adobe Flash Player 10 ActiveX (1 Host) |  
192.168.100.51  
wkan dek-xpt est | 10.2.152.32 
Adobe Reader 9.3 (1 Host) | 
192.168.100.51  
wkan dek-xpt est | 9.3 .0 
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595) (1 Host) | 
192.168.100.51  
wkan dek-xpt est | 1 
Hotfix for Windows XP (KB954550-v5) (1 Host) | 
192.168.100.51  
wkan dek-xpt est | 5 
Look@LAN 2.50 Build 35 (1 Host) | 
192.168.100.51  
wkan dek-xpt est |
CC2: Software Inventory

Asset Visibility
- Operating Systems
- Applications
- Versions
- Patch Levels
- Blacklisting
- Whitelisting

Interactive Search

QUALYS GUARD ENTERPRISE SUITE

Dashboard  Scans  Reports  Remediation  Assets  KnowledgeBase  Users

Assets  Asset Groups  Host Assets  Asset Search  Virtual Hosts  Domains  Applications  Ports/Services

Search for Application:  and Asset Group:  and IP Address or Net Block

mIRC

IP / DNS Hostname  Version

mIRC (4 Hosts)

192.168.100.51
wkandek-xptest

192.168.100.55
wkandek-xptest3

192.168.100.56
wkandek-xptest4

192.168.100.54
wkandek-xptest2

wkandek-xptest

7.19

7.19

7.19

7.19
CC2: Software Inventory

- Automation
  - Scans are scheduled
  - Reports are scheduled
  - Reports can be emailed
  - Alerting on Exceptions
    - Via API
  - Integration into Asset Management Systems
    - Via API
  - Coming: Ticket generation on Exceptions
CC3: Secure Base Configurations

- Configuration Validation
- SCAP/FDCC
CC3: Secure Base Configurations

```
Results

192.168.100.54 (Score: 10.96 / 100)
IP Address: 192.168.100.54
DNS Name: wkandek-xptest2
NetBIOS Name: WKADEK-XPTEST2
OS: Windows XP
Last Scan Date: 09/10/2012 at 11:30:05 (GMT-0700)

<table>
<thead>
<tr>
<th>CCE</th>
<th>Rule ID</th>
<th>Rule Title</th>
<th>Posture</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCE</td>
<td>account_lockout_duration</td>
<td>Account Lockout Duration</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>account_lockout_threshold</td>
<td>Account Lockout Threshold</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>GuestAccountStatus</td>
<td>Accounts: Guest account status</td>
<td>Passed</td>
</tr>
<tr>
<td>CCE</td>
<td>LimitBlankPassword</td>
<td>Accounts: Limit local account use of blank passwords to console logon only</td>
<td>Passed</td>
</tr>
<tr>
<td>CCE</td>
<td>RenameAdministrator</td>
<td>Accounts: Rename administrator account</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>RenameGuest</td>
<td>Accounts: Rename guest account</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>DebugPrograms_Admnistrators</td>
<td>Administrators Have Right To Debug Programs</td>
<td>Passed</td>
</tr>
<tr>
<td>CCE</td>
<td>AlertService</td>
<td>Alert Service Disabled</td>
<td>Passed</td>
</tr>
<tr>
<td>CCE</td>
<td>AlwaysUseClassicLogon</td>
<td>Always Use Classic Logon</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>arp.exePermissions</td>
<td>arp.exe Permissions</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>at.exePermissions</td>
<td>at.exe Permissions</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>attrib.exePermissions</td>
<td>attrib.exe Permissions</td>
<td>Failed</td>
</tr>
<tr>
<td>CCE</td>
<td>AuditAccessToGlobalObjects</td>
<td>Audit: Audit the access of global system objects</td>
<td>Passed</td>
</tr>
</tbody>
</table>

231 of 231 Items Shown, 0 selected
```
CC3: Secure Base Configurations

- Configuration Validation
  - SCAP/FDCC
  - Cyberscope Reporting
  - CIS
CC3: Secure Base Configurations

- Configuration Validation
  - SCAP

Compliance Policy Library

Policies
Browse the following list of Sample Policies to quickly import and apply the full set of controls created to meet the requirements of the benchmark mentioned in each description.


This Policy includes the CIS Benchmark-based Controls with Enterprise-level security settings preconfigured. When protection standards vary for an individual control within a specific configuration type, such as 'Enterprise,' which may have differing requirements for desktops and laptops, the most stringent value will be set as the default. The controls defined within this importable policy match the requirements listed by the CIS Benchmark for the Microsoft Windows XP-Professional operating system. In the case of CIS-required Control duplication (where a Control requirement appears in more than one section of the benchmark), QualysGuard Policy Compliance limits the existence of any Controls within a single policy to one (1) occurrence of each.
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning
CC4: Continuous Vulnerability Assessment/Remediation
CC4: Continuous Vulnerability Assessment/Remediation
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning
- Verify Patching
CC4: Continuous Vulnerability Assessment/Remediation
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning
- Verify Patching
- Report on Unauthorized Services
CC4: Continuous Vulnerability Assessment/Remediation

Edit Scan Template

Services
- Required Services
  - Required Services
  - Available Services
  - Unauthorized Services
- Service Info
- Ports
  - Required Ports:
  - Ports

Launch Help
Cancel
Save
Test
Save As...
CC4: Continuous Vulnerability Assessment/Remediation
CC4: Continuous Vulnerability Assessment/Remediation

- Weekly/Daily Scheduled Vulnerability Scanning
- Authenticated Scanning
- Verify Patching
- Report on Unauthorized Services
CC4: Continuous Vulnerability Assessment/Remediation

- Automation
  - Scans are scheduled
  - Reports are scheduled
  - Reports are emailed
  - Alerting on Vulnerabilities
  - Tickets for Vulnerabilities, Remediation SLA and Confirmation
  - Integration into Asset Management Systems
    - Via API
Other Critical Controls

• CC6: Application Software Security
  • Automated Web Application Scans

• CC7: Wireless Device Controls
  • Wiresside Detection

• CC11: Control of Network Ports
  • Scans and Reports for authorized and unauthorized Ports and Services

• CC16: Account Monitoring
  • Controls for Admin accounts, password policies, account lockout settings
Policy Dynamics

• Ability to add tactical controls
• Example: Recent Internet Explorer Vulnerabilities CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
• Mitigated by use of EMET
Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)

Microsoft Releases Security Advisory 2757760

Today we released Security Advisory 2757760 to address an issue that affects Internet Explorer 9 and earlier versions if a user views a website hosting malicious code. Internet Explorer 10 is not affected.

We have received reports of only a small number of targeted attacks and are working to develop a security update to address this issue. In the meantime, customers using Internet Explorer are protected when they deploy the following workarounds and mitigations included in the advisory:

- Deploy the Enhanced Mitigation Experience Toolkit (EMET)
  This will help prevent exploitation by providing mitigations to help protect against this issue and should not affect usability of websites.
Ability to add tactical controls
Example: Recent Internet Explorer Vulnerabilities CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
Mitigated by use of EMET
Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
Policy Dynamics

• Ability to add tactical controls
• Example: Recent Internet Explorer Vulnerabilities CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
• Mitigated by use of EMET
• Audit the Deployment
Ability to add tactical controls

Example: Recent Internet Explorer Vulnerabilities

- CVE-2012-4969

Mitigated by use of EMET

Audit the Deployment Policy Dynamics
Policy Dynamics

- Ability to add tactical controls
- Example: Recent Internet Explorer Vulnerabilities CVE-2012-4969 (Sep/12)/KB2794220 (Dec/12)
- Mitigated by use of EMET
- Audit the Deployment
  - User Defined Registry Check
Summary

- Functionality to assess Controls exist
- Automation available, but frequently API integrations is needed
- Offerings are improving with better workflow coming
Thank You

Wolfgang Kandek – wkandek@qualys.com

@wkandek

http://laws.qualys.com