

Check Yourself!

Three Self-Awareness Keys To Improve Your Organization's Security

Justin Hall
Director, Security Services



/usr/bin/whoami

Twelve years with CBTS as security consultant to shops small (5 person) and large (Fortune 5)

GIAC Certified Penetration Tester, Incident Handler, Forensic Analyst

BSidesCincinnati cofounder

Husband, dad, Christ follower, gamer

A black and white photograph of a river with rapids. The water is turbulent and white with foam as it flows over rocks. The background is dark and out of focus, showing some trees. A solid blue rectangular box is positioned on the left side of the image, containing white text.

The rocks you can see &
the ones you can't

what you know



what you don't

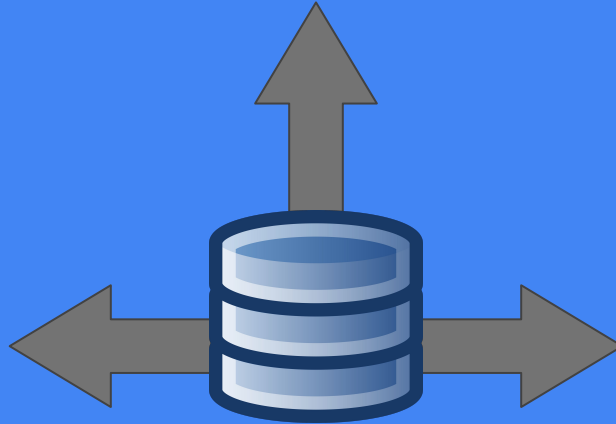


1. Your assets
2. Your threats
3. Your vulnerabilities



user accounts

software



hardware



Installed Software

Current IP

Current User

Physical Location

Defense Status

The screenshot displays the Lansweeper interface with the following details:

- Asset options:** New asset, Edit asset, Rescan Asset, Wake on Lan, Refresh Warranty, QR Code, Deploy Package.
- Basic actions:** Ping, Pathping, Traceroute, NBTstat, HTTP, HTTPS, SSH (putty), Remote desktop, Open C\$, Open Admin\$, Computer management, Services management, Event viewer, Shared folders, Reboot, Shutdown, Abort shutdown.
- Advanced actions:** Device tester.
- Asset details:**
 - Asset name:** CHI-DC01 (circled in red)
 - IP:** 172.16.30.200 (circled in red)
 - Manufacturer:** Microsoft Corporation
 - Model:** Virtual Machine
 - Memory:** 1.0 GB
 - Processor:** 1 * Intel Core i7-4500U CPU @ 1.80GHz
 - Domain:** globomantics
 - OU:** OU=Domain Controllers, DC=GLOBOMANTICS, DC=local
 - C:** 0.9 GB free of 14.9 GB
- Scan status:** Active
- Scan server:** chi-win81
- State:** Active
- IP Location:** Local Subnet
- Asset location:** Undefined (circled in red)
- Serial:** 8469-9638-6902-1028-1552-2278-75
- Uptime:** 22 days 4 h 23 m
- First seen:** 24/03/2015 13:50:20
- Last seen:** 24/03/2015 14:03:09
- Purchased:** unknown
- Warranty:** unknown

The **Software** tab is selected, showing the following information:

- Asset Type:** Windows
- Last user:** Jeff Hicks (circled in red)
- OS:** Microsoft Windows Server 2008 R2 Enterprise (x64) SP1
- Manufacturer:** Microsoft Corporation
- Model:** Virtual Machine
- Memory:** 1.0 GB
- Processor:** 1 * Intel Core i7-4500U CPU @ 1.80GHz
- Domain:** globomantics
- OU:** OU=Domain Controllers, DC=GLOBOMANTICS, DC=local
- C:** 0.9 GB free of 14.9 GB

The **Anti-Virus** section shows:

- Name:** No antivirus installed (circled in red)
- Status:** Virus Signature

The **Recent event log entries** section shows:

- No event log information scanned**

The **Uptime calendar** section shows:

- No event log information scanned**

Data Awareness

- What data do we have?
- Who owns our data?
- What data is sensitive? How sensitive?
- How do we protect the data?
- How do we destroy the data?
- If the data is exposed, what steps must we take?



1. Your assets
2. Your threats
3. Your vulnerabilities



State
Sponsored



Organized
Crime



Hacktivism



Insider
Threat

What Might A Threat Want?

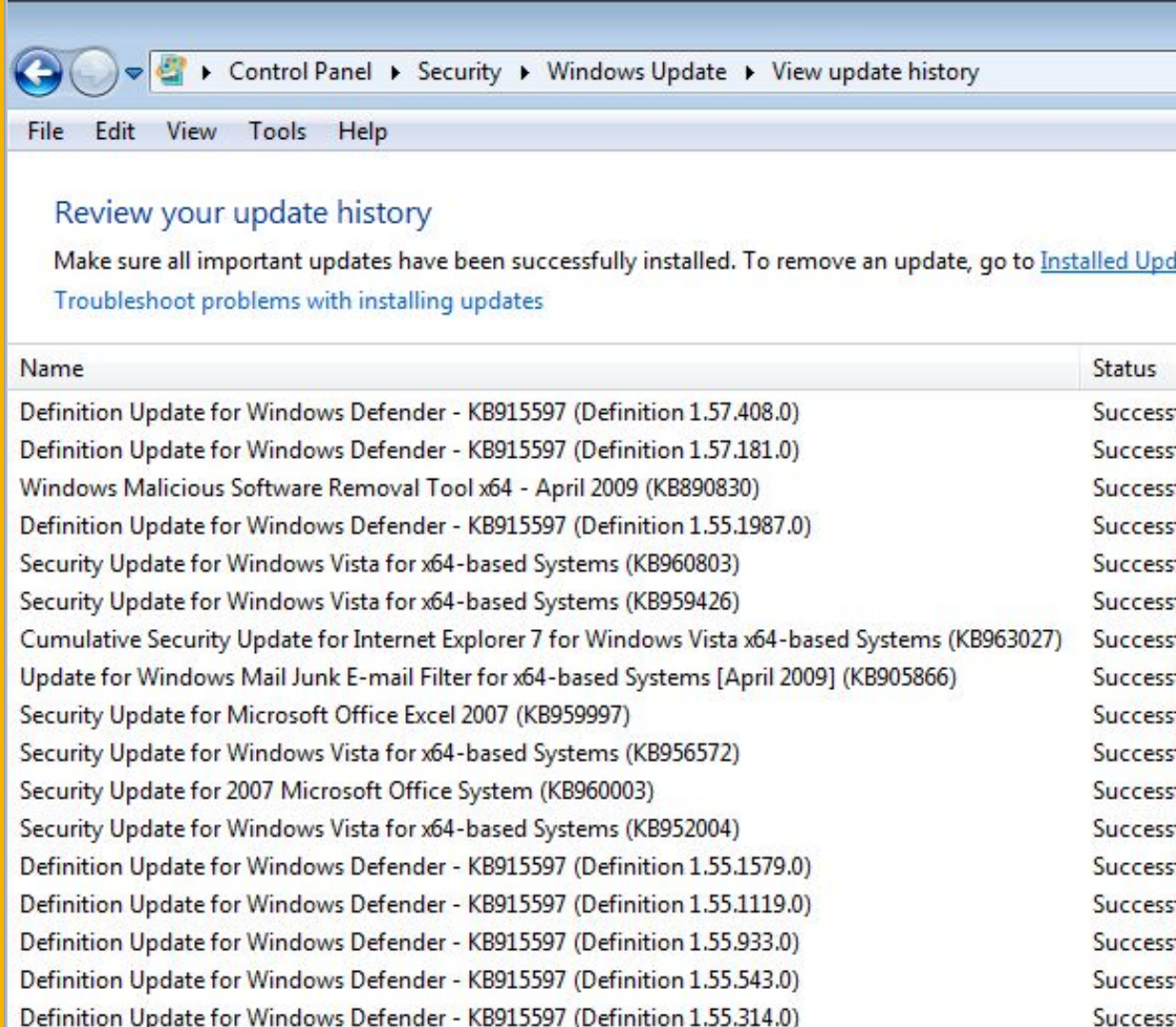
- Customer records
- Financial data
- Intellectual property
- Technical information
- Credentials and keys
- Employee information



1. Your assets
2. Your threats
3. Your vulnerabilities

Technical Vulnerabilities

- Missing patches
- Obsolete operating systems and software
- Weak passwords
- Insufficient / no encryption
- Configuration flaws



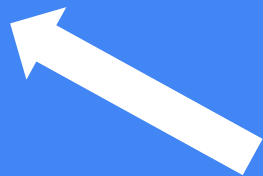
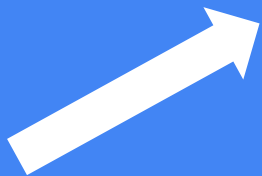
The screenshot shows the Windows Update history window. The title bar indicates the path: Control Panel > Security > Windows Update > View update history. The window has a menu bar with File, Edit, View, Tools, and Help. Below the menu bar, there is a heading "Review your update history" followed by instructions: "Make sure all important updates have been successfully installed. To remove an update, go to [Installed Updates](#)." and a link "Troubleshoot problems with installing updates". Below this is a table with two columns: "Name" and "Status". The table lists various updates, all of which are marked as "Successful".

Name	Status
Definition Update for Windows Defender - KB915597 (Definition 1.57.408.0)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.57.181.0)	Successful
Windows Malicious Software Removal Tool x64 - April 2009 (KB890830)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.55.1987.0)	Successful
Security Update for Windows Vista for x64-based Systems (KB960803)	Successful
Security Update for Windows Vista for x64-based Systems (KB959426)	Successful
Cumulative Security Update for Internet Explorer 7 for Windows Vista x64-based Systems (KB963027)	Successful
Update for Windows Mail Junk E-mail Filter for x64-based Systems [April 2009] (KB905866)	Successful
Security Update for Microsoft Office Excel 2007 (KB959997)	Successful
Security Update for Windows Vista for x64-based Systems (KB956572)	Successful
Security Update for 2007 Microsoft Office System (KB960003)	Successful
Security Update for Windows Vista for x64-based Systems (KB952004)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.55.1579.0)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.55.1119.0)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.55.933.0)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.55.543.0)	Successful
Definition Update for Windows Defender - KB915597 (Definition 1.55.314.0)	Successful

Organizational Vulnerabilities

- Missing or vague policies
- Poor user behavior
- Insecure software development practices
- Lack of exec focus







Vulnerability Assessments

Penetration Tests

Web Application Reviews

Security Program & Architecture

BSidesCincinnati 2017 - May 20

Listen to excellent talks! Network! Learn! Beer! Food! Swag!

@bsidescincy / bsidescincy.org



Thanks!

@justinhall
justin.hall@cbts.net