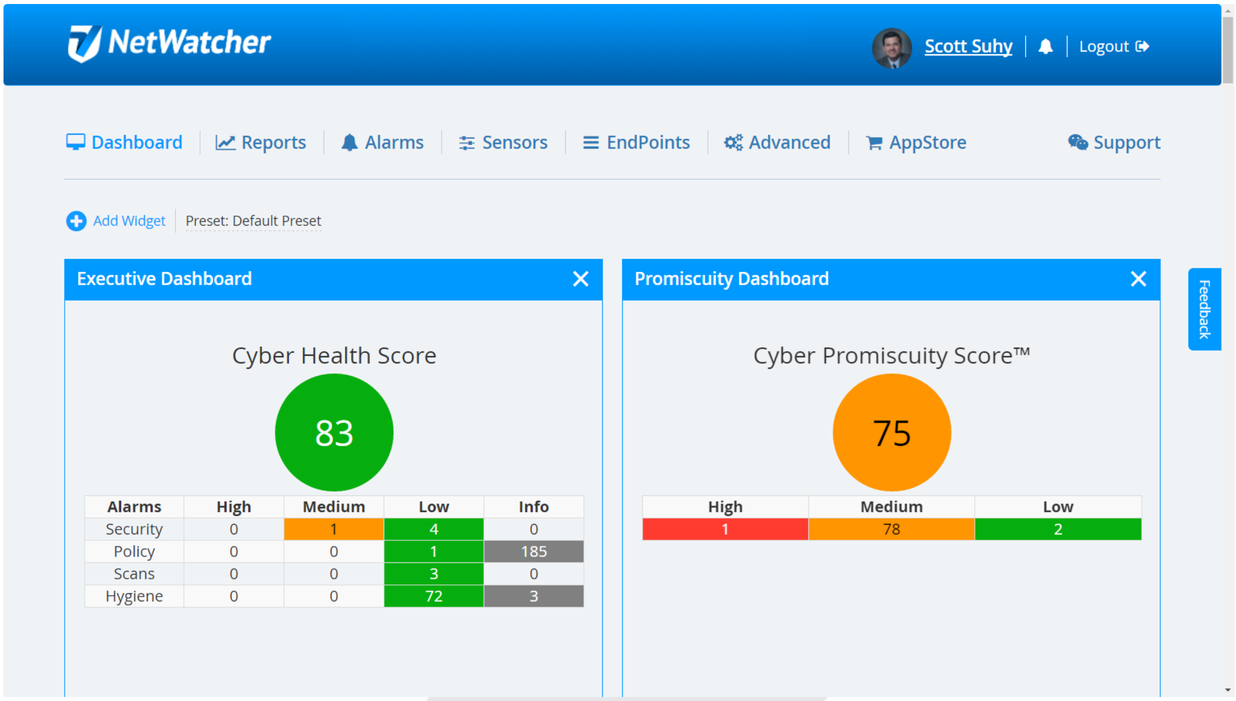
NetWatcher

NetWatcher® Managed Detection & Response Services & the CSC 20

*"The CIS Critical Security Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "what should my enterprise do" to "what should we ALL be doing" to improve security across a broad scale… Controls CSC 1 through CSC 5 are essential to success and should be considered among the very first things to be done." from--***"CIS Critical Security Controls,"** ***www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf***

NetWatcher® can accelerate and simplify your path to implementing the CIS Controls. The NetWatcher sensor, endpoint and service provide built-in security capabilities and integrated threat intelligence to help you detect and respond to threats faster and without the need for deep security expertise or investment in numerous point products. The NetWatcher dashboard provides the visibility you need to see the status of all security controls such as your risk today (Health Score) and in the future (Promiscuity Score).



Executive Dashboard

Cyber Health Score

83

Alarms	High	Medium	Low	Info
Security	0	1	4	0
Policy	0	0	1	185
Scans	0	0	3	0
Hygiene	0	0	72	3

Promiscuity Dashboard

Cyber Promiscuity Score™

75

High	Medium	Low
1	78	2

What is NetWatcher®:

NetWatcher is a 24x7 network and endpoint security monitoring service designed specifically for ease of use, accuracy and affordability. With NetWatcher you can reduce risk and support regulatory compliance security requirements. You get: ♣ An advanced, tightly integrated, security platform that only the Fortune 5000 could afford in the past ♣ Actionable threat intelligence on what malware exists in your enterprise and remediation guidance ♣ Visibility into the unintentional insider threat -- what your employees are doing on the network that is exposing the organization to exploit ♣ A Secure Operation Center with security analysts monitoring your data and reaching out to your team when necessary ♣ Easy to use customer portal designed for managers and IT, not for those hard to find security analysts, however you can go deep if you want… ♣ Real time scores for today's security situational awareness picture and the risk of exploit in the future

NetWatcher Includes:

♣ Host Intrusion Detection System (HIDS) Endpoint Agents ♣ Network Intrusion Detection System (NIDS) ♣ Security Information & Event Management System (SIEM) ♣ Vulnerability Scanner ♣ Net-flow Analysis ♣ Actionable Threat Intelligence Use Cases: ♣ Monitor Corporate Network and Assets for Security Exploits and Hygiene Issues ♣ Monitor AWS, Azure or Google Cloud Servers ♣ Monitor Off Network Assets (via Sensor-in-the-Cloud™) ♣ Regulatory Compliance-as-a-Service support for HIPAA, FINRA, NIST 800-171, PCIDSS, GLBA, NYCRR 500, etc.)

As we go through each of the 20 controls we will also contrast and compare the control to other security mandates/regulations.

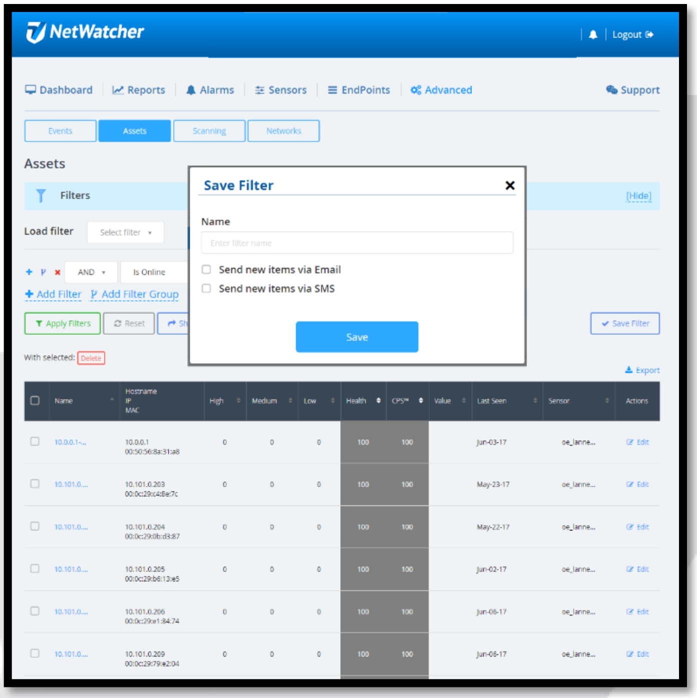
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	A.8.1.1 A.9.1.2 A.13.1.1		2.4	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	

NetWatcher builds its inventory of assets as well as the software running on them in 3 ways:

1. Passive Network Monitoring via Network Intrusion Detection that highlights hosts IP, hostname and hardware MAC address pairings of assets on your network and indicators of installed software packages.
2. In addition, the NetWatcher Netagent does a thorough inventory of the desktop, laptop and server assets.



Assets

Save Filter

Name

Enter filter name

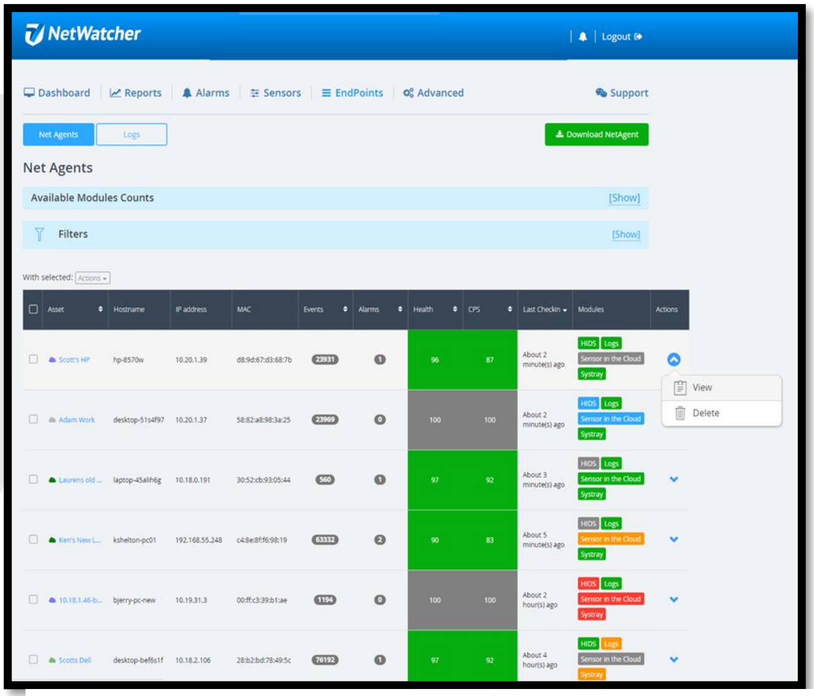
□ Send new items via Email

□ Send new items via SMS

With selected: Delete

Name	Hostname IP MAC	High	Medium	Low	Health	CPS™	Value	Last Seen	Sensor	Actions
10.0.0.1-...	10.0.0.1 00:50:56:8a:31:a8	0	0	0	100	100		Jun-03-17	oe_lanne...	Edit
10.101.0....	10.101.0.203 00:0c:29:c4:8e:7c	0	0	0	100	100		May-23-17	oe_lanne...	Edit
10.101.0....	10.101.0.204 00:0c:29:0b:d3:87	0	0	0	100	100		May-22-17	oe_lanne...	Edit
10.101.0....	10.101.0.205 00:0c:29:b6:13:e5	0	0	0	100	100		Jun-02-17	oe_lanne...	Edit
10.101.0....	10.101.0.206 00:0c:29:e1:84:74	0	0	0	100	100		Jun-06-17	oe_lanne...	Edit
10.101.0....	10.101.0.209 00:0c:29:79:e2:04	0	0	0	100	100		Jun-06-17	oe_lanne...	Edit

Figure 1 Asset Inventory



Net Agents

Available Modules Counts

With selected: Actions

Asset	Hostname	IP address	MAC	Events	Alarms	Health	CPS	Last Checkin	Modules	Actions
Scott's HP	hp-8570w	10.20.1.39	d8:9d:67:d3:68:7b	23931	1	96	87	About 2 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
Adam Work	desktop-51s4f97	10.20.1.37	58:82:a8:98:3a:25	23969	0	100	100	About 2 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
Laurens old ...	laptop-45alih6g	10.18.0.191	30:52:cb:93:05:44	560	1	97	92	About 3 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
Ken's New L...	kshelton-pc01	192.168.55.248	c4:8e:8f:f6:98:19	63332	2	90	83	About 5 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
10.18.1.46-b...	bjerry-pc-new	10.19.31.3	00:ff:c3:39:b1:ae	1194	0	100	100	About 2 hour(s) ago	HIDS Logs Sensor in the Cloud Systray	
Scotts Dell	desktop-bef6s1f	10.18.2.106	28:b2:bd:78:49:5c	76192	1	97	92	About 4 hour(s) ago	HIDS Logs Sensor in the Cloud Systray	

Figure 2 Assets running the NetAgent

3. Active Network scanning (Vulnerability Scanner Discovery Scans) that helps identify the device, the OS, running services, and the software installed on it.

Critical Security Control #2: Inventory of Authorized and Unauthorized Software

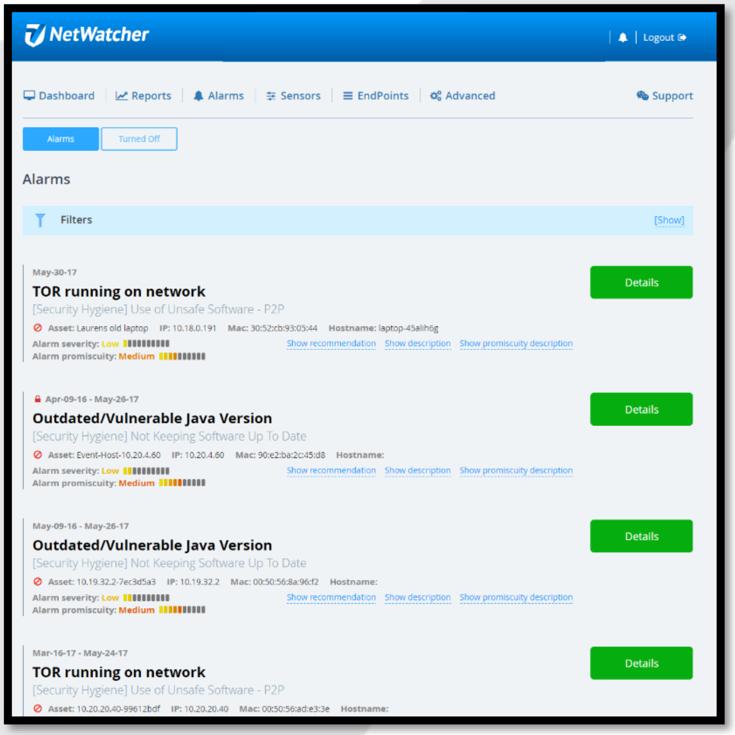
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
ID.AM-2 PR.DS-6	A.12.5.1 A.12.6.2	3.4.8 3.4.9	2.4	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	

The NetWatcher Netagent queries a software inventory of each device where it is installed.

Even without the Netagent installed the discovery and vulnerability assessment processes will Identify the software and services running on the assets and enhances your understanding of the devices on your network, resulting in a more dynamic and accurate inventory.

Intrusion Detection Systems (IDS) can also detect traffic patterns indicative of many applications especially prohibited clients such as TOR and BitTorrent or even outdated software such as Flash and Java that draw in ransomware.



Alarms

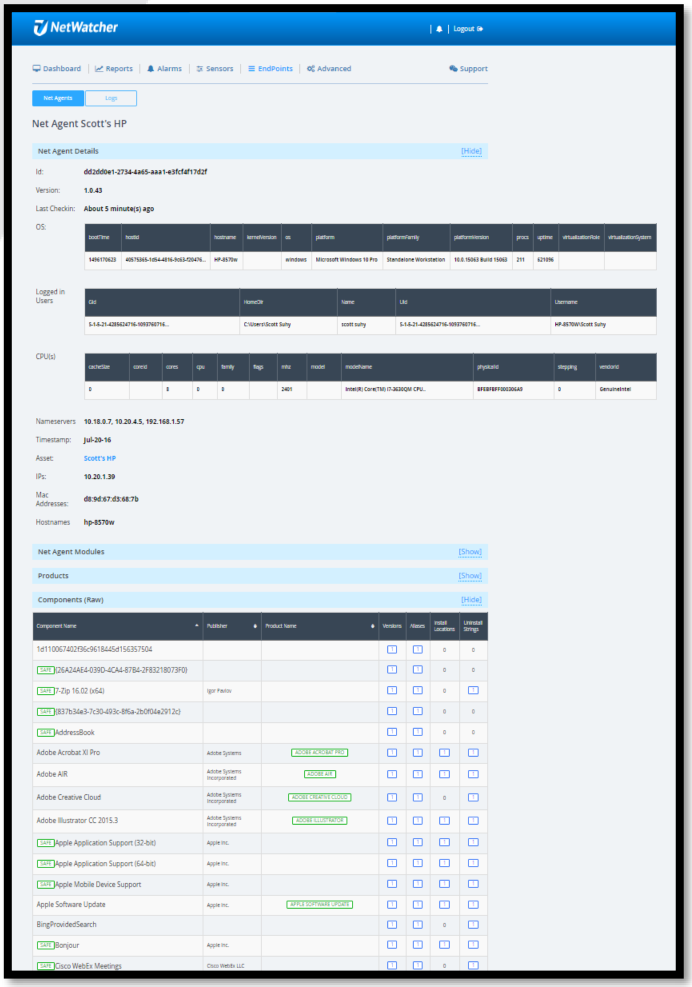
Filters [Show]

May-30-17
TOR running on network
[Security Hygiene] Use of Unsafe Software - P2P
Asset: Laurens old laptop IP: 10.18.0.191 Mac: 30:52:cb:93:05:44 Hostname: laptop-45alih6g
Alarm severity: Low
Alarm promiscuity: Medium
Show recommendation Show description Show promiscuity description
Details

Apr-09-16 - May-26-17
Outdated/Vulnerable Java Version
[Security Hygiene] Not Keeping Software Up To Date
Asset: Event-Host-10.20.4.60 IP: 10.20.4.60 Mac: 90:e2:ba:2c:45:d8 Hostname:
Alarm severity: Low
Alarm promiscuity: Medium
Show recommendation Show description Show promiscuity description
Details

May-09-16 - May-26-17
Outdated/Vulnerable Java Version
[Security Hygiene] Not Keeping Software Up To Date
Asset: 10.19.32.2-7ec3d5a3 IP: 10.19.32.2 Mac: 00:50:56:8a:96:f2 Hostname:
Alarm severity: Low
Alarm promiscuity: Medium
Show recommendation Show description Show promiscuity description
Details

Mar-16-17 - May-24-17
TOR running on network
[Security Hygiene] Use of Unsafe Software - P2P
Asset: 10.20.20.40-99612bdf IP: 10.20.20.40 Mac: 00:50:56:ad:e3:3e Hostname:
Details



Net Agent Scott's HP

Net Agent Details [Hide]

Id: dd2dd0e1-2734-4a65-aaa1-e3fcf4f17d2f
Version: 1.0.43
Last Checkin: About 5 minute(s) ago

OS:

bootTime	hostid	hostname	kernelVersion	os	platform	platformFamily	platformVersion	procs	uptime	virtualizationRole	virtualizationSystem
1496170623	40575365-1d54-4816-9c63-f20476...	HP-8570w		windows	Microsoft Windows 10 Pro	Standalone Workstation	10.0.15063 Build 15063	211	621096		

Logged in Users

Gid	HomeDir	Name	Uid	Username
S-1-5-21-4285624716-1093760716...	C:\Users\Scott Suhy	scott suhy	S-1-5-21-4285624716-1093760716...	HP-8570W\Scott Suhy

CPU(s)

cacheSize	coreId	cores	cpu	family	flags	mhz	model	modelName	physicalId	stepping	vendorId
0		8	0	0		2401		Intel(R) Core(TM) i7-3630QM CPU...	BFEBFBFF000306A9	0	GenuineIntel

Nameservers 10.18.0.7, 10.20.4.5, 192.168.1.57
Timestamp: Jul-20-16
Asset: Scott's HP
IPs: 10.20.1.39
Mac Addresses: d8:9d:67:d3:68:7b
Hostnames hp-8570w

Net Agent Modules [Show]

Products [Show]

Components (Raw) [Hide]

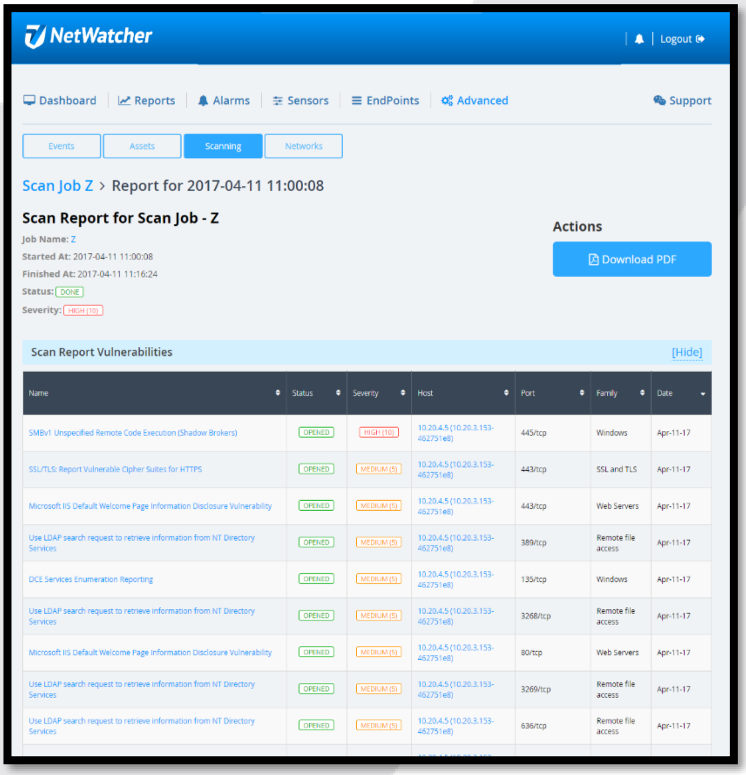
Component Name	Publisher	Product Name	Versions	Aliases	Install Locations	Uninstall Strings
1d110067402f36c9618445d156357504			1	1	0	0
SAFE {26A24AE4-039D-4CA4-87B4-2F83218073F0}			1	1	0	0
SAFE 7-Zip 16.02 (x64)	Igor Pavlov		1	1	0	1
SAFE {837b34e3-7c30-493c-8f6a-2b0f04e2912c}			1	1	0	0
SAFE AddressBook			1	1	0	0
Adobe Acrobat XI Pro	Adobe Systems	ADOBE ACROBAT PRO	1	1	1	1
Adobe AIR	Adobe Systems Incorporated	ADOBE AIR	1	1	1	1
Adobe Creative Cloud	Adobe Systems Incorporated	ADOBE CREATIVE CLOUD	1	1	0	1
Adobe Illustrator CC 2015.3	Adobe Systems Incorporated	ADOBE ILLUSTRATOR	1	1	1	1
SAFE Apple Application Support (32-bit)	Apple Inc.		1	1	1	1
SAFE Apple Application Support (64-bit)	Apple Inc.		1	1	1	1
SAFE Apple Mobile Device Support	Apple Inc.		1	1	1	1
Apple Software Update	Apple Inc.	APPLE SOFTWARE UPDATE	1	1	1	1
BingProvidedSearch			1	1	0	1
SAFE Bonjour	Apple Inc.		1	1	1	1
SAFE Cisco WebEx Meetings	Cisco WebEx LLC		1	1	0	1

Critical Security Control #3: Secure Configurations for Hardware and Software

Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.IP-1	A.14.2.4 A.14.2.8 A.18.2.3	3.4.1 - 3.4.3	2.2 2.3 6.2 11.5	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	

- Vulnerability Scans of your environment will identify when devices, operating systems, applications, etc. are configured with the vendor default password.
- File Integrity Monitoring alerts you to changes of critical system files including network device configurations, Windows registry entries, and any other text-based file that falls under your security policy. This Host-based Intrusion Detection can detect potentially exploitable faulty configurations by the way a service communicates.



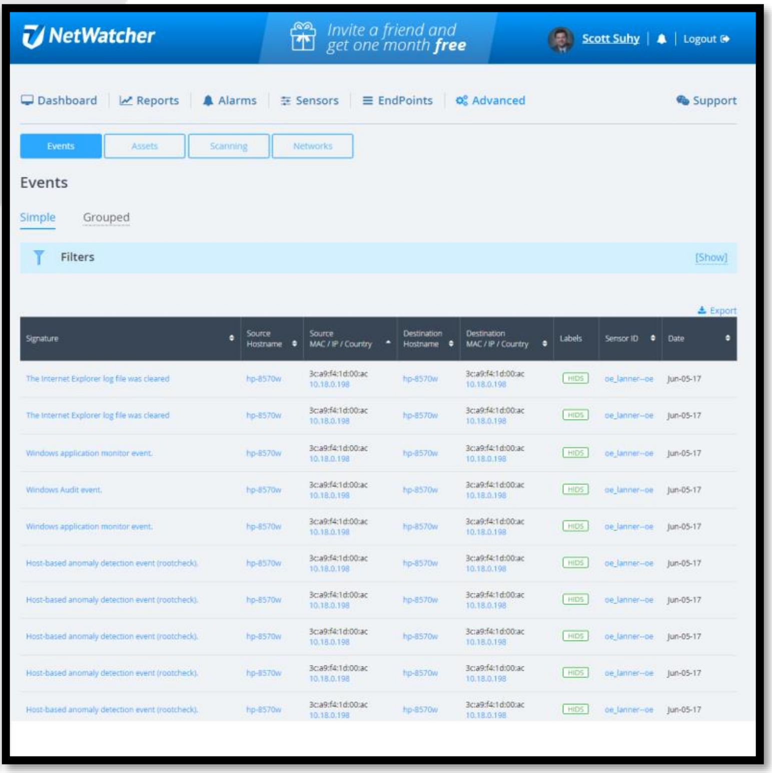
Scan Job Z > Report for 2017-04-11 11:00:08

Scan Report for Scan Job - Z

Job Name: Z
Started At: 2017-04-11 11:00:08
Finished At: 2017-04-11 11:16:24
Status: DONE
Severity: HIGH (10)

Scan Report Vulnerabilities

Name	Status	Severity	Host	Port	Family	Date
SMBv1 Unspecified Remote Code Execution (Shadow Brokers)	OPENED	HIGH (10)	10.20.4.5 (10.20.3.153-462751e8)	445/tcp	Windows	Apr-11-17
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	443/tcp	SSL and TLS	Apr-11-17
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	443/tcp	Web Servers	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	389/tcp	Remote file access	Apr-11-17
DCE Services Enumeration Reporting	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	135/tcp	Windows	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	3268/tcp	Remote file access	Apr-11-17
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	80/tcp	Web Servers	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	3269/tcp	Remote file access	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	636/tcp	Remote file access	Apr-11-17



Events

Signature	Source Hostname	Source MAC / IP / Country	Destination Hostname	Destination MAC / IP / Country	Labels	Sensor ID	Date
The Internet Explorer log file was cleared	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
The Internet Explorer log file was cleared	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Windows application monitor event.	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Windows Audit event.	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Windows application monitor event.	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Host-based anomaly detection event (rootcheck).	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Host-based anomaly detection event (rootcheck).	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Host-based anomaly detection event (rootcheck).	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Host-based anomaly detection event (rootcheck).	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17
Host-based anomaly detection event (rootcheck).	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	hp-8570w	3c:a9:f4:1d:00:ac 10.18.0.198	HIDS	oe_lanner--oe	Jun-05-17

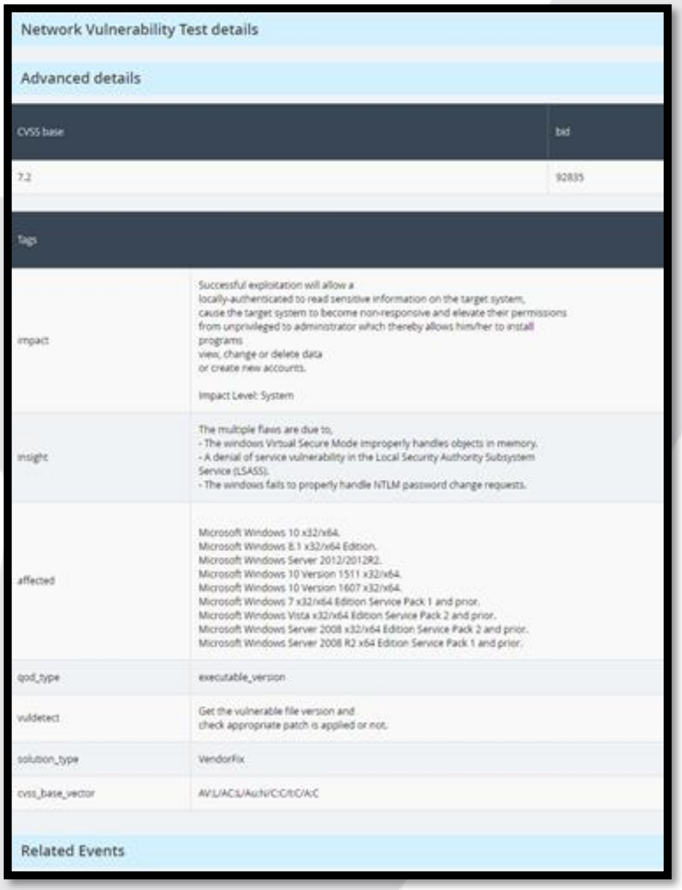
Critical Security Control #4: Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and act on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	A.12.6.1 A.14.2.8	3.11.2 3.11.3 3.12.2 3.14.1	6.1 6.2 11.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	Section 500.05

NetWatcher provides integrated vulnerability scanning, assessment, and reporting that quickly identifies misconfigurations and missing updates that could leave you susceptible to attack. With NetWatcher, you can:

- Schedule scans to run on a recurring basis with the ability to scan some assets more frequently than others
- Scan assets from authenticated and unauthenticated perspectives



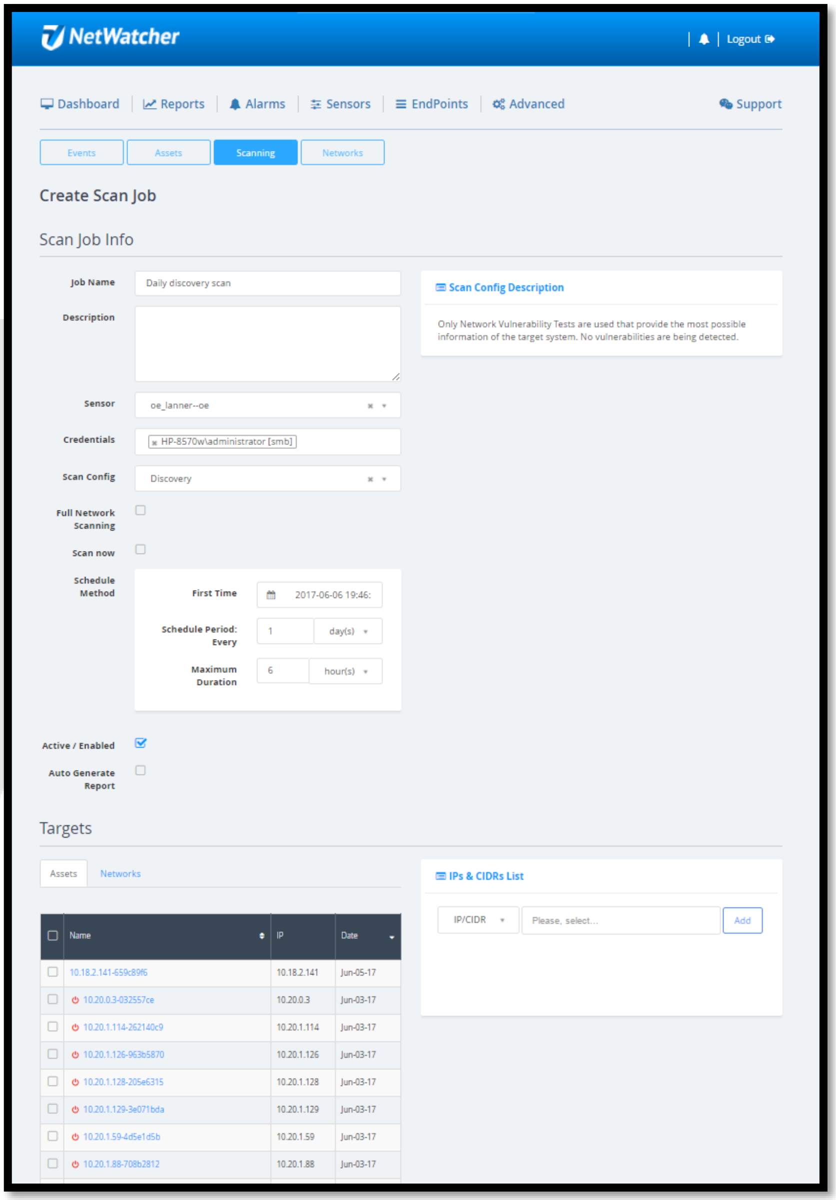
Network Vulnerability Test details

Advanced details

CVSS base	bid
7.2	92835

Tags	
impact	Successful exploitation will allow a locally-authenticated to read sensitive information on the target system, cause the target system to become non-responsive and elevate their permissions from unprivileged to administrator which thereby allows him/her to install programs view, change or delete data or create new accounts. Impact Level: System
insight	The multiple flaws are due to, - The windows Virtual Secure Mode improperly handles objects in memory. - A denial of service vulnerability in the Local Security Authority Subsystem Service (LSASS). - The windows fails to properly handle NTLM password change requests.
affected	Microsoft Windows 10 x32/x64. Microsoft Windows 8.1 x32/x64 Edition. Microsoft Windows Server 2012/2012R2. Microsoft Windows 10 Version 1511 x32/x64. Microsoft Windows 10 Version 1607 x32/x64. Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior. Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior. Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior. Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior.
qod_type	executable_version
vuldetect	Get the vulnerable file version and check appropriate patch is applied or not.
solution_type	VendorFix
cvss_base_vector	AV:L/AC:L/Au:N/C:C/I:C/A:C

Related Events



Create Scan Job

Scan Job Info

Job Name: Daily discovery scan

Description:

Sensor: oe_lanner--oe

Credentials: HP-8570w\administrator [smb]

Scan Config: Discovery

Full Network Scanning: □

Scan now: □

Schedule Method:
First Time: 2017-06-06 19:46:
Schedule Period: Every 1 day(s)
Maximum Duration 6 hour(s)

Active / Enabled: ☑

Auto Generate Report: □

Scan Config Description

Only Network Vulnerability Tests are used that provide the most possible information of the target system. No vulnerabilities are being detected.

Targets

□	Name	IP	Date
□	10.18.2.141-659c89f6	10.18.2.141	Jun-05-17
□	10.20.0.3-032557ce	10.20.0.3	Jun-03-17
□	10.20.1.114-262140c9	10.20.1.114	Jun-03-17
□	10.20.1.126-963b5870	10.20.1.126	Jun-03-17
□	10.20.1.128-205e6315	10.20.1.128	Jun-03-17
□	10.20.1.129-3e071bda	10.20.1.129	Jun-03-17
□	10.20.1.59-4d5e1d5b	10.20.1.59	Jun-03-17
□	10.20.1.88-708b2812	10.20.1.88	Jun-03-17

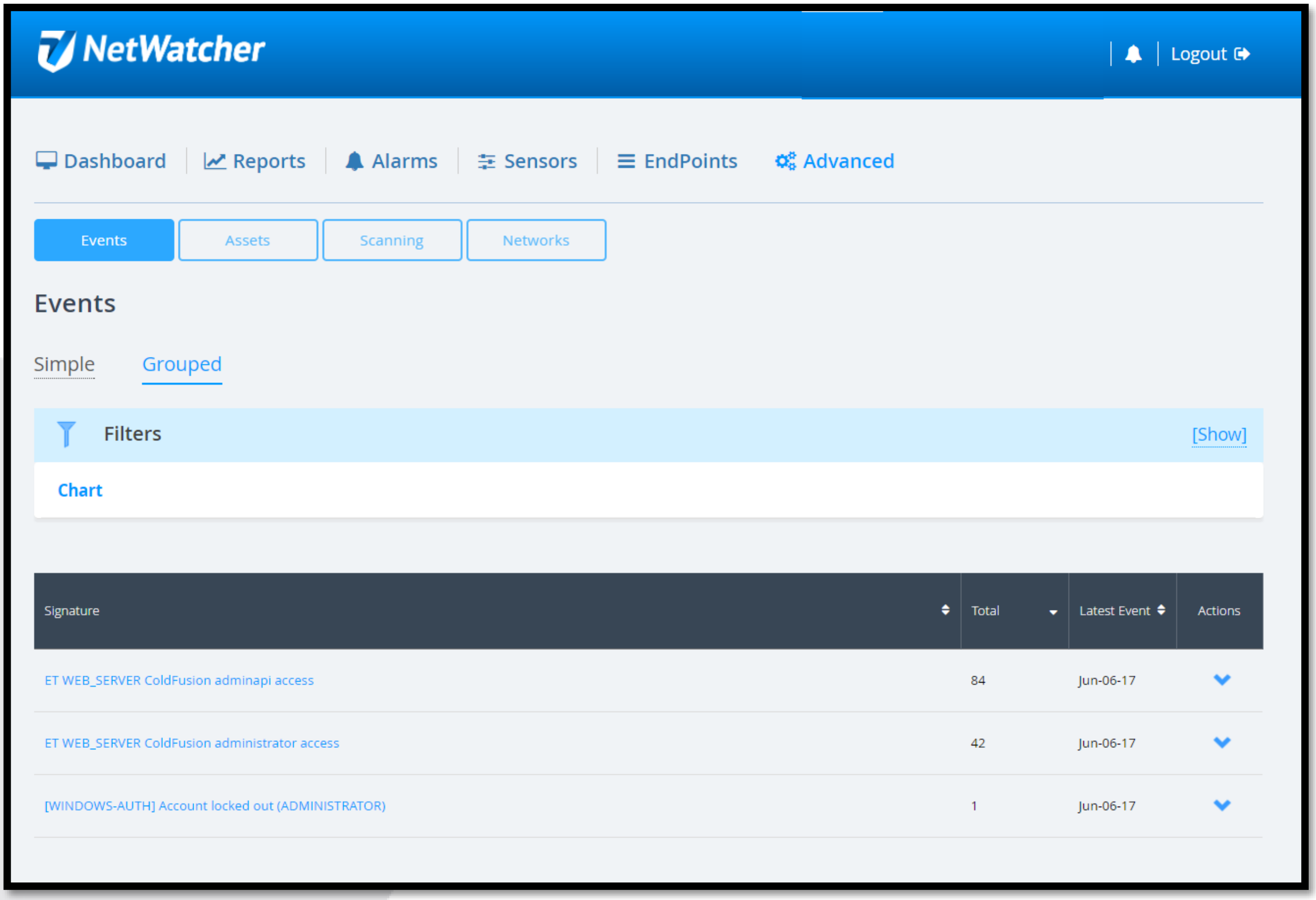
IPs & CIDRs List

Critical Security Control #5: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	3.1.5 - 3.1.7 3.4.5 - 3.4.6 3.7.1 - 3.7.2 3.7.5 - 3.7.6 3.13.3	2.1 7.1 - 7.3 8.1 - 8.3 8.7	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	Section 500.12

NetWatcher is not a Data Loss Prevention Service or Administrative management service but does detect issues and use of Administrative accounts.



Signature	Total	Latest Event	Actions
ET WEB_SERVER ColdFusion adminapi access	84	Jun-06-17	
ET WEB_SERVER ColdFusion administrator access	42	Jun-06-17	
[WINDOWS-AUTH] Account locked out (ADMINISTRATOR)	1	Jun-06-17	

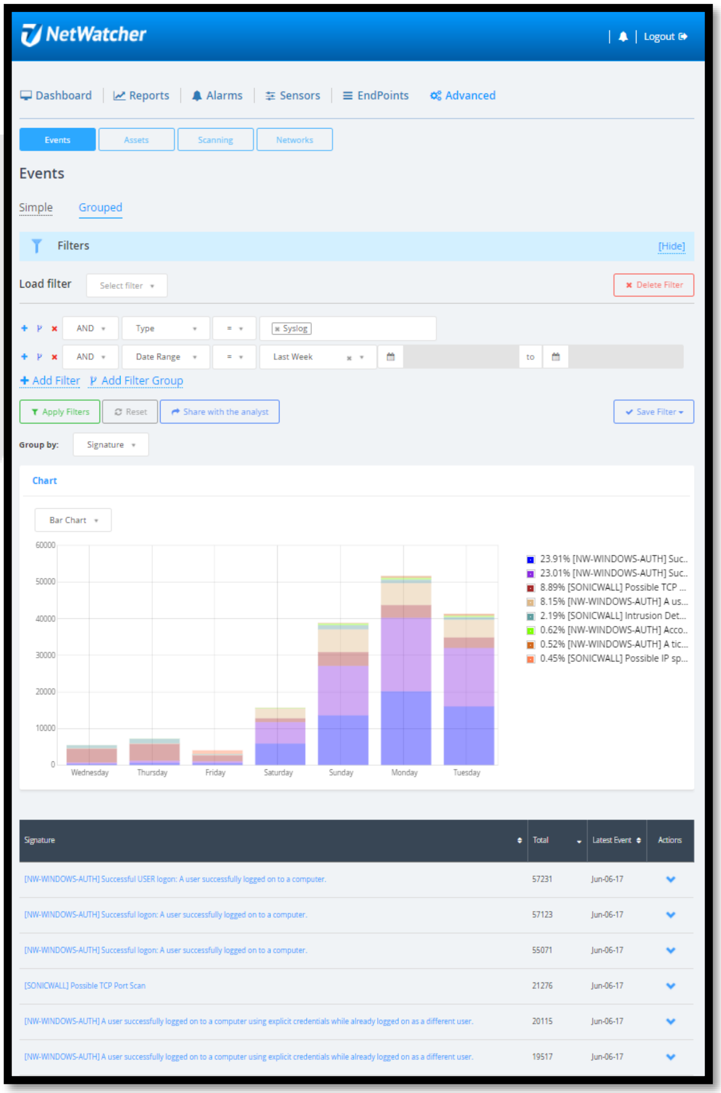
Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

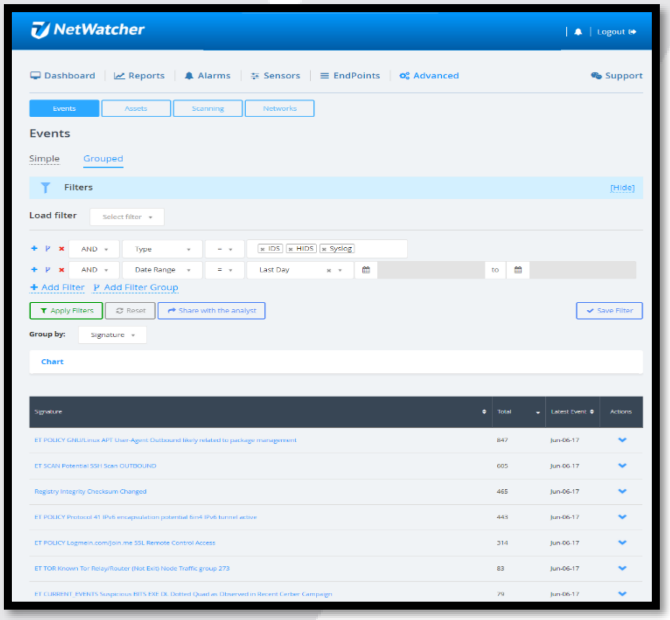
NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.PT-1 DE.AE-3 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5	A.12.4.1 - A.12.4.4 A.12.7.1	3.3.1 - 3.3.9 3.14.7	10.1 - 10.9	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	Domain 2: Threat Intelligence & Collaboration - Monitoring and Analyzing Domain 3: Cybersecurity Controls - Detective Controls	Section 500.06

NetWatcher allows you to easily correlate raw logs and pull out important indicators of compromise for audit purposes from both device logs (such as firewalls) and endpoint / server logs (via the NetAgent).

Single-purpose SIEM software or log management tools provide valuable information, but often require expensive integration efforts to bring in log files from disparate sources such as asset management, vulnerability assessment, and IDS products. With NetWatcher, SIEM is built-in with other essential security tools for complete security visibility that simplifies and accelerates threat detection, incident response, and compliance management.



Signature	Total	Latest Event	Actions
[NW-WINDOWS-AUTH] Successful USER logon: A user successfully logged on to a computer.	57231	Jun-06-17	
[NW-WINDOWS-AUTH] Successful logon: A user successfully logged on to a computer.	57123	Jun-06-17	
[NW-WINDOWS-AUTH] Successful logon: A user successfully logged on to a computer.	55071	Jun-06-17	
[SONICWALL] Possible TCP Port Scan	21276	Jun-06-17	
[NW-WINDOWS-AUTH] A user successfully logged on to a computer using explicit credentials while already logged on as a different user.	20115	Jun-06-17	
[NW-WINDOWS-AUTH] A user successfully logged on to a computer using explicit credentials while already logged on as a different user.	19517	Jun-06-17	



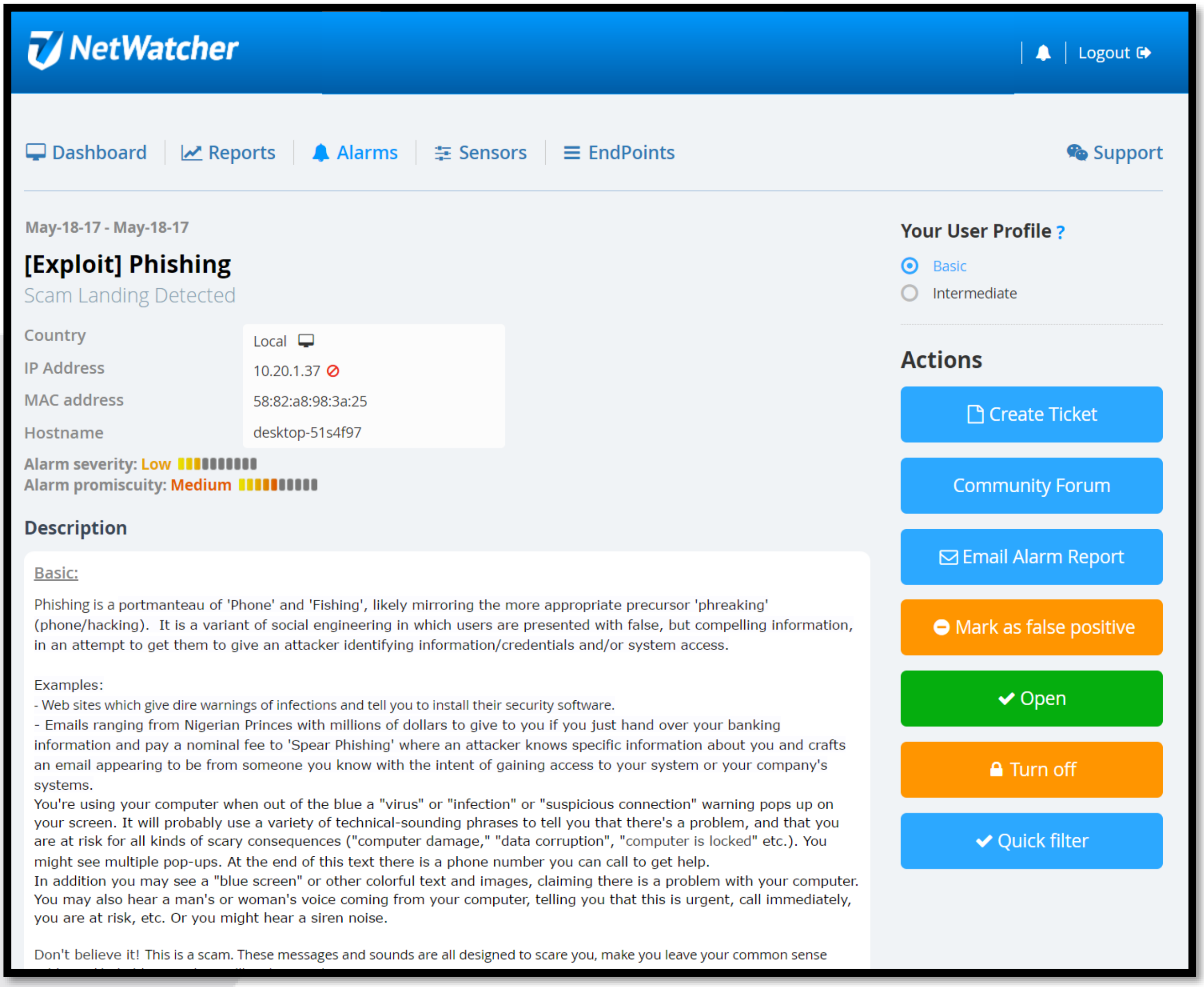
Signature	Total	Latest Event	Actions
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	847	Jun-06-17	
ET SCAN Potential SSH Scan OUTBOUND	605	Jun-06-17	
Registry Integrity Checksum Changed	465	Jun-06-17	
ET POLICY Protocol 41 IPv6 encapsulation potential 6in4 IPv6 tunnel active	443	Jun-06-17	
ET POLICY Logmein.com/Join.me SSL Remote Control Access	314	Jun-06-17	
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 273	83	Jun-06-17	
ET CURRENT_EVENTS Suspicious BITS EXE DL Dotted Quad as Observed in Recent Cerber Campaign	79	Jun-06-17	

Critical Security Control #7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.IP-1	A.14.2.4 A.14.2.8 A.18.2.3		2.2 2.3 6.2 11.5	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	

NetWatcher is not a secure DNS or an email security service however it is particularly well-equipped to help you improve the security by noticing when end users go to websites or click on links that make the organization vulnerable.



May-18-17 - May-18-17

[Exploit] Phishing

Scam Landing Detected

Country	Local
IP Address	10.20.1.37
MAC address	58:82:a8:98:3a:25
Hostname	desktop-51s4f97

Alarm severity: Low

Alarm promiscuity: Medium

Description

Basic:

Phishing is a portmanteau of 'Phone' and 'Fishing', likely mirroring the more appropriate precursor 'phreaking' (phone/hacking). It is a variant of social engineering in which users are presented with false, but compelling information, in an attempt to get them to give an attacker identifying information/credentials and/or system access.

Examples:
- Web sites which give dire warnings of infections and tell you to install their security software.
- Emails ranging from Nigerian Princes with millions of dollars to give to you if you just hand over your banking information and pay a nominal fee to 'Spear Phishing' where an attacker knows specific information about you and crafts an email appearing to be from someone you know with the intent of gaining access to your system or your company's systems.

You're using your computer when out of the blue a "virus" or "infection" or "suspicious connection" warning pops up on your screen. It will probably use a variety of technical-sounding phrases to tell you that there's a problem, and that you are at risk for all kinds of scary consequences ("computer damage," "data corruption", "computer is locked" etc.). You might see multiple pop-ups. At the end of this text there is a phone number you can call to get help.
In addition you may see a "blue screen" or other colorful text and images, claiming there is a problem with your computer. You may also hear a man's or woman's voice coming from your computer, telling you that this is urgent, call immediately, you are at risk, etc. Or you might hear a siren noise.

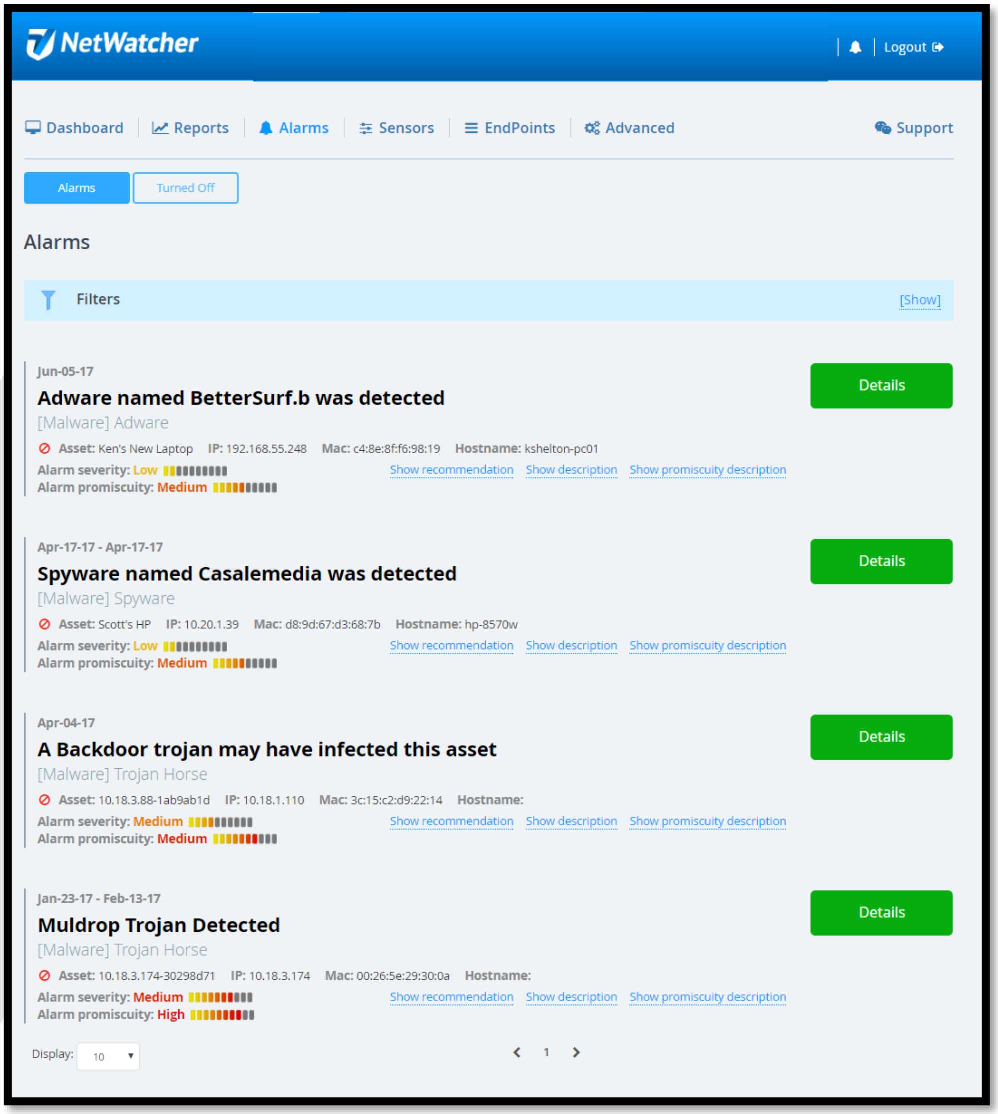
Don't believe it! This is a scam. These messages and sounds are all designed to scare you, make you leave your common sense

Critical Security Control #8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.PT-2 DE.CM-4 DE.CM-5	A.8.3.1 A.12.2.1 A.13.2.3	3.7.4 3.14.2 - 3.14.6	5.1 - 5.4	164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.310(d)(1): Device and Media Controls - Accountability A 164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 2: Threat Intelligence & Collaboration - Monitoring and Analyzing Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	

NetWatcher comes with built-in Network IDS (NIDS) to spot the delivery of malicious software; certain attack patterns, as well as other types of suspicious traffic. You can deploy NIDS detection points throughout your environment to get better visibility into the potentially dangerous traffic on your network. An added benefit of using the IDS capability found in NetWatcher is the continuous updates to the IDS signatures, or attributes of data packet known to be indicative of malicious behavior.



Jun-05-17
Adware named BetterSurf.b was detected
[Malware] Adware
Asset: Ken's New Laptop **IP:** 192.168.55.248 **Mac:** c4:8e:8f:f6:98:19 **Hostname:** kshelton-pc01
Alarm severity: Low
Alarm promiscuity: Medium
Show recommendation Show description Show promiscuity description

Apr-17-17 - Apr-17-17
Spyware named Casalemedia was detected
[Malware] Spyware
Asset: Scott's HP **IP:** 10.20.1.39 **Mac:** d8:9d:67:d3:68:7b **Hostname:** hp-8570w
Alarm severity: Low
Alarm promiscuity: Medium
Show recommendation Show description Show promiscuity description

Apr-04-17
A Backdoor trojan may have infected this asset
[Malware] Trojan Horse
Asset: 10.18.3.88-1ab9ab1d **IP:** 10.18.1.110 **Mac:** 3c:15:c2:d9:22:14 **Hostname:**
Alarm severity: Medium
Alarm promiscuity: Medium
Show recommendation Show description Show promiscuity description

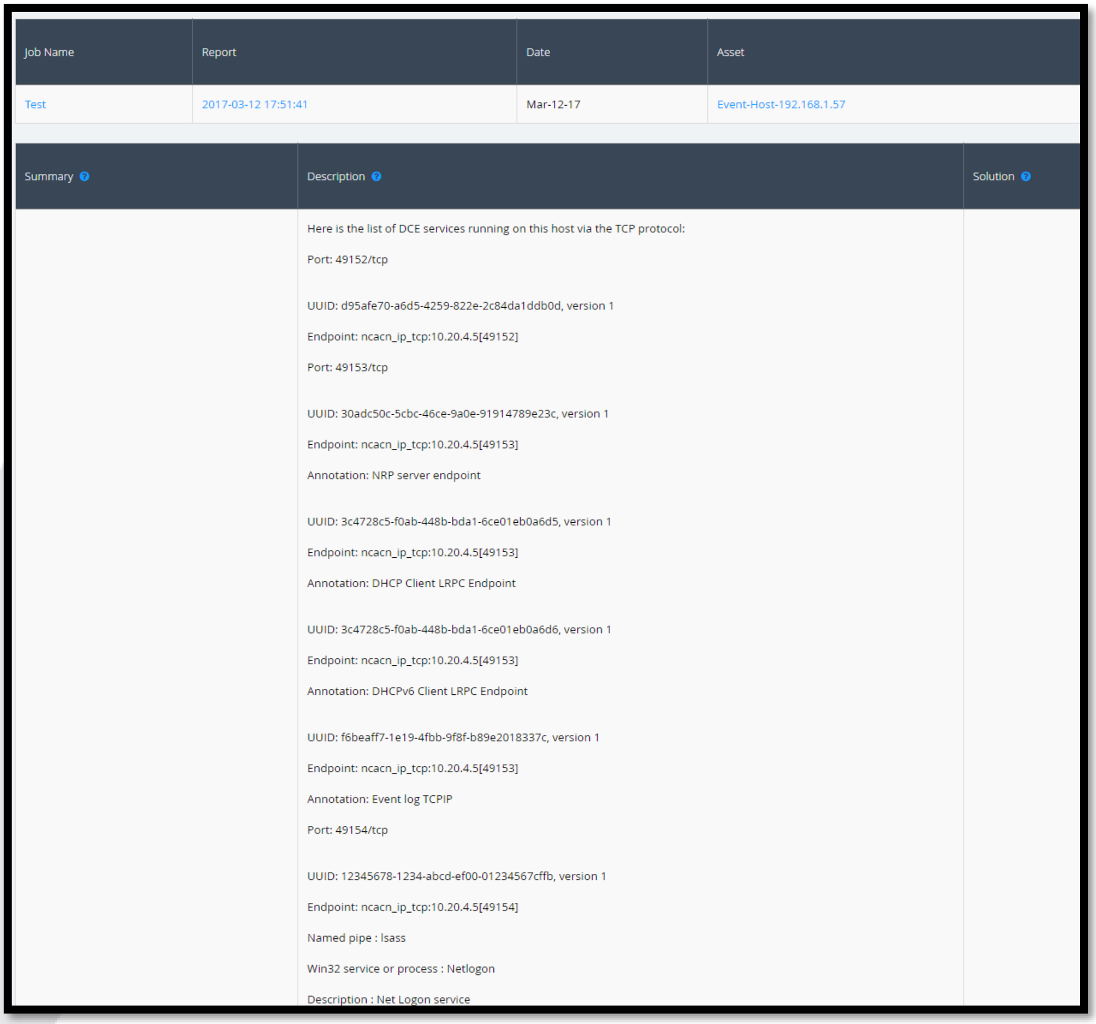
Jan-23-17 - Feb-13-17
Muldrop Trojan Detected
[Malware] Trojan Horse
Asset: 10.18.3.174-30298d71 **IP:** 10.18.3.174 **Mac:** 00:26:5e:29:30:0a **Hostname:**
Alarm severity: Medium
Alarm promiscuity: High
Show recommendation Show description Show promiscuity description

Critical Security Control #9: Limitation and Control of Network Ports

Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices to minimize windows of vulnerability available to attackers.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.AC-5 DE.AE-1	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	3.4.7	1.4	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	

NetWatcher can ingest LOG/HIDS data from endpoint servers, laptops and desktops as well as SYSLOG data from devices such as firewalls. The sensor ingests the data, parses the data, and then feed that into its correlation engine to determine if an event is necessary. It looks for specific entries in logs that will highlight unauthorized and/or potentially malicious traffic in real-time. To help identify problems in advance, though, NetWatcher includes built-in asset discovery that includes scanning for available ports and services. This will give you a better idea of what exactly is exposed to the outside and let you evaluate the business need. You can also leverage the scheduling functionality to run these asset scans regularly without manual intervention.



Job Name	Report	Date	Asset
Test	2017-03-12 17:51:41	Mar-12-17	Event-Host-192.168.1.57

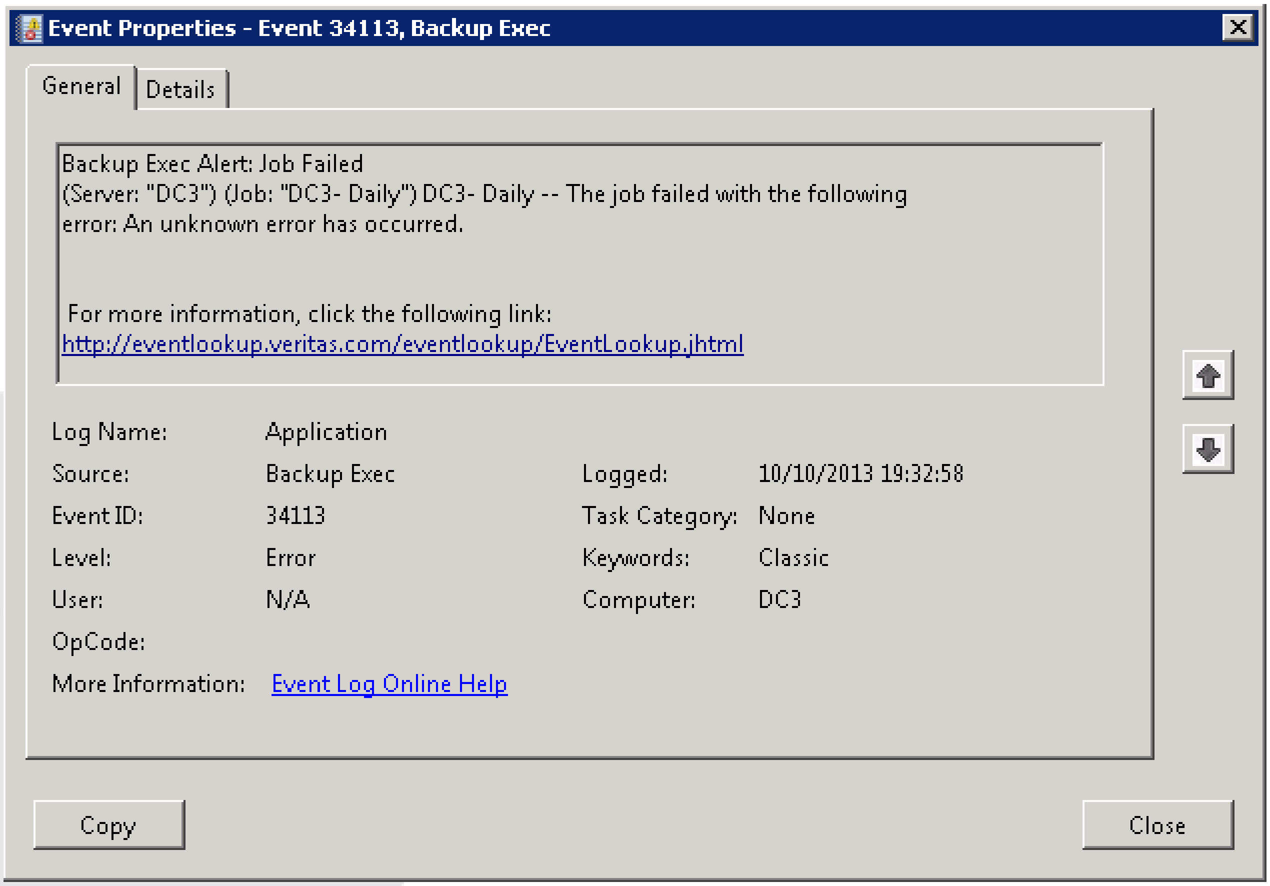
Summary	Description	Solution
	Here is the list of DCE services running on this host via the TCP protocol: Port: 49152/tcp UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:10.20.4.5[49152] Port: 49153/tcp UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.20.4.5[49153] Annotation: NRP server endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.20.4.5[49153] Annotation: DHCP Client LRPC Endpoint UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:10.20.4.5[49153] Annotation: DHCPv6 Client LRPC Endpoint UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:10.20.4.5[49153] Annotation: Event log TCPIP Port: 49154/tcp UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:10.20.4.5[49154] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service	

Critical Security Control #10: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.IP-4	A.10.1.1 A.12.3.1	3.8.9	4.3 9.5 - 9.7	164.308(a)(7): Contingency Plan - Data Backup Plan R 164.308(a)(7): Contingency Plan - Disaster Recovery Plan R 164.308(a)(7): Contingency Plan - Testing and Revision Procedure A 164.310(d)(1): Device and Media Controls - Data Backup and Storage A	Domain 3: Cybersecurity Controls - Preventative Controls	

Since backup solutions log the status of failed and successful jobs as well as the status of regular maintenance checks, NetWatcher can be customized to alert you to issues with the backup/restore process.



Backup Exec Alert: Job Failed
(Server: "DC3") (Job: "DC3- Daily") DC3- Daily -- The job failed with the following error: An unknown error has occurred.

For more information, click the following link:
http://eventlookup.veritas.com/eventlookup/EventLookup.jhtml

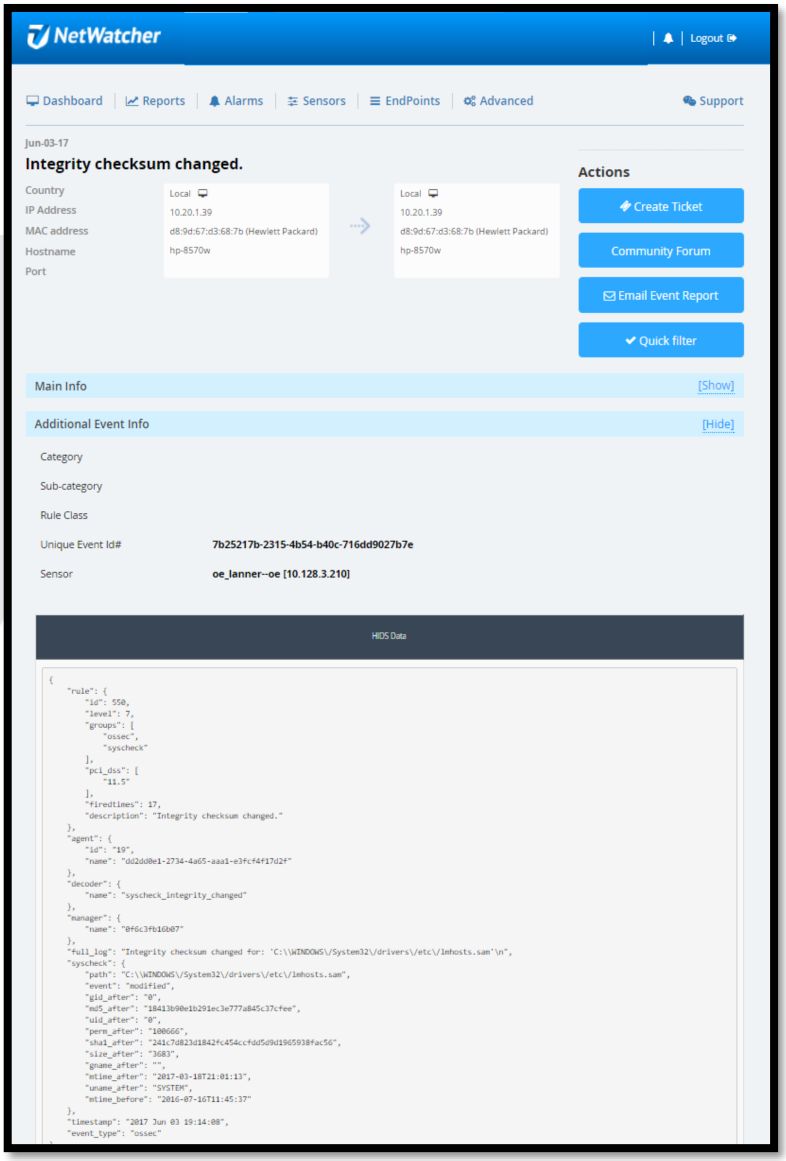
Log Name: Application
Source: Backup Exec
Logged: 10/10/2013 19:32:58
Event ID: 34113
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: DC3
OpCode:
More Information: Event Log Online Help

Critical Security Control #11: Secure Configurations for Network Devices

Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.AC-5 PR.IP-1 PR.PT-4	A.9.1.2 A.13.1.1 A.13.1.3	3.4.1 - 3.4.3 3.7.5 - 3.7.6	1.1 - 1.2 2.2 6.2		Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	Section 500.12

The host-based IDS (HIDS) functionality integrated within NetWatcher's Netagent allows you to monitor files for changes, including the configuration files found on desktops and servers. In some cases, this could alert you of the initial steps of an in-progress attack and give you precious time needed to remediate any issues before they wreak complete havoc.



Jun-03-17

Integrity checksum changed.

Country	Local	Local
IP Address	10.20.1.39	10.20.1.39
MAC address	d8:9d:67:d3:68:7b (Hewlett Packard)	d8:9d:67:d3:68:7b (Hewlett Packard)
Hostname	hp-8570w	hp-8570w
Port		

Category	
Sub-category	
Rule Class	
Unique Event Id#	7b25217b-2315-4b54-b40c-716dd9027b7e
Sensor	oe_lanner--oe [10.128.3.210]

```
{
    "rule": {
        "id": 550,
        "level": 7,
        "groups": [
            "ossec",
            "syscheck"
        ],
        "pci_dss": [
            "11.5"
        ],
        "firedtimes": 17,
        "description": "Integrity checksum changed."
    },
    "agent": {
        "id": "19",
        "name": "dd2dd0e1-2734-4a65-aaa1-e3fcf4f17d2f"
    },
    "decoder": {
        "name": "syscheck_integrity_changed"
    },
    "manager": {
        "name": "0f6c3fb16b07"
    },
    "full_log": "Integrity checksum changed for: 'C:\\WINDOWS\/System32\/drivers\/etc\/lmhosts.sam'\n",
    "syscheck": {
        "path": "C:\\WINDOWS\/System32\/drivers\/etc\/lmhosts.sam",
        "event": "modified",
        "gid_after": "0",
        "md5_after": "18413b90e1b291ec3e777a845c37cfee",
        "uid_after": "0",
        "perm_after": "100666",
        "sha1_after": "241c7d823d1842fc454ccfdd5d9d1965938fac56",
        "size_after": "3683",
        "gname_after": "",
        "mtime_after": "2017-03-18T21:01:13",
        "uname_after": "SYSTEM",
        "mtime_before": "2016-07-16T11:45:37"
    },
    "timestamp": "2017 Jun 03 19:14:08",
    "event_type": "ossec"
```

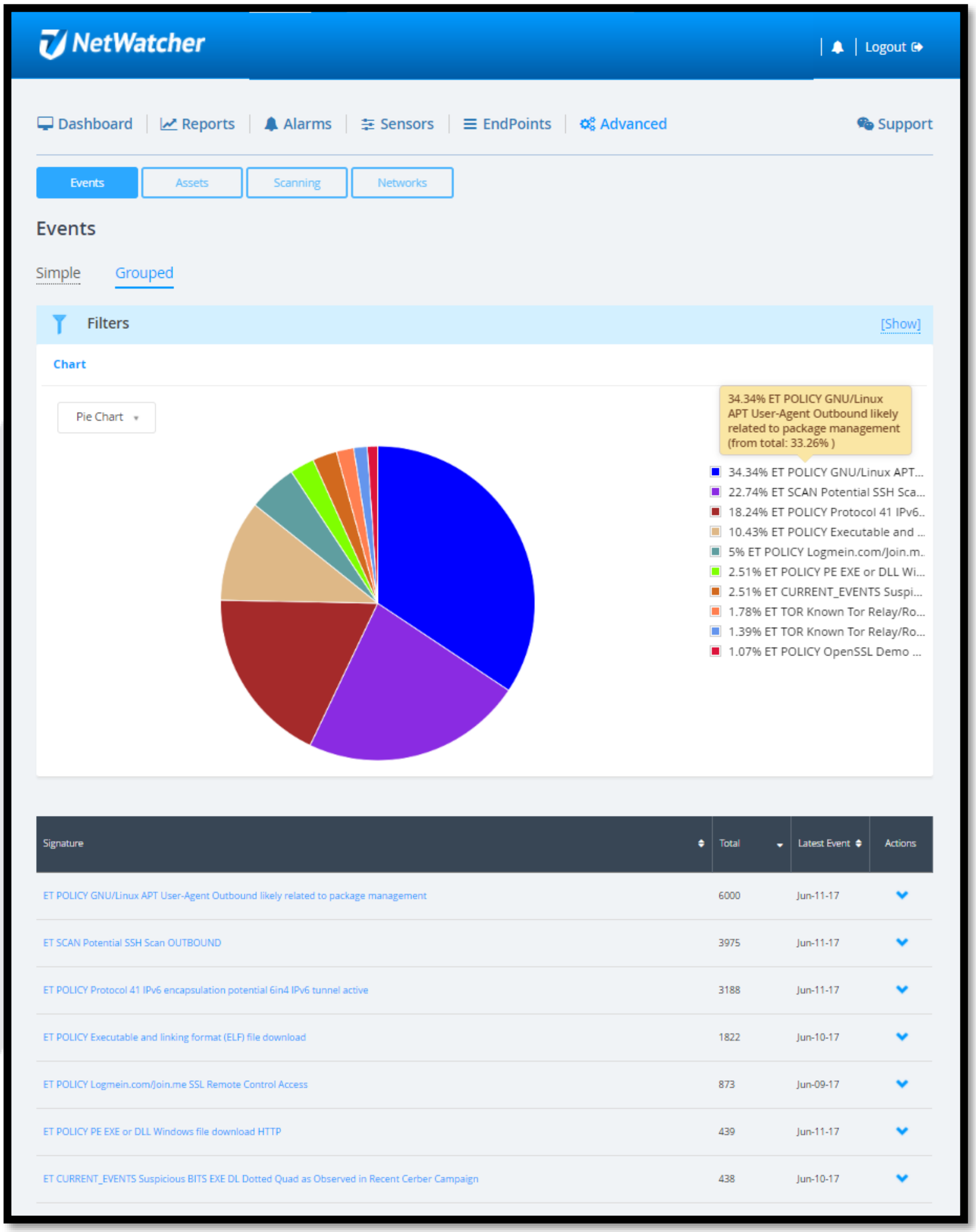
Critical Security Control #12: Boundary Defense

Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security- damaging data.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	A.9.1.2 A.12.4.1 A.12.7.1 A.13.1.1 A.13.1.3 A.13.2.3	3.1.3 3.1.12 - 3.1.15 3.1.18 3.1.20 - 3.1.22 3.13.1 3.13.6 - 3.13.8 3.13.12 - 3.13.13 3.13.15	1.1 - 1.3 8.3 10.9 11.4		Domain 2: Threat Intelligence & Collaboration - Monitoring and Analyzing Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	Section 500.11 Section 500.12

NetWatcher's IDS functionality is second to none, offering built-in network and host-based IDS. These capabilities, bolstered with integrated threat intelligence that ensure you are made aware of any activity related to the most recent threats.

You can build complex queries and set tripwires and get notified via SMS or Email if a queries trips in the future.



Events

Simple Grouped

Filters [Show]

Chart

Pie Chart

34.34% ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management (from total: 33.26%)

- 🟦 34.34% ET POLICY GNU/Linux APT...
- 🟪 22.74% ET SCAN Potential SSH Sca...
- 🟥 18.24% ET POLICY Protocol 41 IPv6..
- 🟫 10.43% ET POLICY Executable and ...
- 🟦 5% ET POLICY Logmein.com/Join.m..
- 🟩 2.51% ET POLICY PE EXE or DLL Wi...
- 🟧 2.51% ET CURRENT_EVENTS Suspi...
- 🟧 1.78% ET TOR Known Tor Relay/Ro...
- 🟦 1.39% ET TOR Known Tor Relay/Ro...
- 🟥 1.07% ET POLICY OpenSSL Demo ...

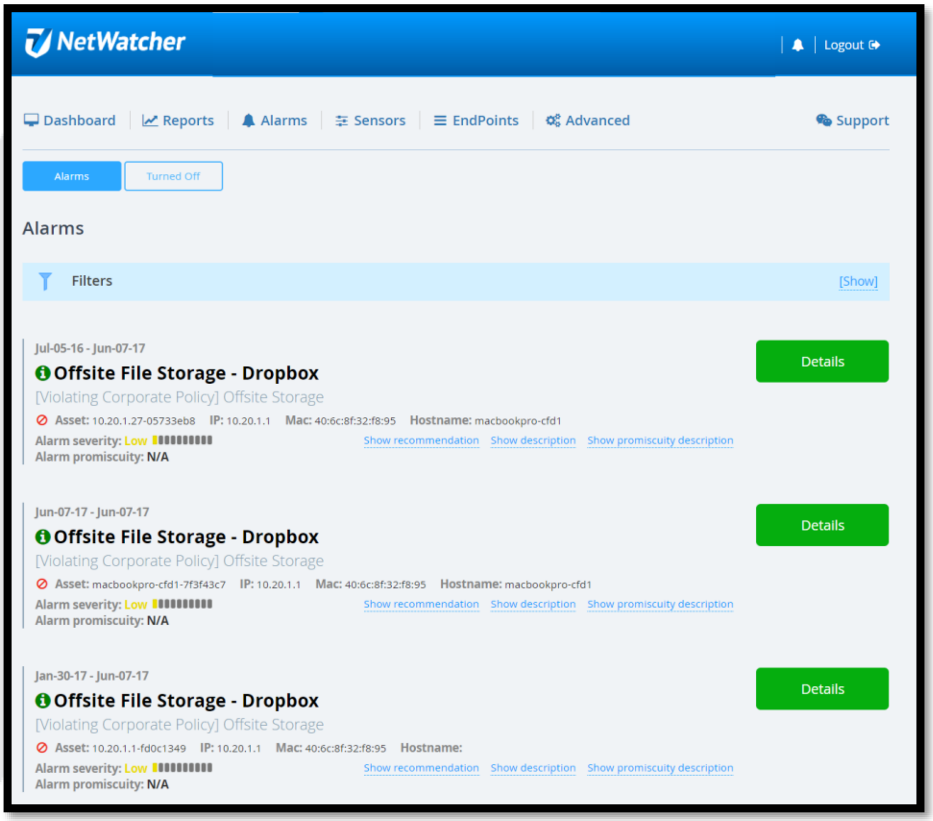
Signature	Total	Latest Event	Actions
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	6000	Jun-11-17	⌄
ET SCAN Potential SSH Scan OUTBOUND	3975	Jun-11-17	⌄
ET POLICY Protocol 41 IPv6 encapsulation potential 6in4 IPv6 tunnel active	3188	Jun-11-17	⌄
ET POLICY Executable and linking format (ELF) file download	1822	Jun-10-17	⌄
ET POLICY Logmein.com/Join.me SSL Remote Control Access	873	Jun-09-17	⌄
ET POLICY PE EXE or DLL Windows file download HTTP	439	Jun-11-17	⌄
ET CURRENT_EVENTS Suspicious BITS EXE DL Dotted Quad as Observed in Recent Cerber Campaign	438	Jun-10-17	⌄

Critical Security Control #13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2	A.8.3.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	3.1.19 3.1.21 3.8.7 - 3.8.8 3.13.16	3.6 4.1 - 4.3	164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R 164.310(d)(1): Device and Media Controls - Accountability A 164.312(a)(1): Access Control - Encryption and Decryption A 164.312(e)(1): Transmission Security - Integrity Controls A	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	Section 500.15

NetWatcher gives you visibility into data leaving your network, either accidentally or intentionally by keeping a close watch on the traffic patterns via the integrated IDS and the correlation of collected data. This can identify attackers leveraging FTP or even web-based services like Dropbox to steal information.



Alarms

Jul-05-16 - Jun-07-17
Offsite File Storage - Dropbox
[Violating Corporate Policy] Offsite Storage
Asset: 10.20.1.27-05733eb8 IP: 10.20.1.1 Mac: 40:6c:8f:32:f8:95 Hostname: macbookpro-cfd1
Alarm severity: Low
Alarm promiscuity: N/A
Show recommendation Show description Show promiscuity description

Jun-07-17 - Jun-07-17
Offsite File Storage - Dropbox
[Violating Corporate Policy] Offsite Storage
Asset: macbookpro-cfd1-7f3f43c7 IP: 10.20.1.1 Mac: 40:6c:8f:32:f8:95 Hostname: macbookpro-cfd1
Alarm severity: Low
Alarm promiscuity: N/A
Show recommendation Show description Show promiscuity description

Jan-30-17 - Jun-07-17
Offsite File Storage - Dropbox
[Violating Corporate Policy] Offsite Storage
Asset: 10.20.1.1-fd0c1349 IP: 10.20.1.1 Mac: 40:6c:8f:32:f8:95 Hostname:
Alarm severity: Low
Alarm promiscuity: N/A
Show recommendation Show description Show promiscuity description

14, 15 and 16 are important but, at the moment, NetWatcher's support for these items does not rise to the top hence we are leaving them out until we have further support.

Critical Security Control #14: Controlled Access Based on the Need to Know

The processes and tools used to track, control, prevent, and correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

The ability to analyze and correlate log data into events is one of NetWatcher's core capabilities, and gives you a deeper level of insight into who and what is using elevated access to traverse the network. Using NetWatcher's built-in IDS and log parsing functionality, users can identify when specific accounts are being used for specific systems (or on any system), and be alerted to it.

Critical Security Control #15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

NetWatcher provides the ability to ingest SYSLOGs from Wireless access points to aid in the security management of wireless access points.

Critical Security Control #16: Account Monitoring and Control

Actively manage the life-cycle of system and application accounts — their creation, use, dormancy, and deletion — to minimize opportunities for attackers to leverage them.

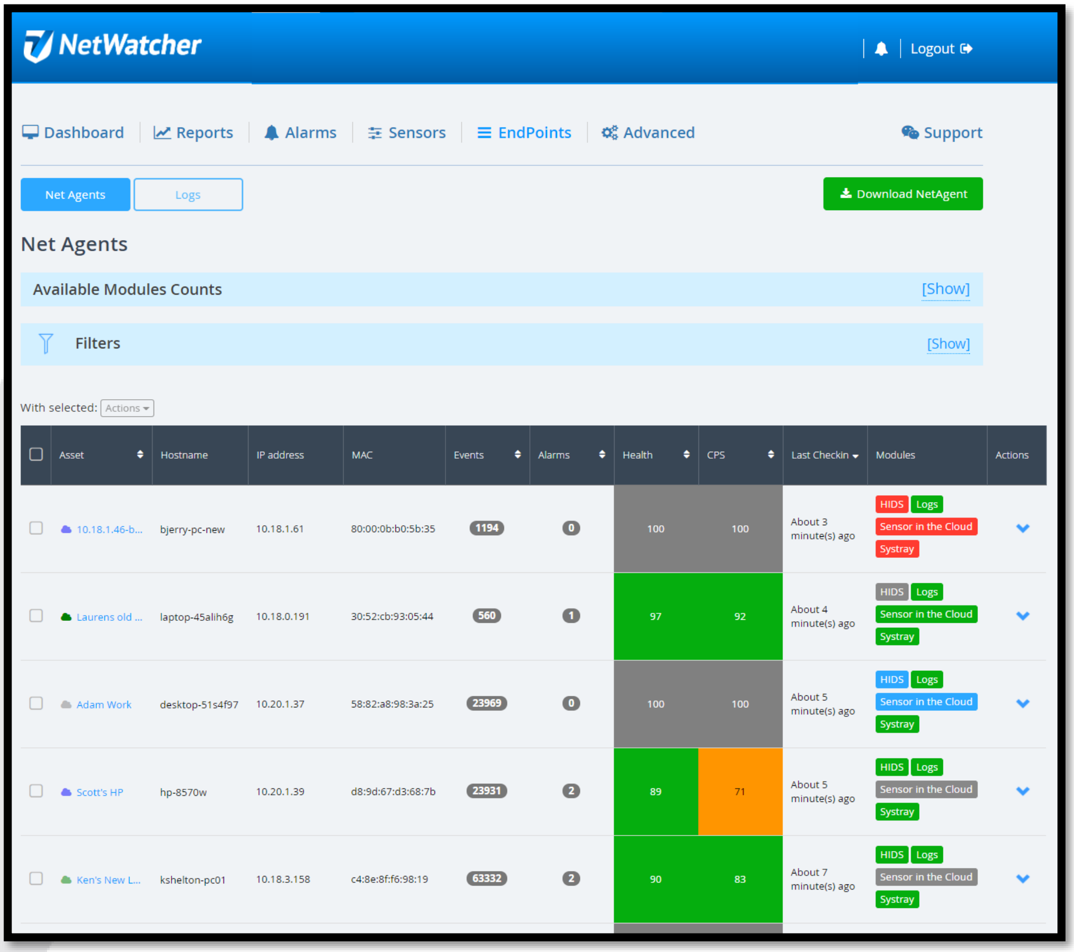
As mentioned in the CSC 15 section, NetWatcher can parse logs and Windows events to identify use of specific user accounts, allowing you to disable them before they are used for malicious purposes.

Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	A.7.2.2	3.2.2 - 3.2.3	12.6	164.308(a)(5): Security Awareness and Training - Security Reminders A 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	Domain 1: Cyber Risk Management & Oversight - Training and Culture Domain 3: Cybersecurity Controls - Preventative Controls	Section 500.10 Section 500.14

Each endpoint that runs the NetAgent gets both a Health Score and a Promiscuity Score providing an easy way to look out into your enterprise to determine who are the people that are most likely going to cause a breach to occur on the network. If you know your riskiest people you know who needs to go to cyber training and who's assets need to be more tightly controlled.



Net Agents

Available Modules Counts [Show]

Filters [Show]

With selected: Actions

□	Asset	Hostname	IP address	MAC	Events	Alarms	Health	CPS	Last Checkin	Modules	Actions
□	10.18.1.46-b...	bjerry-pc-new	10.18.1.61	80:00:0b:b0:5b:35	1194	0	100	100	About 3 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
□	Laurens old ...	laptop-45alih6g	10.18.0.191	30:52:cb:93:05:44	560	1	97	92	About 4 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
□	Adam Work	desktop-51s4f97	10.20.1.37	58:82:a8:98:3a:25	23969	0	100	100	About 5 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
□	Scott's HP	hp-8570w	10.20.1.39	d8:9d:67:d3:68:7b	23931	2	89	71	About 5 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	
□	Ken's New L...	kshelton-pc01	10.18.3.158	c4:8e:8f:f6:98:19	63332	2	90	83	About 7 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	

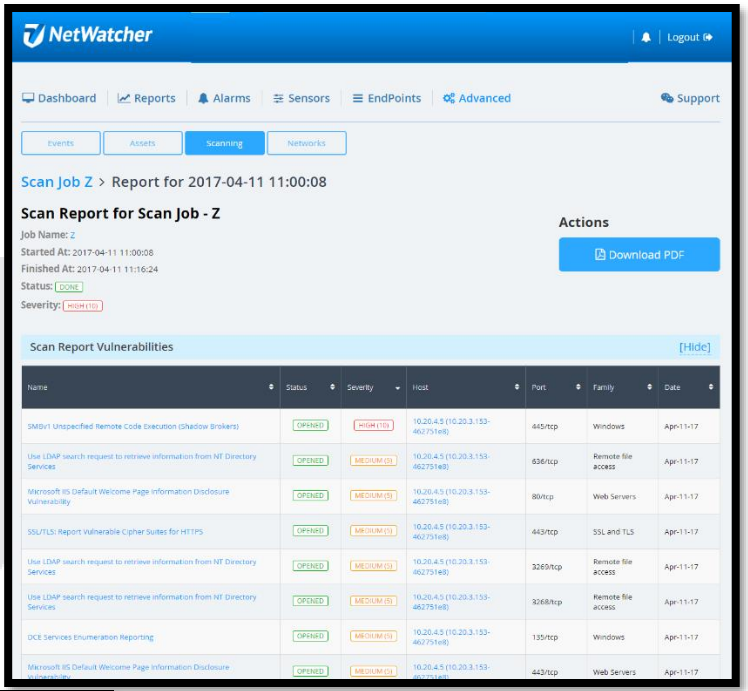
Critical Security Control #18: Application Software Security

Manage the security lifecycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.DS-7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8		6.3 6.5 - 6.7		Domain 3: Cybersecurity Controls - Preventative Controls	Section 500.08

NetWatcher comes with a built-in vulnerability assessment engine that is continuously updated with new threat intelligence. This capability allows you to identify unpatched or poorly misconfigured applications that will leave you open to attacks, even in recently developed applications or those with newly discovered exploits.

In addition, NetWatcher's built-in IDS functionality powered by integrated threat intelligence spots common web application exploits like SQL injection and Cross Site Scripting (XSS) attacks as they are happening. This allows you to stop the attack in progress and gives you time to remediate the issue and prevent future attacks.



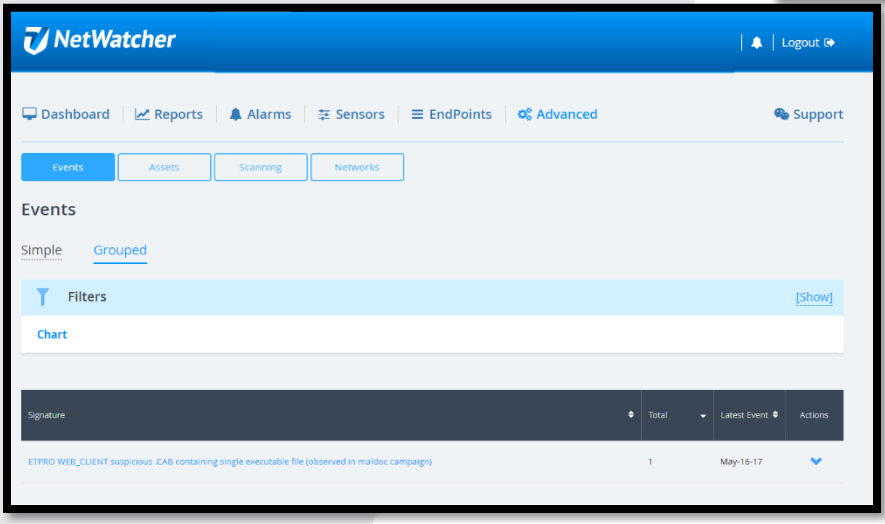
Scan Job Z > Report for 2017-04-11 11:00:08

Scan Report for Scan Job - Z

Job Name: Z
Started At: 2017-04-11 11:00:08
Finished At: 2017-04-11 11:16:24
Status: DONE
Severity: HIGH (10)

Scan Report Vulnerabilities

Name	Status	Severity	Host	Port	Family	Date
SMBv1 Unspecified Remote Code Execution (Shadow Brokers)	OPENED	HIGH (10)	10.20.4.5 (10.20.3.153-462751e8)	445/tcp	Windows	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	636/tcp	Remote file access	Apr-11-17
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	80/tcp	Web Servers	Apr-11-17
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	443/tcp	SSL and TLS	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	3269/tcp	Remote file access	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	3268/tcp	Remote file access	Apr-11-17
DCE Services Enumeration Reporting	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	135/tcp	Windows	Apr-11-17
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	443/tcp	Web Servers	Apr-11-17



Events

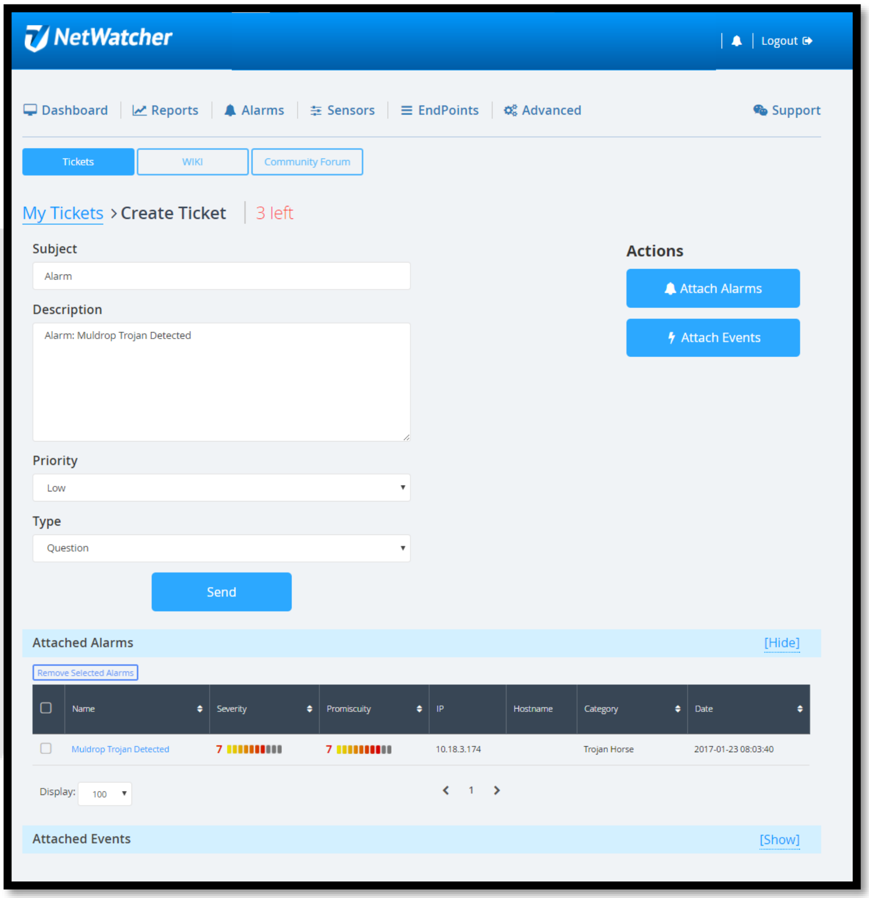
Signature	Total	Latest Event	Actions
ETPRO WEB_CLIENT suspicious .CAB containing single executable file (observed in maldoc campaign)	1	May-16-17	

Critical Security Control #19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure plan.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
PR.IP-10 DE.AE-2 DE.AE-4 DE.AE-5 DE.CM-1-7 RS.RP-1 RS.CO-1-5 RS.AN-1-4 RS.MI-1-2 RS.IM-1-2 RC.RP-1 RC.IM-1-2 RC.CO-1-3	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	3.6.1 - 3.6.3	12.10	164.308(a)(6): Security Incident Procedures - Response and Reporting R	Domain 5: Cyber Incident Management and Resilience - Incident Resilience Planning and Strategy Domain 5: Cyber Incident Management and Resilience - Detection, Response, and Mitigation Domain 5: Cyber Incident Management and Resilience - Escalation and Reporting	Section 500.16

The event correlation and integrated threat intelligence built into the NetWatcher platform minimizes the amount of time IT teams need to spend researching new threats. The single pane of glass management console presents the information they need to visualize all the relevant threat data, and each alarm contains detailed response guidance. In other words, the IT team can spend its time mitigating the threat rather than researching each alarm. While incident response and management deals with procedures outlined when a breach or security event occurs, NetWatcher becomes a tool that greatly accelerates an organization's ability to respond. It can also be used as a post-mortem tool for future refinement of IR/M policies. f you are an IT team with limited resources, you likely don't have time to mount an effective defense against cyber threats. You probably deploy a patchwork of security technologies that provide only some of the security capabilities you need, leaving gaps in your ability to detect and respond to malicious activity on your network. You also probably spend precious time manually trying to consolidate and analyze logs from a wide range of security point products, looking for indicators of compromise (IoC). Ultimately, you are unable to accurately answer questions like "Are we at risk from this new threat?" or "Are we compliant?"



My Tickets > Create Ticket | 3 left

Subject: Alarm

Description: Alarm: Muldrop Trojan Detected

Priority: Low

Type: Question

Attached Alarms

☐	Name	Severity	Promiscuity	IP	Hostname	Category	Date
☐	Muldrop Trojan Detected	7	7	10.18.3.174		Trojan Horse	2017-01-23 08:03:40

Display: 100

‹ 1 ›

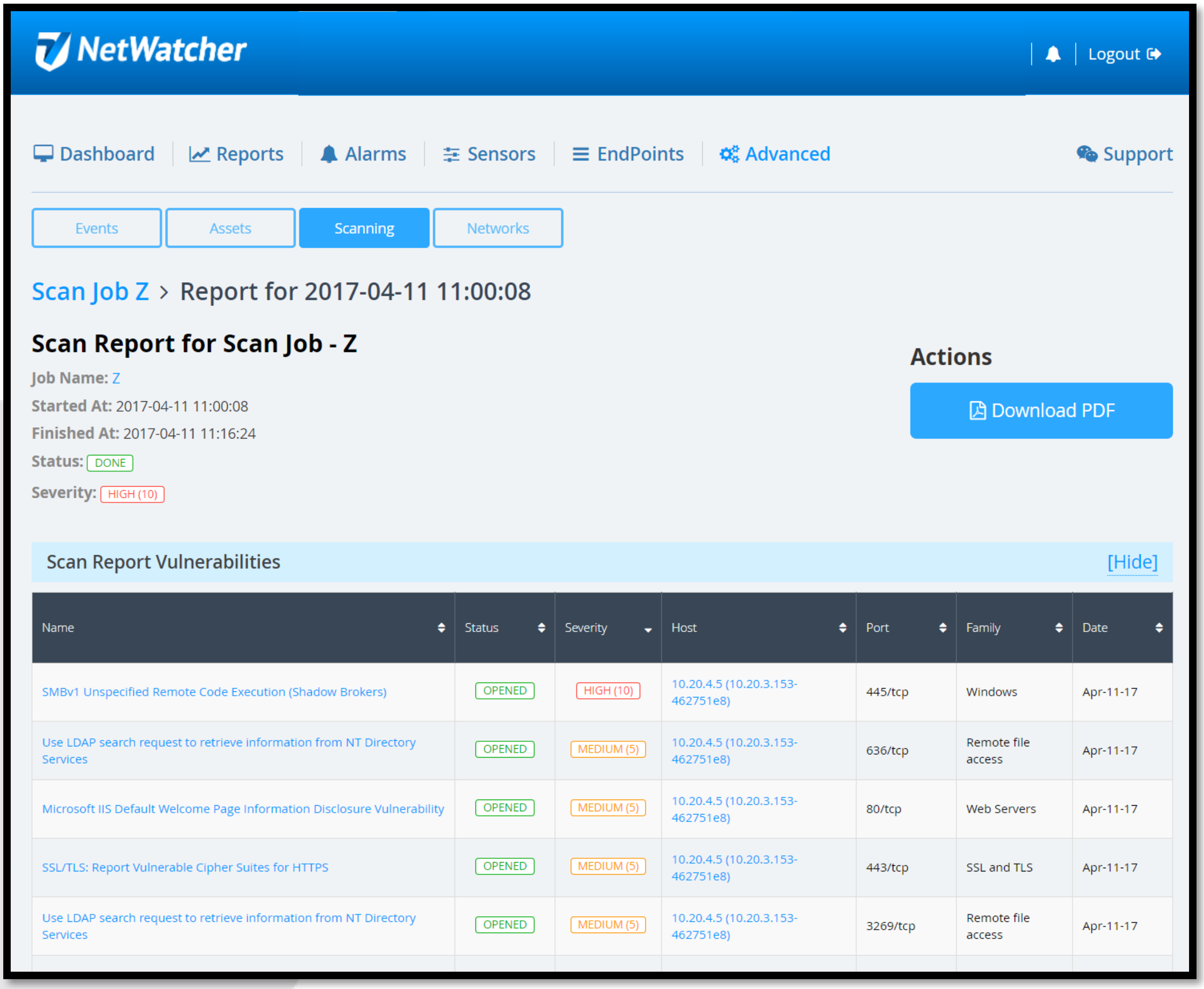
Attached Events

Critical Security Control #20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

NIST Cybersecurity Framework	ISO 27002:2013	NIST 800-171	PCI DSS 3.2	HIPAA	FFIEC Cybersecurity Assessment Tool	NY - NYCRR 500
	A.14.2.8 A.18.2.1 A.18.2.3		11.3		Domain 3: Cybersecurity Controls - Detective Controls	Section 500.05

Vulnerability scanning is a crucial phase of a penetration test and having an updated vulnerability scanner in your security toolkit can often make a real difference by helping you discover overlooked vulnerable items.   NetWatcher ships with a vulnerability scanner that can be configured to schedule different scans daily, weekly and monthly to find vulnerable surfaces.



Scan Job Z > Report for 2017-04-11 11:00:08

Scan Report for Scan Job - Z

Job Name: Z
Started At: 2017-04-11 11:00:08
Finished At: 2017-04-11 11:16:24
Status: DONE
Severity: HIGH (10)

Actions

Download PDF

Scan Report Vulnerabilities [Hide]

Name	Status	Severity	Host	Port	Family	Date
SMBv1 Unspecified Remote Code Execution (Shadow Brokers)	OPENED	HIGH (10)	10.20.4.5 (10.20.3.153-462751e8)	445/tcp	Windows	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	636/tcp	Remote file access	Apr-11-17
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	80/tcp	Web Servers	Apr-11-17
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	443/tcp	SSL and TLS	Apr-11-17
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	3269/tcp	Remote file access	Apr-11-17

The alignment of compliance mandates to controls is a subset of work found at AuditScripts.com and is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. You can also find these controls at the cisecurity.org website.

We hope you enjoy the NetWatcher service. We've designed the service to be useful for managers, help desk techs and for advanced security analysts. We've tried to make the User Interface (UI) intuitive and easy to use as well as powerful. If you have any questions don't hesitate to contact us at info@netwatcher.com

Follow us on Twitter @netwatcher.

https://netwatcher.com