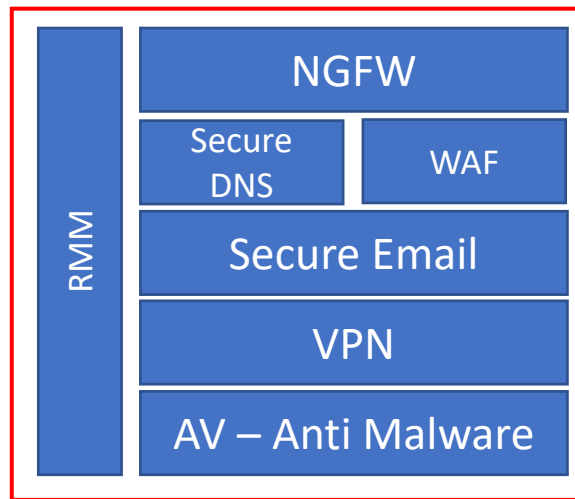


The logo features a blue shield icon with a white checkmark-like shape inside, followed by the word "NETWATCHER" in a bold, white, italicized sans-serif font. A small "TM" trademark symbol is positioned to the upper right of the word.

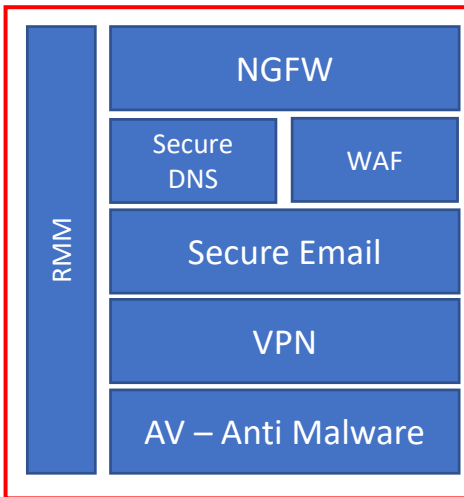
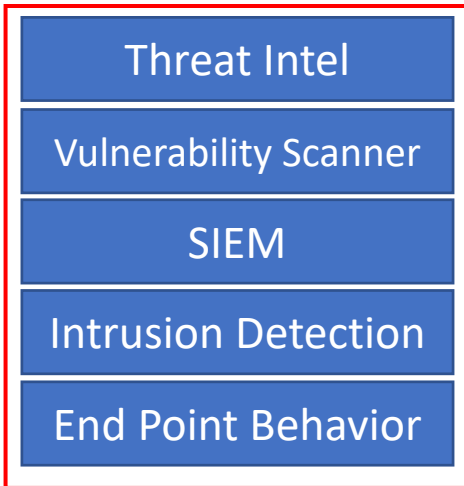
NETWATCHER™

NetWatcher Customer Overview

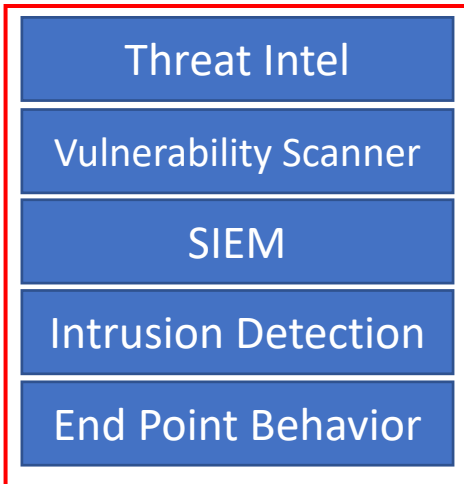
The Problem...



**Most SMBs
have this stack**
It's relatively inexpensive

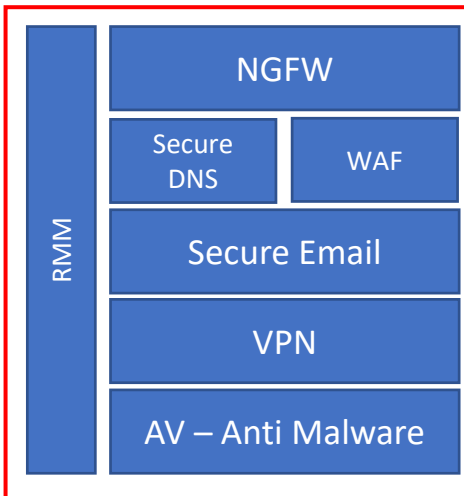


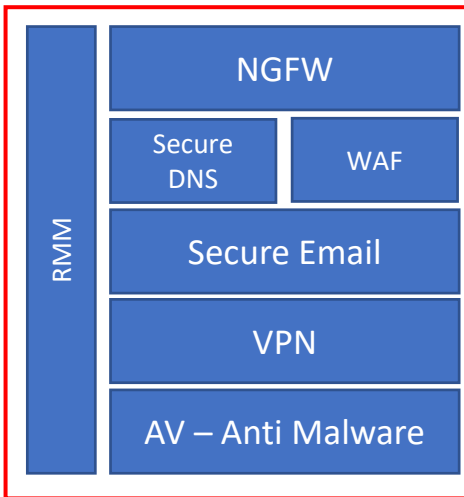
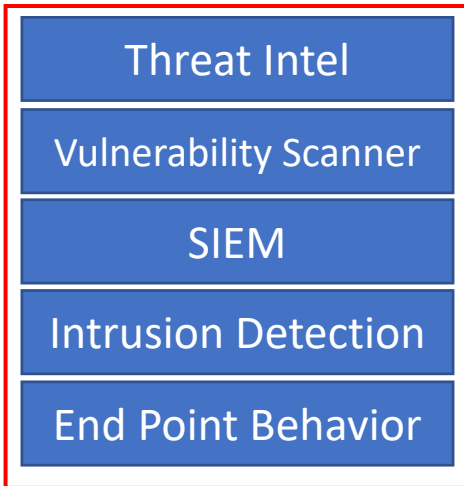
← **All Enterprises have this stack**
...but it's **expensive** and
requires **scarce** security talent



← SBM's can't have this stack

It's **expensive** and
requires **scarce** security talent

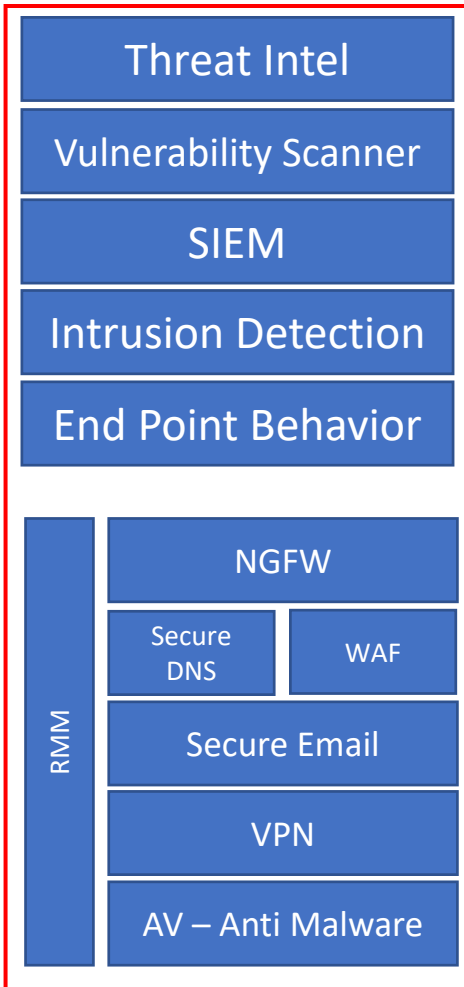




Unfortunately for Regulated SMBs

39% have to have this stack
HIPAA, PCI-DSS, NIST 800-171,
23 NYCRR 500, GLBA etc...

So what are they supposed to do?



● **What if this entire stack was**

Easy to install

Easy to use

Inexpensive

and provided as a service?

Welcome to NetWatcher®

What is...

NetWatcher® “Managed Detection & Response”

- ✓ You deploy Sensors &/or Endpoints
 - ✓ Sensor(s) (hardware or VM) sit on the inside of customers network and listens for anomalies... (IDS, Netflow, SIEM, Scanner). Sensors are not inline.
 - ✓ Endpoint agent (HIDS, Logs, Sensor-in-Cloud VPN/IDS)
- ✓ Sensors/Endpoints send indicators of compromise (events) over a secure VPN to the cloud
- ✓ Automated (cloud) “hunting” for creating Actionable Threat Intelligence Alarms about poor security hygiene, vulnerabilities, active exploits and malware
- ✓ Delivered as a multi-tenant service
- ✓ Backstopped by a team of SOC analysts that become YOUR SOC!

What is...

The Value of NetWatcher

- ✓ Enterprise security provided at a fraction of the **price** of legacy providers
- ✓ Support for security **compliance** line items that are costly and difficult to deploy and manage
- ✓ Access to enterprise security **analysts** working your issues
- ✓ Easy to understand portal with **alerting/reporting** for exploits and hygiene issues that will cause you to be exploited.
 - ✓ Remediation guidance
 - ✓ Access to additional support

Customer Portal Dashboard



Invite a friend and get one month free

Scott Suhy | Logout

Dashboard | Reports | Alarms | Sensors | EndPoints | Advanced | Support

Add Widget | Preset: Default Preset

Executive Dashboard

Cyber Health Score

57

Alarms	High	Medium	Low	Info
Security	0	1	3	0
Policy	0	0	0	43
Scans	0	0	0	0
Hygiene	1	0	19	2

Promiscuity Dashboard

Cyber Promiscuity Score™

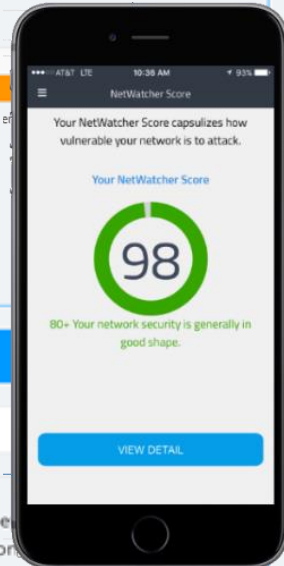
55

High	Medium
2	21

Risky Software

Switch to table | Show Risky Soft | Last Day

- TOR running on ne
- BitTorrent in use on



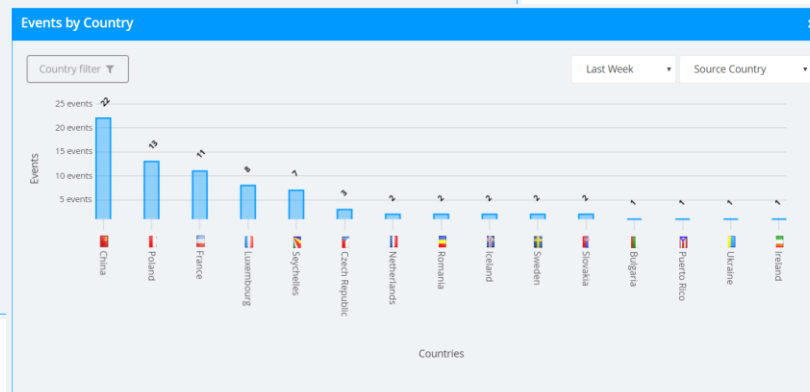
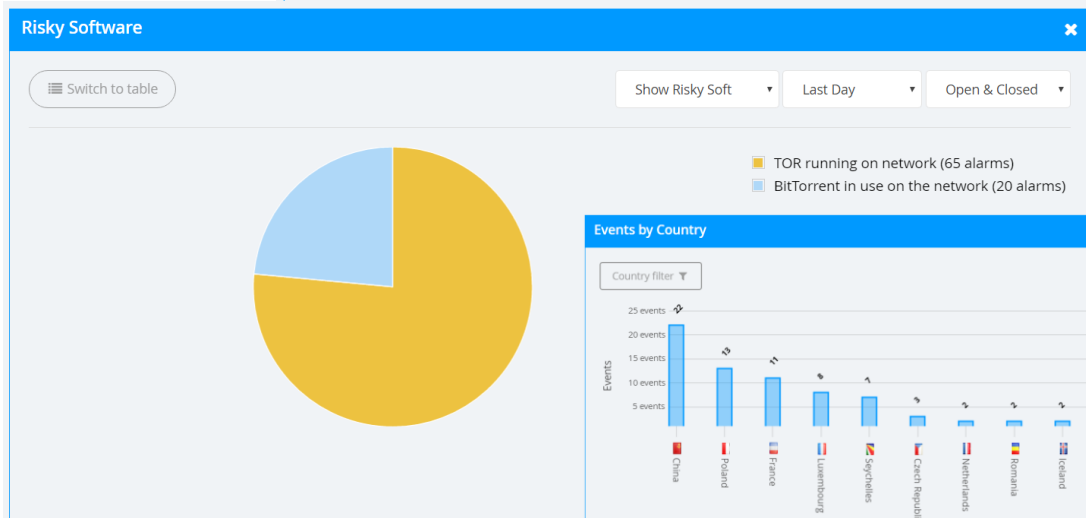
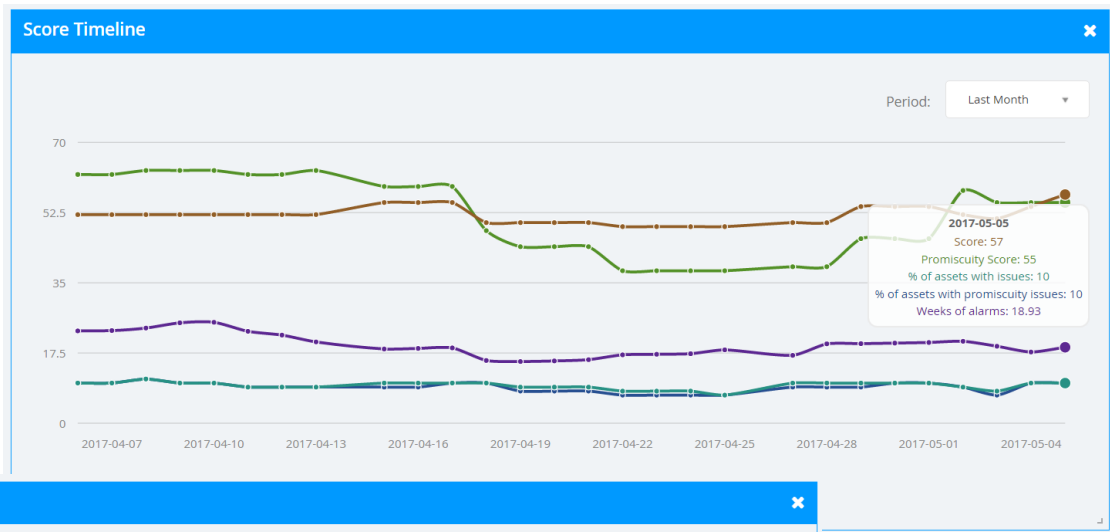
On the customer portal dashboard you will find 2 scores that change as the security situational awareness picture of the customer changes. Both scores are out of 100 (the best you can get).

The Cyber Health Score - This score helps you understand how bad your organization is compromised today.

Cyber Promiscuity Score(TM) - This score helps you understand how much the activity going on in your organization today expose you to future compromise.

If you click on an item in the Executive Dashboard Widget you will be taken directly to that alarm.

Dashboard - Widgets



There are many widgets that you can install onto the dashboard. Some of those include:

1. Score over time
2. Risky Software running on the network
3. Vulnerable Software running on the network
4. Clear text info being sent over the internet
5. Events by country

Alarm "Security" = Malware / Exploit

Each Alarm has an easy to understand description and recommendation written for the IT helpdesk.

If the users account is setup as an 'intermediate' profile (ie. More technical) then you can also see what events the correlation engine used to determine an alarm was necessary.

The User can also create a ticket on the event to work with their partner (MSP) or the NetWatcher SOC team (direct customer).

There is also a comment field that is date and timestamped that HIPAA security rule users can leverage to document how the alarm was remediated.

NetWatcher Invite a friend and get one month free Scott Suhny | Logout

Dashboard | Reports | Alarms | Sensors | EndPoints | Advanced | Support

Jan-23-17 - Feb-13-17

Muldrop Trojan Detected

[Malware] Trojan Horse

Country: Local
IP Address: 10.18.3.174
MAC address: 00:20:5e:29:30:0a
Hostname:

Alarm severity: Medium
Alarm promiscuity: High

Description

Basic:
Trojan.Agent/Gen-MulDrop is a high-risk Trojan horse that can significantly corrupt your system and steal your personal information by implanting more other malicious virus into your computer. This Trojan may get into your computer via some free software, spam email attachments or social networks. It can attack computers with Windows operating systems worldwide since its developers spread it globally. You didn't realize that it has sneaked into your computer until the antivirus detects it.

Once Trojan.Agent/Gen-MulDrop infiltrates into your computer, it can execute a series of malicious actions. It will modify important system files to consolidate its existence and consume computer space making your computer work extremely slow like a snail. Furthermore, it gathers the email addresses of your contacts and sends unexpected email messages to your friends in your name without your permission. What is worse, it can record your online behaviors including what you type, what program you run and what website you visit. All the information will be sent back to the cyber criminals. It is highly recommended to remove this Trojan as quickly as possible before more damages to your computer and more losses.

This Trojan is tricky. It hides deep in your computer system, mutates fast and injects its code into legitimate antivirus programs to prevent itself from being removed. Therefore, the most effective way to get rid of this Trojan is manual removal. Please note that manual removal is complicated and any wrong operation will lead to mistakes damaging your system seriously.

Actions

- Create Ticket
- Community Forum
- Email
- Mark
- Lock
- Check

Recommendation

Basic:
Usually Muldrop can be removed with a common tool such as a rootkit remover like the one found [here](#).

If this does not work, load GMER and send the NetWatcher team a ticket with out output of the tool for additional analysis. GMER is an anti-rootkit scanner that searches your computer for Rootkits on your computer and then allows you to attempt to remove them. You can find GMER [here](#).

A rootkit is a malware program that is designed to hide itself or other computer infections on your computer. These types of programs are typically harder to remove than generic malware.

Events related to the alarm

Signature	Source Hostname	Source MAC / IP / Country	Destination Hostname	Destination MAC / IP / Country	Labels	Sensor ID	Date
ETFRD TROJAN Muldrop Checkin		00:20:5e:29:30:0a 10.18.3.174	courte23.51yes.com	50:c5:8d:7d:1e:10 38.99.159.23 (Canada)	ID5 HAS ALARMS (1)	oe_lanner- -oe	Feb-13-17
ETFRD TROJAN Muldrop Checkin		00:20:5e:29:30:0a 10.18.3.174	courte23.51yes.com	50:c5:8d:7d:1e:10 38.99.159.23 (Canada)	ID5 HAS ALARMS (1)	oe_lanner- -oe	Feb-13-17
ETFRD TROJAN Muldrop Checkin		00:20:5e:29:30:0a 10.18.3.174	courte23.51yes.com	50:c5:8d:7d:1e:10 38.99.159.23 (Canada)	ID5 HAS ALARMS (1)	oe_lanner- -oe	Feb-13-17

Display: 1n

Comments

Please submit comment

Submit

MSP Partners can get this same detail sent to ConnectWise.

Users can also receive Alarms via SMS and email.

Alarm "Policy" "Scans" "Hygiene"

Policy alarms are related to users visiting sites that are not appropriate such as pornography and online gambling...

Scan alarms are when a bad actor is doing reconnaissance on the organization (example: someone running Metasploit on internal assets).

Hygiene alarms are when a user is doing something that opens the organization up for exploit.

An alarm is only created 1 time per asset per alarm type to ensure alarm fatigue is not an issue. The alarm is then aged over a 2 week period and closed if it is not seen again.

Alarm 'triggers' can be created to forward alarms based on search query via SMS and email.

The screenshot displays the NetWatcher dashboard interface. At the top, there is a navigation bar with the NetWatcher logo, a promotional banner for a free trial, and user information for Scott Suhy. Below the navigation bar, there are tabs for Dashboard, Reports, Alarms, Sensors, EndPoints, and Advanced. The main content area shows a list of alerts with filters and a 'Show' button. The first alert is titled 'Cisco Telnet in use over the internet' with a severity of High and a promiscuity of High. The second alert is 'Outdated/Vulnerable Java Version' with a severity of Low and a promiscuity of Medium. The third alert is 'TOR running on network' with a severity of Low and a promiscuity of Medium. Each alert includes a 'Details' button and links for 'Show recommendation', 'Show description', and 'Show promiscuity description'. The dashboard also features a 'Display' dropdown set to 10 items.

Reports – Compliance as a Service

Reports can be created across any of the data in the system (events, alarms, assets, tickets etc..)

Reoccurring Reports can be created and sent via email and also stored for future download by users and auditors.

Download as PDF or CSV.

The screenshot displays the NetWatcher Reports interface. At the top, there's a navigation bar with 'Dashboard', 'Reports', 'Alarms', 'Sensors', 'EndPoints', 'Advanced', and 'Support'. Below this, a 'Create Report' button and 'Your reports' link are visible. The main area is divided into three steps: 1. Type (with a dropdown menu showing 'Events', 'Assets', 'Alarms', 'Tickets', 'Situational Awareness', and 'Alarms With Comments'), 2. Include columns (with a list of columns like 'Date', 'Severity', 'Is new', 'Sensor', 'Manual', and 'False positive'), and 3. Period (with 'From' and 'To' date fields). A line graph is shown on the left side of the interface. Below the graph, there's a summary section with 'You have 2 reoccurring reports' and 'You have 3 saved report templates'. The 'Report History' table is shown below, with columns for Report Category, Report Type, Filters, Send To, Status, and Action. A dropdown menu is open over the first row, showing 'Download' and 'Delete' options.

Report Category	Report Type	Filters	Send To	Status	Action
May-04-17 2:39:42 PM (America/New_York -04:00)	Scan report PDF for OE 1020 at 2017-02-21 16:04:41	Scan Job Result	pdf	COMPLETED	Download, Delete
May-02-17	Scan report PDF for Z at 2017-04-19 13:18:33	Scan Job Result	pdf	COMPLETED	Download, Delete
Apr-21-17	Situational Awareness OE	Situational Awareness	pdf	COMPLETED	Download, Delete
Apr-11-17	Scan report PDF for OE TEST at 2017-02-15 13:30:57	Scan Job Result	pdf	COMPLETED	Download, Delete
Apr-10-17	suhy	Events	csv	COMPLETED	Download, Delete
Apr-10-17	sa	Situational Awareness	pdf	COMPLETED	Download, Delete
Mar-27-17	suhy	Situational Awareness	pdf	COMPLETED	Download, Delete

NetWatcher Endpoint

The NetAgent for Linux/Windows (and soon MAC) provides the organization with a “health” and “promiscuity” score per asset so it is easy to see the trouble spots in the organization that may need additional cyber training.

The HIDS module enable File Integrity Monitoring, Rootkit checks and Process monitoring via OSSEC and the Wazuh ruleset.

The LOGS module pushes the operating system logs to the sensor for additional correlation.

The Sensor-in-the-Cloud module allows administrators to track corporate assets event when they are not on the network. This opens a secure VPN and leverage a sensor hosted in the NetWatcher Cloud.

The screenshot displays the NetWatcher Endpoint dashboard. At the top, there is a navigation bar with the NetWatcher logo, a promotional banner for a free month, and user information for Scott Suhy. Below the navigation bar, there are tabs for Dashboard, Reports, Alarms, Sensors, EndPoints, and Advanced, along with a Support link. The main content area features a 'Net Agents' section with a 'Download NetAgent' button. Below this, there are sections for 'Available Modules Counts' and 'Filters'. A table titled 'With selected: Actions' lists several assets. The table columns are: Asset, Hostname, IP address, MAC, Events, Alarms, Health, CPS, Last Checkin, Modules, and Actions. The 'Health' column uses color-coded bars to represent the health score, and the 'CPS' column shows the promiscuity score. The 'Modules' column lists installed modules like HIDS, Logs, Sensor in the Cloud, and Systray. The 'Actions' column includes 'View' and 'Delete' options.

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	22513	3	72	52	About 5 minute(s) ago	HIDS, Logs, Sensor in the Cloud, Systray	View, Delete
Scotts Dell	desktop-bef6s1f	10.238.134.180	28:b2:bd:78:49:5c	74147	1	90	82	About 15 hour(s) ago	HIDS, Logs, Sensor in the Cloud, Systray	View, Delete
asset2733-0...	cstack-pc	10.18.1.180	34:02:86:1e:5e:d8	1346	1	96	87	About 21 hour(s) ago	HIDS, Logs, Sensor in the Cloud, Systray	View, Delete
Adam Work	desktop-51s4f97	10.20.1.37	58:82:a8:98:3a:25	23036	1	97	92	About 1 minute(s) ago	HIDS, Logs, Sensor in the Cloud	View, Delete

NetWatcher Endpoint Detail

Net Agent Scott's HP

Net Agent Details [Hide]

Id: dd2dd0e1-2734-4a65-aaa1-e3fcf4f17d2f

Version: 1.0.43

Last Checkin: About 3 minute(s) ago

OS:

bootTime	hostid	hostname	kernelVersion	os	platform	platformFamily	platformVersion	procs	uptime	virtualizationRole	virtualizationType
1493987987	40575365-1d54-4816-9c63-f20476...	HP-8570w		windows	Microsoft Windows 10 Pro	Standalone Workstation	10.0.14393 Build 14393	132	17914		

Logged in Users

Gid	HomeDir
S-1-9-21-4285624716-1093760716...	C:\Users\Scott.Suhay

CPU(s)

cacheSize	coreId	cores	cpu	family	flags	mhz
						7401

Software Components Table:

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
ADAAudit Plus	ZOHO Corp	ADAAUDIT	1	1	1	1
[SAFE]_AddressBook			1	1	0	0
Adobe Acrobat XI Pro	Adobe Systems	ADOBE ACROBAT PRO	1	1	0	0
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
Any Video Converter Professional 6.0.7	Any-Video-Converter.com		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
AVS Audio Editor 8.2.1	Online Media Technologies Ltd.		1	1	1	1
BingProvidedSearch			1	1	0	1

Uninstall String Detail: c:\Program Files (x86)\Common Files\Adobe AIR\Versions\1.0\Resources\Adobe AIR Updater.exe -arp:uninstall

The NetAgent also provides detail on the operating system and hardware detail as well as all the software corresponding components as well as versions, install / uninstall location.

All software detail can also be used for correlation purposes.

NetWatcher SYSLOG Ingestion

The screenshot displays the NetWatcher web interface. At the top, there is a navigation bar with the NetWatcher logo, a promotional message "Invite a friend and get one month free", and user information for Scott Suhy. Below the navigation bar, there are tabs for Dashboard, Reports, Alarms, Sensors, EndPoints, and Advanced, along with a Support link.

The main section is titled "My Sensors" and contains a table with the following data:

Active or Not	Sensor Name	IP address	Events	Opened Alarms	Service Installed	Groups	Actions
●	oe-virtual-ken-test	192.168.55.113	0	0	SYSLOG SCANNER OSSEC		⌵
●	oe-ken-test		0	0	SYSLOG SCANNER OSSEC		⌵
●	oe-virtual00	192.168.134.223	21064	2	SYSLOG SCANNER OSSEC		⌵
●	oe_lanner-oe	10.20.7.68	957181	31	SYSLOG SCANNER OSSEC		⌵

Below the table, there are options to "Enable Logs for all Sensors" and "Enable Scanning for all Sensors". A dropdown menu is open, showing options for "Log IPs", "Log Rules", "Syslog Questionnaire", and "NetFlow".

The bottom section is titled "Manual Log Assets" and shows a summary: "Total Log Assets: 14 Manual Log Assets: 4 NetAgent Log Assets: 10". There is a button to "Add manual IP for Syslog". Below this, there is a "Filters" section and a table with the following data:

Source IP	Sensor	Timestamp	Actions
192.168.99.99	oe_lanner-oe	Sep-25-16	⌵
10.20.20.1	oe_lanner-oe	Jul-07-16	⌵
10.20.4.22	oe_lanner-oe	Jul-07-16	⌵
10.18.0.7	oe_lanner-oe	Jul-07-16	⌵

NetWatcher can also ingest SYSLOGs from hardware devices such as a firewall for correlation purposes.

NetWatcher Vulnerability Scanner

The screenshot displays the NetWatcher web interface. At the top, there is a navigation bar with the NetWatcher logo, a promotional banner for a free trial, and user information for Scott Suhy. Below the navigation bar, there are tabs for Dashboard, Reports, Alarms, Sensors, EndPoints, and Advanced. A secondary navigation bar includes buttons for Events, Assets, Scanning, and Networks. The main content area is titled 'Vulnerability Scanner' and features a '+ Create Scan Job' button. A table lists several scan jobs, all with a status of 'DONE'. A modal window titled 'Scan Job - Z' is open, showing details for a specific scan job. This modal includes a 'Sensor' field, a 'Status' field (set to 'DONE'), and a 'Scan Config' section with options for 'Full Network Scanning', 'Credentials', and 'Auto Generate Report'. A 'Schedule Method' section allows for scheduling a scan. Below the configuration, there is a 'Scan Reports' table with columns for 'Started At', 'Finished At', 'Status', 'Severity', and 'Vulnerabilities'. The modal also features an 'Actions' panel with buttons for 'Set inactive', 'Run', 'Edit', and 'Delete'.

Name	Sensor	Status	Status Timestamp	Reports	Waiting for	Actions
Discovery (Reoccurring Daily)	oe_lanner-oe	DONE	Jul 19 13:03:02			
Full and Fast (Reoccurring Weekends)	oe_lanner-oe	DONE	Jul 19 13:03:02			
Z	oe_lanner-oe	DONE	Apr 19 13:03:02			
OE Test	oe_lanner-oe	DONE	Apr 19 13:03:02			
Test	oe_lanner-oe	DONE	Apr 19 13:03:02			
Disc Test	oe_lanner-oe	DONE	Apr 19 13:03:02			

Started At	Finished At	Status	Severity	Vulnerabilities
2017-04-19 13:03:02	2017-04-19 13:18:33	DONE	MEDIUM (5)	85
2017-04-11 11:00:08	2017-04-11 11:16:24	DONE	HIGH (10)	85

NetWatcher can easily create reoccurring vulnerability scans that can be used for PCI-DSS internal scans.

Users can schedule reoccurring scans or run one – time scans of specific assets.

NetWatcher Vulnerability Scanner

The screenshot displays the NetWatcher web interface. At the top, there's a navigation bar with 'Dashboard', 'Reports', 'Alarms', 'Sensors', 'EndPoints', 'Advanced', and 'Support'. Below this, there are tabs for 'Events', 'Assets', 'Scanning', and 'Networks'. The main content area shows a 'Scan Report for Scan Job - Z' with a 'Download PDF' button. A table titled 'Scan Report Vulnerabilities' lists several vulnerabilities. The first one is 'SMBv1 Unspecified Remote Code Execution (Shadow Brokers)' with a status of 'OPENED' and a severity of 'HIGH (10)'. Below this, there's a detailed view for this specific vulnerability, including a table with columns for Name, Severity, Host, Port, and Status. The detailed view also includes a 'Summary' section with a 'Solution' section.

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	
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	
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	
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)	443/tcp	Web Servers	
Use LDAP search request to retrieve information from NT Directory Services	OPENED	MEDIUM (5)	10.20.4.5 (10.20.3.153-462751e8)		Remote file access	

Name	Severity	Host	Port	Status
SMBv1 Unspecified Remote Code Execution (Shadow Brokers)	HIGH (10)	10.20.4.5	445/tcp	OPENED

Job Name	Report	Date	Asset	Event
Z	2017-04-11 11:00:08	Apr-11-17	10.20.3.153-462751e8	SMBv1 Unspecified Remote Code Execution (Shadow Brokers)

Summary

The remote Windows host is prone to an unspecified remote code execution vulnerability in SMBv1 protocol.

Solution

Disable SMB v1 and/or block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Once scans are run events are produced that line up with CSV priorities (low, med, high).

Users can report on all vulnerabilities or that can work the issues from top to bottom.

The NetWatcher cloud correlation service uses the vulnerability events as just another data source.

NetWatcher Accounts and Alerts

The screenshot displays the NetWatcher user interface. At the top, there is a navigation bar with the NetWatcher logo, a promotional banner for inviting a friend, and user information for Scott Suhy. Below the navigation bar, there are tabs for Base Info, Searches, and Credentials. The main content area is divided into several sections:

- Contact Information:** Fields for First Name (scott), Last Name (suhy), Company (Ocean's Edge), Email (scott.suhy@gmail.com), Phone (+1 (202) 5576937), and Time Zone (UTC -04:00) America/New York.
- User Experience Profile:** Radio buttons for Basic and Intermediate (selected). A description states: "Shows more information and uses technical terms. You should understand networking (TCP/IP) and basic security principles (different kinds of malware)." There is also a section for Multi-factor Authentication (ENABLED) with an Enable button.
- Alerts:** A table with columns for Email, SMS, and How often. The rows are Security, Hygiene, and Scan.
- Contacts List:** A list of contacts with their names and email addresses. A green "+ Add Contact" button is visible.

	Email	SMS	How often
Security	Send Medium and High	Send only High	Send as soon as occurs
Hygiene	Don't send	Don't send	Send as soon as occurs
Scan	Don't send	Don't send	Send as soon as occurs

Name	Email
tom shanley	tom@oceansedge.biz
Fiz Pop	t77@decryptic.com
Karpagam Balan	karpagam.balan@defensive.com
Temp User	t25@decryptic.com
Kenneth Shelton	kenneth.shelton@oceansedgeinc.com
Lauren Sexton	lauren.sexton@defensive.com

Customer Portal “Contacts” can be setup with different profiles (basic/intermediate) and can be configured to have alarms pushed to them as emails or SMS messages.

Contacts can also have the score sent to them via email.

A great way to setup a customer is for the management to get the score and reports sent to them weekly and to have alarms sent directly to the IT helpdesk or MSP for remediation.

NetWatcher Advanced

The screenshot shows the NetWatcher Advanced interface. The top navigation bar includes 'Dashboard', 'Reports', 'Alarms', 'Sensors', 'EndPoints', 'Advanced', and 'Support'. The user is logged in as 'Scott Suhny'. The 'Events' tab is active, showing a 'Filters' section with a 'Load filter' dropdown set to 'China - All events last week'. Below this, there are filter rules: 'AND Source Country = China, Russian Federation' and 'AND Type = IDS'. The date range is set to 'Last Week'. There are buttons for 'Apply Filters', 'Reset', 'Share with the analyst', and 'Save Filter'.

The 'Save Filter' dialog box is shown, allowing users to save their current filter configuration. It includes a 'Name' field with the text 'SMS inbound traffic from China on IDS'. There are two checkboxes: 'Send new items via Email' (unchecked) and 'Send new items via SMS' (checked). A blue 'Save' button is at the bottom.



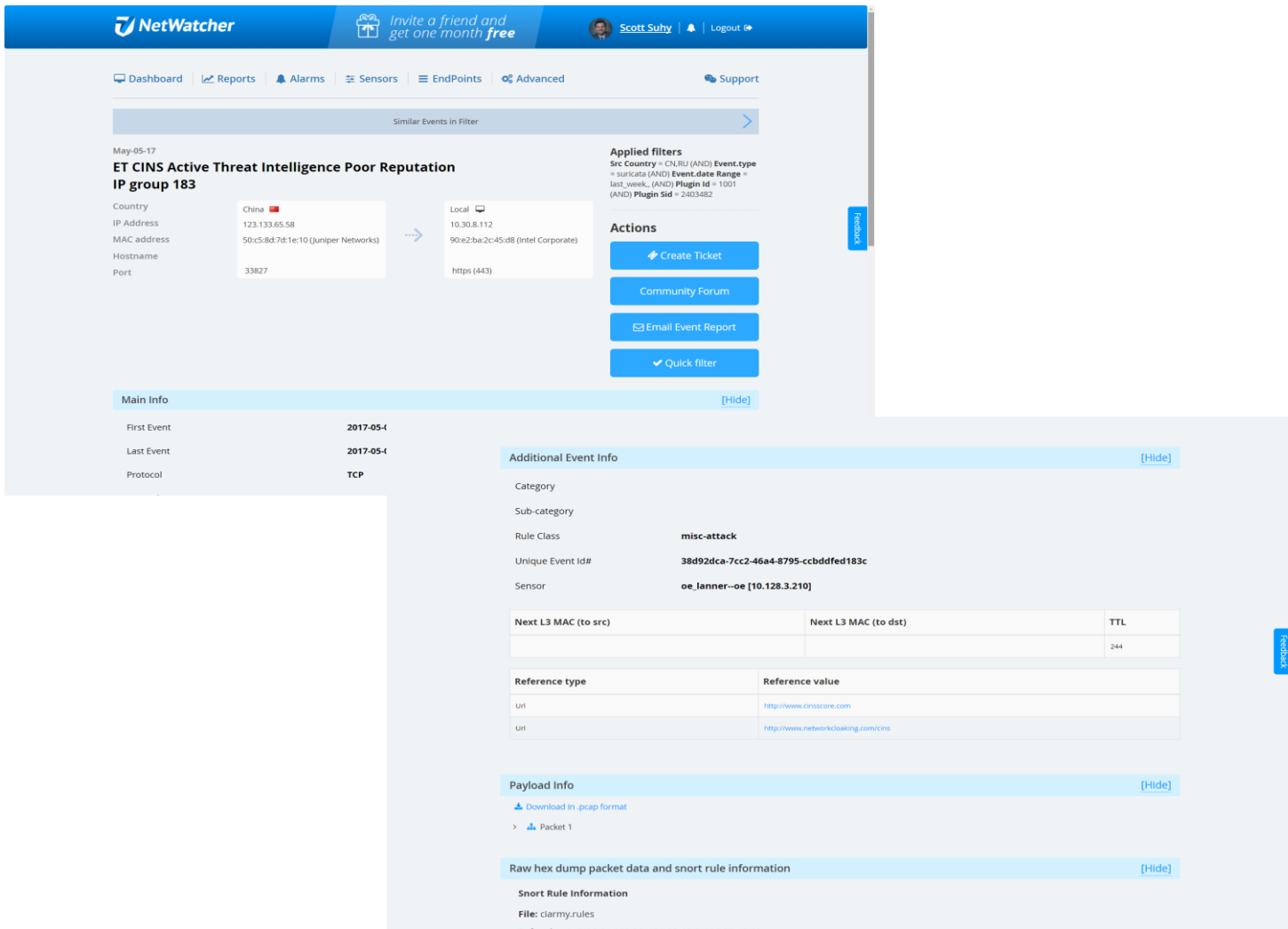
Signature	Total	Latest Event	Actions
ET CINS Active Threat Intelligence Poor Reputation IP group 183	18	May-05-17	▼
ET CINS Active Threat Intelligence Poor Reputation IP group 67	3	May-03-17	▼
ET DROP Dshield Block Listed Source group 1	1	May-04-17	▼

The advanced tab is for customers that have technical people that understand security and want access to the event detail that gets correlated to produce actionable threat intelligence “alarms”.

Users can create any query on the (NIDS, HIDS, LOGS, Products and Vulnerability Scanning data) and turn it into either a report or a tripwire that can send an email or SMS if tripped.

Charts can also be created easily based on the query.

NetWatcher Advanced – Event Detail 1 of 2



The screenshot displays the NetWatcher Advanced interface for an event detail. The top navigation bar includes 'Dashboard', 'Reports', 'Alarms', 'Sensors', 'EndPoints', 'Advanced', and 'Support'. The user 'Scott Sulby' is logged in. The main content area shows event details for 'ET CINS Active Threat Intelligence Poor Reputation IP group 183' on May-05-17. It includes a comparison of IP addresses from China (123.133.65.58) to Local (10.30.8.112). The 'Applied filters' section shows criteria like 'Src Country = CN,RU' and 'Event.type = suricata'. Action buttons include 'Create Ticket', 'Community Forum', 'Email Event Report', and 'Quick filter'. The 'Main info' section shows 'First Event' and 'Last Event' dates, and 'Protocol' as TCP. The 'Additional Event Info' section provides details on 'Rule Class' (misc-attack), 'Unique Event Id#', and 'Sensor'. A table shows 'Next L3 MAC' and 'TTL' values. The 'Reference type' section lists 'Uri' values. The 'Payload Info' section offers a 'Download in pcap format' link. The 'Raw hex dump packet data and snort rule information' section shows 'Snort Rule Information' with file and rule details.

Digging into an event allows the user to get at the details of what external IP the internal asset is communicating with... What country it's in... What Port, Hostname etc.. When did the session start and end... What does the header look like...

Download the packet (pcap) into Wireshark.

NetWatcher Advanced – Event Detail 2 of 2

Raw hex dump packet data and snort rule information [Hide]

Snort Rule Information

File: clammy.rules

Rule: alert ip [123.24.252.99, 123.25.63.3, 123.28.48.62, 123.51.173.155, 123.52.131.70, 123.52.131.94, 123.52.131.114, 123.52.131.211, 123.52.131.215, 123.52.131.217, 123.59.45.141, 123.59.51.8, 123.59.54.89, 123.59.59.89, 123.59.71.2, 123.59.74.3, 123.59.76.3, 123.59.76.192, 123.59.78.2, 123.59.79.3, 123.59.81.6, 123.59.83.32, 123.59.105.67, 123.59.149.74, 123.59.194.32, 123.59.194.138, 123.59.194.207, 123.59.195.16, 123.65.242.55, 123.75.215.6, 123.75.215.23, 123.98.189.99, 123.100.137.17, 123.100.166.169, 123.100.172.235, 123.110.39.249, 123.110.162.253, 123.110.183.112, 123.110.241.223, 123.111.200.108, 123.111.222.31, 123.115.124.115, 123.124.21.253, 123.125.226.248, 123.127.108.163, 123.133.65.58, 123.139.215.78, 123.140.58.119, 123.140.135.9, 123.140.155.100] any -> \$HOME_NET any

msg: "ET CINS Active Threat Intelligence Poor Reputation IP group 183"

reference: url,www.cinsscore.com

reference: url,www.networkcloaking.com/cins

threshold: type limit, track by_src, seconds 3600, count 1

classtype: misc-attack

sid: 2403482

rev: 3223

Net Flow Data [Hide]

timestamp	2017-05-05 11:53:06
start	2017-05-05 11:42:17
end	2017-05-05 11:42:17
protocol	tcp [Transmission Control]
timestamp	2017-05-05 11:53:06
start	2017-05-05 11:42:17
end	2017-05-05 11:42:17
protocol	tcp [Transmission Control]

Net Flow Data [Hide]

timestamp	2017-05-05 11:53:06
start	2017-05-05 11:42:17
end	2017-05-05 11:42:17
protocol	tcp [Transmission Control]
dst_ip	10.30.8.112
dst_port	443 [secure http]
pkts_to_server	1
pkts_to_client	0
bytes_to_server	60
bytes_to_client	0
age	0
state	New
reason	Timeout

Related Events [Hide]

Within Day Search

Signature	Source Hostname	Source MAC / IP / Country	Destination Hostname	Destination MAC / IP / Country	Labels	Sensor ID	Date
ET CINS Active Threat Intelligence Poor Reputation IP group 183		50:c5:86:76:1e:10 123.133.65.58 (China)	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-05-17
ET CINS Active Threat Intelligence Poor Reputation IP group 51		50:c5:86:76:1e:10 46.174.191.32	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-05-17
ET CINS Active Threat Intelligence Poor Reputation IP group 51		50:c5:86:76:1e:10 46.174.191.28	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-05-17
ET CINS Active Threat Intelligence Poor Reputation IP group 51		50:c5:86:76:1e:10 46.174.191.32	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-05-17
ET CINS Active Threat Intelligence Poor Reputation IP group 51		50:c5:86:76:1e:10 46.174.191.32	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-04-17
ET CINS Active Threat Intelligence Poor Reputation IP group 42	worker-4-27b-69.stretchoid.com	50:c5:86:76:1e:10 45.55.13.8 (United States)	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-04-17
ET DROP Dashed Block Listed Source group 1	worker-4-27b-69.stretchoid.com	50:c5:86:76:1e:10 45.55.13.8 (United States)	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-04-17
ET CINS Active Threat Intelligence Poor Reputation IP group 11	194.145.89-23.rns.scaleddns.com	50:c5:86:76:1e:10 23.86.145.194 (United States)	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-04-17
ET CINS Active Threat Intelligence Poor Reputation IP group 85	scanner2.labs.rapid7.com	50:c5:86:76:1e:10 71.62.216.40 (United States)	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-04-17
ET CINS Active Threat Intelligence Poor Reputation IP group 71		50:c5:86:76:1e:10 46.174.191.31	90:e2:ba:2c:45:d8 10.30.8.112	90:e2:ba:2c:45:d8 10.30.8.112	[OK]	oa_janner-0e	May-04-17

Display: 10

lab-1f59-67d0-2e0bc26ac01e

1e:10

45:d8

What rule tripped the event...

What Netflow analytics for the session are associated with the event...

What other events have occurred on this asset within an hour, day, week and month...

Support

The screenshot displays the NetWatcher user interface. At the top, there is a navigation bar with the NetWatcher logo, a promotional banner for inviting a friend, and user information for Scott Suhy. Below this is a dashboard with tabs for Tickets, WIKI, and Community Forum. The 'My Tickets' section shows 3 tickets left and an 'Add Ticket' button. A table lists various tickets with columns for ID, Summary, Priority, Status, Type, Assignee, Created, and Paid. The 'Create Ticket' form is open, showing fields for Subject, Description, Priority (set to Low), and Type (set to Question). There are also buttons for 'Attach Alarms' and 'Attach Events', and a 'Send' button at the bottom of the form.

ID	Summary	Priority	Status	Type	Assignee	Created	Paid
118	Alarm	LOW	OPEN	incident	Contact: support	Jul-09-17	No
69	Test Ticket	LOW	OPEN	question	Contact: support		
68	Testing Taplica removal ticket	LOW	OPEN	question	Contact: support		
65	Alarm	LOW	OPEN	question	Contact: support		
62	Test Event Alarm	LOW	OPEN	incident	Contact: support		
47	This is a test ticket created by scott suhy2	NORMAL	OPEN	problem	Contact: scott suhy		
46	This is a test ticket created by scott suhy	LOW	OPEN	question	Contact: scott suhy		
45	test	LOW	OPEN	question	Contact: scott suhy		
42	Alarm	LOW	OPEN	question	Contact: scott suhy		
34	Alarm: Potential use of pornography		OPEN	question	Contact: scott suhy		

NetWatcher has a ticketing engine that end users can use to communicate with their MSP or NetWatcher support (direct account).

Ticketing is recorded for monetization purposes. Currently NetWatcher charges 37 dollars a ticket.

<https://netwatcher.com>