

Managing Endpoint Threat Detection and Response Using SanerNow

4.0 User Guide

Contents

ENDPOINT THREAT DETECTION AND RESPONSE (EDR).....	3
Indicators of Attacks	3
Indicators of Compromise.....	4
<i>To add a threat feed</i>	<i>4</i>
<i>To discover and evaluate threats</i>	<i>4</i>
Build your own Detection and Response	5
<i>To create a custom query for threat detection.....</i>	<i>6</i>
Detection Summary	7
Response Summary.....	8
SETTING ALERTS FOR ENDPOINT DETECTION AND RESPONSE.....	8
To Set Alerts for Endpoint Detection and Response.....	8
ENDPOINT DETECTION AND RESPONSE REPORTS	9
To Generate the Endpoint Detection and Response Report	9
To Back Up Reports.....	10

Endpoint Threat Detection and Response (EDR)

The SanerNow EDR tool helps detect current and on-going attacks and includes commands to respond to threats.

SanerNow supports STIX/TAXII, OpenIOC and Yara feeds and can use threat Intelligence from other sources to detect Indicators of Compromise (IoC). You can execute queries based on attack symptoms to investigate abnormal behavior or detect an on-going attack on the network.

If an attack is in progress, you can take various mitigation actions, including blocking the execution of an application or executable, killing a process, cleaning registry entries, terminating a network connection, quarantining files, cleaning up startup folders and temp folders. Vulnerabilities can be easily linked to an exploit or an attack to apply a more permanent remediation strategy of rolling out security patches.

SanerNow allows you to add and manage threat feeds. By default, SanerNow has a default threat feed supplied by SecPod. Threat feeds must be in the JSON format. Registry and file checks, and md5sum checks are performed for threat feeds.

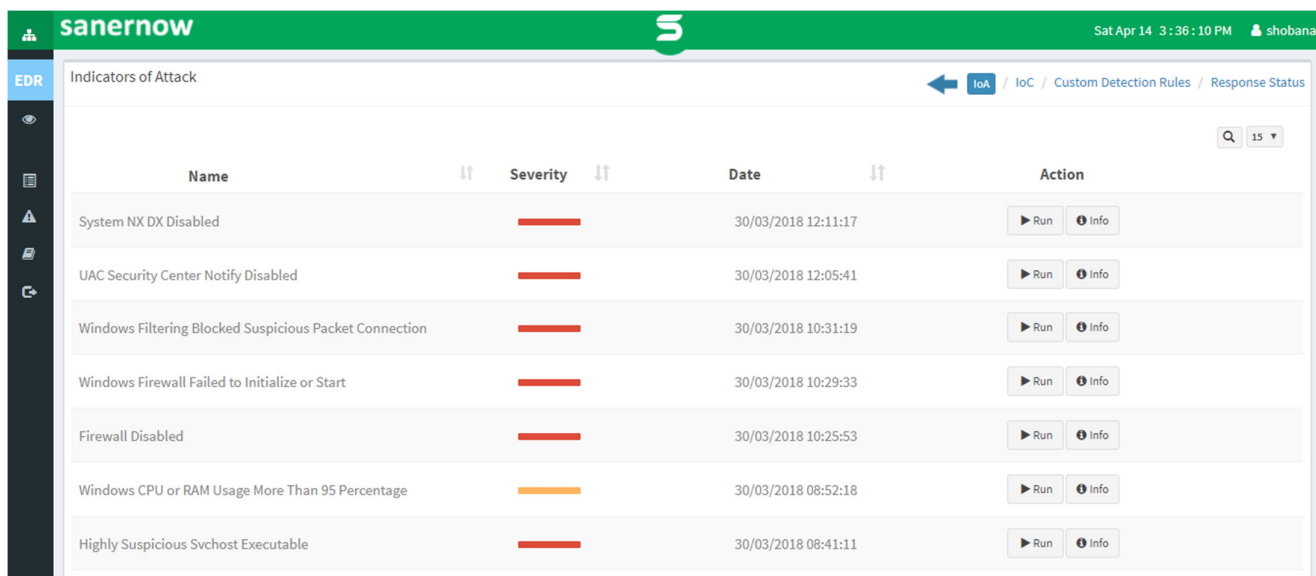
To access the EDR tool:

1. Logon to SanerNow using your SanerNow credentials.
2. Select an account to manage by clicking the icon at the upper left corner of the window. A dashboard with the summary view of the account is displayed.
3. Click the SanerNow icon on the header. Click the EDR icon. The EDR dashboard is displayed.

Indicators of Attacks

This pane shows any ongoing malware attacks in progress. Click the expand button to run a query or to find out details about the attack.

Query	Family	Risk	Detected	Hosts
Firewall Disabled	IoA	<div></div>	Sat Apr 07 12:30:50 UTC 2018	17
System GateKeeper Disabled	IoA	<div></div>	Sat Apr 07 12:29:46 UTC 2018	1
System UAC Off	IoA	<div></div>	Sat Apr 07 12:30:10 UTC 2018	4
Windows CPU or RAM Usage...	IoA	<div></div>	Tue Apr 10 06:24:47 UTC 2018	2



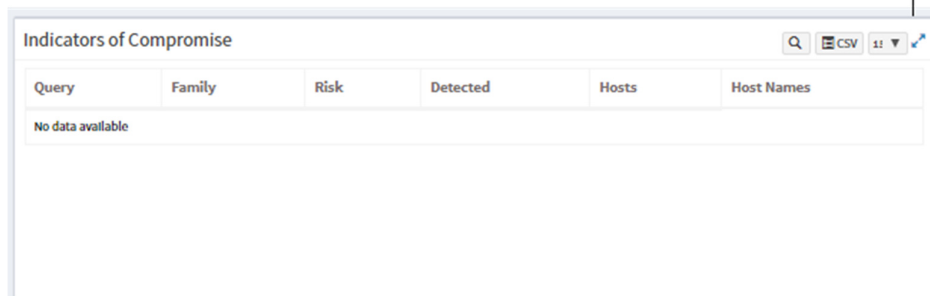
SanerNow interface showing Indicators of Attack (IoA). The table lists various security events with their severity, date, and actions.

Name	Severity	Date	Action
System NX.DX Disabled	High	30/03/2018 12:11:17	Run Info
UAC Security Center Notify Disabled	High	30/03/2018 12:05:41	Run Info
Windows Filtering Blocked Suspicious Packet Connection	High	30/03/2018 10:31:19	Run Info
Windows Firewall Failed to Initialize or Start	High	30/03/2018 10:29:33	Run Info
Firewall Disabled	High	30/03/2018 10:25:53	Run Info
Windows CPU or RAM Usage More Than 95 Percentage	Medium	30/03/2018 08:52:18	Run Info
Highly Suspicious Svchost Executable	High	30/03/2018 08:41:11	Run Info

Indicators of Compromise

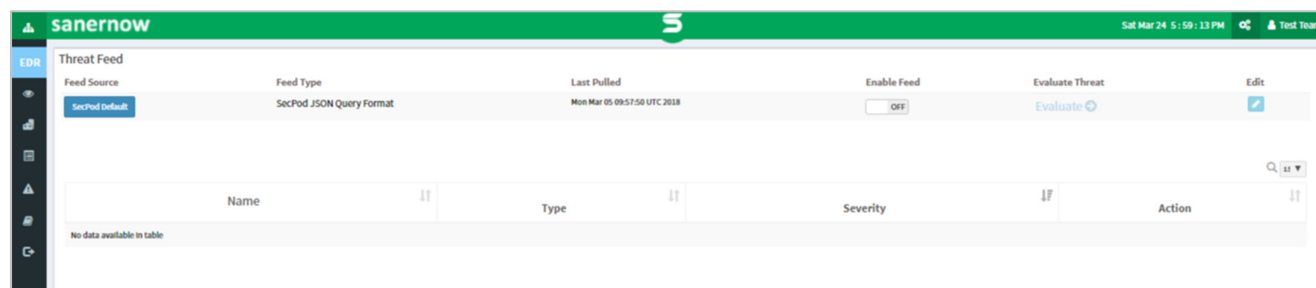
This pane shows potential threats that can evolve into an attack if left unchecked. By default, the SecPod Threat feed is included with the EDR Tool. Click the Expand icon to enable the threat feed and to evaluate or edit it.

Click to enable the threat feed or evaluate , or edit it!



Indicators of Compromise (IoC) interface. The table shows no data available.

Query	Family	Risk	Detected	Hosts	Host Names
No data available					



SanerNow interface showing Threat Feed. The table lists threat feed sources with their type, last pulled date, and actions.

Feed Source	Feed Type	Last Pulled	Enable Feed	Evaluate Threat	Edit
SecPod Default	SecPod JSON Query Format	Mon Mar 05 09:57:50 UTC 2018	OFF	Evaluate	Edit

Below the table, there is a section for detailed threat information with columns: Name, Type, Severity, Action. This section also shows 'No data available in table'.

Name	Type	Severity	Action
No data available in table			

To add a threat feed

If you have purchased a threat feed and would like to add the feed source in SanerNow, contact SecPod.

To discover and evaluate threats

By default, threat evaluation is done during every scan. However, you can choose to manually evaluate the threats.

1. Make sure the Enable Feed toggle is in the On position with the Feed Source you want to use.
2. Click Evaluate under the Evaluate Threat column. The threats are displayed below in the Evaluated Threats table, along with the name and family of the threat, the risk rating of the threat, time and date of evaluation, and the number of hosts that are affected by the threat.
3. Click Info to view details about the threat.
 - Click **More** to drill down into the details such as the system details, and the probe details such as the file path, file name, hive, program name, etc. Click the back arrow to return to the details page.
 - Click the value under Hosts to see the names of the affected devices. Click the name of a host to view the vulnerability, compliance, and hardware and software details of that particular device in a new page.
 - Click **Submit** to submit the details to the Saner agents.
 - Click **Edit** to modify the query you want to submit to the agents.

Build your own Detection and Response

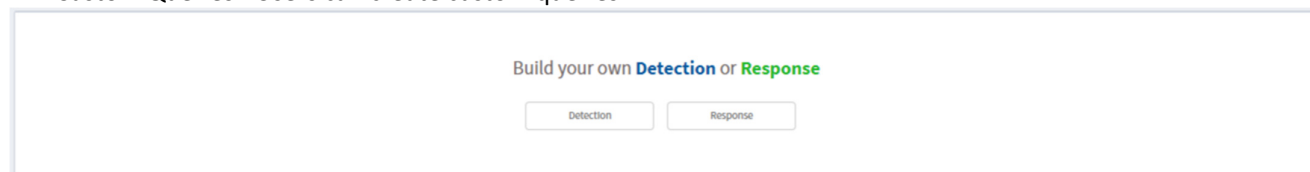
SanerNow helps you write custom detection scripts or scripts to respond to threats through its query module.

A query is a request for information from a database or live data from endpoints where the SanerNow agent is installed. SanerNow supports natural language-based queries, related to processes, services, users, registry, network, and device configurations on the endpoint. The SanerNow platform's metadata model makes it easy to search using unstructured natural language-based queries. SanerNow is fully compliant with well-established standards, such as SCAP, STIX/TAXII,

Query results are fetched in microseconds to help make quick decisions around endpoint activities. Complex queries can be created, or multiple queries can be cascaded with AND and OR combinations. The scalable architecture of SanerNow allows responses to IoCs in seconds without impacting the network or systems.

Queries are categorized into two types:

1. Default Queries - The SanerNow solution provides default queries that can fetch information such as anti-virus information, hosts that have disabled the firewall, hosts that have disabled Bit locker protection, etc.
2. Custom Queries - Users can create custom queries.



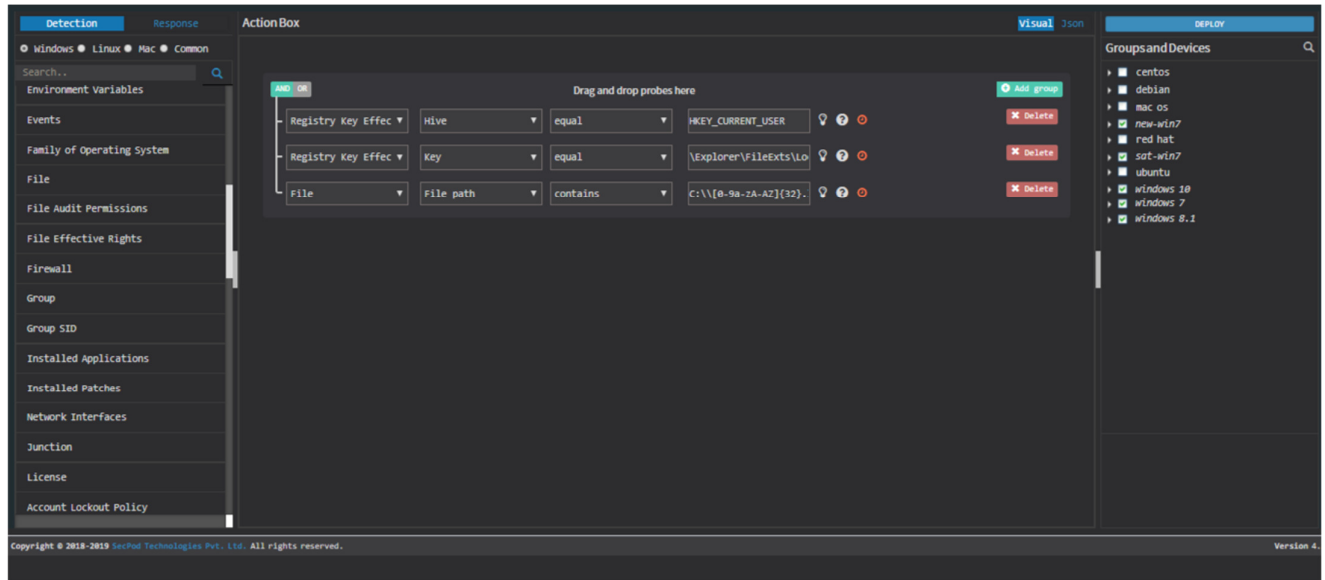
To create a custom query, click the Detection or Response button. A query contains two options:

- Add Rule, to select supported probes. Multiple rules can be selected with AND or OR operations.
- Add Group, to join rules based on conditions. Multiple rules can be joined into one group.

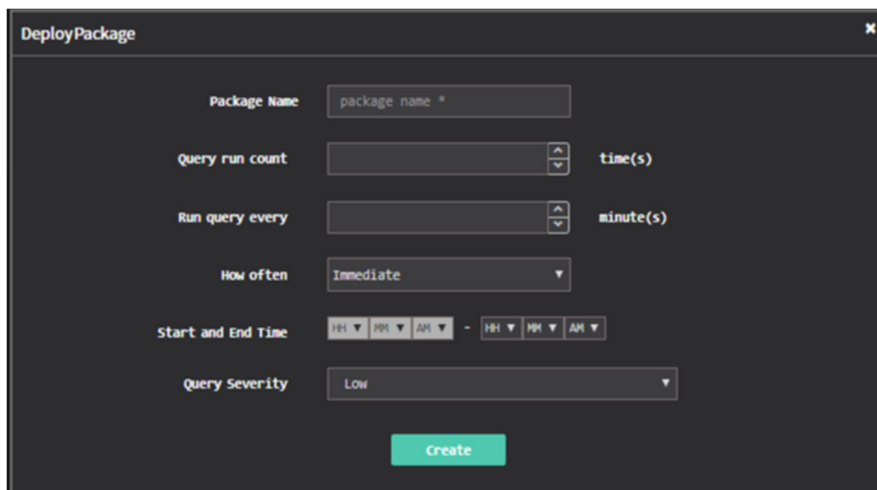
The Run option displays the query results fetched from the database. The Edit and Delete buttons allow you to edit or delete the queries.

To create a custom query for threat detection

1. Click Detection in the Build your own detection and response pane. The query building page is displayed, with a drag and drop library of probes.
2. Filter the probes according to the operating system for which you want to write a query.
3. For example, to check for Locky using multiple rules, drag and drop Registry Key Effective Rights probes into the Action Box pane as shown in the example below. Drag and drop Hive and Key as the parameters. Add a file and the file path.



4. Select the devices and groups you want to query. Click Deploy. The Deploy Package dialog is displayed.



- Specify a package name, the number of times you want to run the query, and the intervals at which you want to run it.
- Specify when you want to run the query – immediately, daily, weekly, monthly or a specific date. Specify the time, and the corresponding days of the week, days of the month or a date.
- Assign a severity of low, medium, high or critical to the query. Click Create.

The figure displays a query with multiple rules to check for Locky malware. Once the query is created or updated it

displays the result in real-time.

After the task is created, SanerNow searches in the local database of system reports. To retrieve the report click Submit. Clicking Submit sends the queries to the Saner Agent to fetch the current data.

Detection Summary

This pane shows a list of the query, the affected hosts, and the risk severity.

Query	Risk	Hosts
Antivirus Information - Windows	<div></div>	23
Applications with Unknown Publisher - Lin...	<div></div>	5
Applications with Unknown Publisher - Mac	<div></div>	2
Disk - Windows	<div></div>	50
DPKG Package - Linux	<div></div>	8

- Click the value under Hosts to see the names of the affected devices. Click the name of a host to view the hardware and software details of that particular device, and the vulnerability, compliance, patch, endpoint details in a new page. Go to the Endpoint Threat Detection tab to view all the EDR details related to the host.
- Click **the Query name** to drill down into the details such as the system details, and the probe details such as the file path, file name, hive, program name, etc. Click the back arrow to return to the details page.
 - Click Submit to submit the query to the Saner agents.
 - Click Edit to modify the query you want to submit to the agents.
- Click the Expand icon to modify the query, run it, or delete the scheduled detection job.

</

Response Summary

This pane shows a list of all the response scripts written to prevent, stop, or cleanup malware, the date on which it was run, the description or purpose for which it was created, and the status of the job. Click the Expand icon to delete the scheduled response job, to edit the description or view the code.

Name	Type	Date	Status
bk-addentry	network	2018-04-13.07:49:34(UTC+0...	Completed
bk-blockserver	network	2018-04-03.12:26:30(UTC+0...	Completed
bk-cleartempfiles	systemcleanup	2018-03-29.06:32:46(UTC+0...	Completed
bk-fbblock	network	2018-03-28.15:44:58(UTC+0...	Completed
bk-irdebian	network	2018-04-03.13:17:55(UTC+0...	Completed

Name	Type	Description	Date	Status	Edit
bk-addentry	Network	testing	2018-04-13.07:49:34(UTC+0...	Completed	
bk-block domain	Network	testing	2018-03-28.15:42:48(UTC+0...	Completed 0 out of 1	
bk-blockserver	Network	oldste	2018-04-03.12:26:30(UTC+0...	Completed	
bk-cleartempfiles	Systemcleanup	testing	2018-03-29.06:32:46(UTC+0...	Completed	
bk-fbblock	Network	testing	2018-03-28.15:44:58(UTC+0...	Completed	
bk-irdebian	Network	test	2018-04-03.13:17:55(UTC+0...	Completed	
bk-sethostname	System	testing	2018-04-03.13:37:58(UTC+0...	Completed	
bk-test0-post	Registrycleanup	test	2018-03-27.11:55:07(UTC+0...	Completed	
Block-domain	Network	test	2018-04-05.06:32:19(UTC+0...	Completed	
block-domain	Network	test	2018-03-27.12:46:12(UTC+0...	Completed	
clear-temp	Systemcleanup	win	2018-03-29.06:41:34(UTC+0...	Completed	

Setting Alerts for Endpoint Detection and Response

To act proactively when there is an indication of threat, or to act quickly to minimize the spread of an attack in progress, you can set alerts.

To Set Alerts for Endpoint Detection and Response

1. Click Alerts > Endpoint Detection and Response.
2. Set the subscription status to On.
3. Specify an email address to which you want the alerts sent.
4. Specify when you want the alerts sent:
 - Threats (Indicators of Compromise) - You can choose to receive alerts for all threats levels, critical threats, high and critical threats, and medium, high and critical threats.
 - IoA (Indicators of Attacks) – You can choose to receive alerts for all indicators of attack, critical attacks, high and critical attacks, or medium, high and critical attacks.
 - Query – You can choose to receive alerts for all queries that are executed on the endpoints, or for custom queries. If you select custom, you must specify the custom values for which you wish to receive alerts.
 - Response fields – You can choose to receive alerts when actions on the endpoints pass, fail, or for a custom condition or for all responses.
5. Click Update to complete.

The screenshot shows the SanerNow web interface. The top navigation bar is green with the 'sanernow' logo on the left and the user 'shobana' on the right. Below the navigation bar, there's a breadcrumb trail: Alerts > Vulnerability Management > Compliance Management > Endpoint Detection & Response > Endpoint Management > Patch Management > Asset Management. The 'Endpoint Detection & Response' tab is selected. The main content area is titled 'Alerts' and contains the following configuration options:

- Subscription status:** A dropdown menu set to 'OFF'.
- Send to E-mail*:** A text input field containing 'rsmitha@secpod.com'.
- Detection*:**
 - Threats (Indicator of Compromise):**
 - ☒ Critical threats
 - ☐ All threats
 - ☐ Medium, High and Critical threats
 - ☐ High and Critical threats
 - IoA (Indicator of Attack):**
 - ☒ All indicators of attack
 - ☐ Medium, High and Critical indicators of attack
 - ☐ High and Critical indicators of attack
 - ☐ Critical indicators of attack
 - Query Detection:**
 - ☒ All queries
 - ☐ Custom
- Response*:**
 - ☒ All failure actions
 - ☐ Custom
 - ☒ All successful actions
 - ☐ All actions

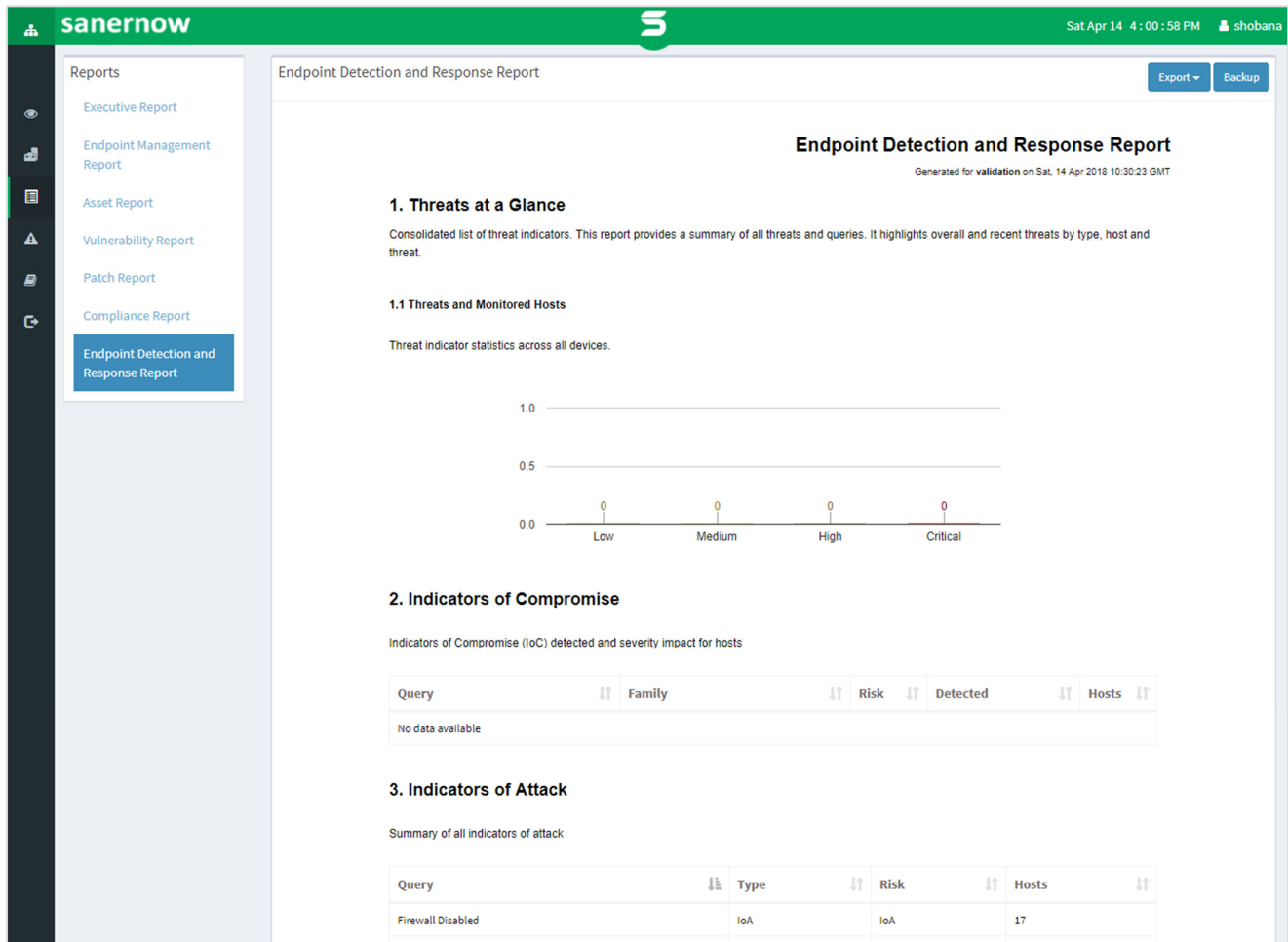
An 'Update' button is located at the bottom right of the configuration area. The footer of the page contains the copyright notice 'Copyright © 2018-2019 SecPod Technologies Pvt. Ltd. All rights reserved.' and the version number 'Version 4.0'.

Endpoint Detection and Response Reports

Endpoint Detection and Response Reports provide a bird's eye-view of the overall threats and the monitored hosts, the specific indicators of attack and compromise, and a summary of the detection and response queries.

To Generate the Endpoint Detection and Response Report

- Click Reports > Endpoint Detection and Response Report.



To export the report to a PDF

Click Export > PDF

To export the report and send it via email:

1. Click Export > Email.
2. Specify the email addresses.

To Back Up Reports

The backup settings under Reports allow IT administrators to obtain a backup report showing the history of threats. The backup time should be scheduled. The backup report can be scheduled to run automatically daily or weekly.

To configure backup settings for reports:

1. Click **Backup**.
2. Specify the frequency of backup in the **How Often** drop-down. You can back up reports daily, or weekly. If you choose weekly, you can specify the days.
3. Specify the number of days that a backup should be maintained in the **Keep Only the Latest** box. Files older than the specified value will be deleted. You can maintain backups for a maximum of 30 days.
4. Specify the **Backup Time**, that is, the time when SanerNow will create an archive of the report. Specify **Email** addresses.

5. Click **Save**.

About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. Founded in 2008 and headquartered in Bangalore with operations in USA, the company provides computer security software for proactively managing risks and threats to endpoint computers.

Contact Us

Web: www.secpod.com

Tel: +91-80-4121 4020 | +1-918-625-3023

Email: info@secpod.com