indeni

Evaluating Indeni

A Hands-On Guide

Evaluating Indeni

Overview

Indeni is a Security Infrastructure Automation platform (SIA). SIA automates the detection and triage of infrastructure issues in security devices. The core components of SIA include:

- Collecting performance and configuration data from physical and virtual security devices.
- Automatically performing tasks on behalf of administrators.
- Providing automation elements such as rules and scripts out of the box.
- Connecting with existing ticketing, monitoring, and email systems.
- Using a system of open APIs or development platforms for integration purposes.

Indeni builds on core SIA concepts to provide:

- Detection of issues that have the potential to cause outages, based on current system configuration and state.
- Validation of alignment with best practices, based on vendor recommendations and real-world expert experiences.
- Automated root cause diagnosis for select issues.
- Recommended remediation for every issue.

Install Requirements

There are two main elements in an Indeni evaluation:

1. Hosting the Indeni VM
2. Persistent connection to Security infrastructure devices (e.g. firewalls, load balancers)

Indeni VM

System Requirements

System requirements vary based on the test environment. Here are the three most typical test environments, with their respective requirements and relevant notes.

Lab Evaluation

VM running 24x7 on a shared VM server in a lab with 5-10 security infrastructure devices.

- RAM: 6GB
- Storage: 180GB
- CPU cores: 4

Minimum

VM running occasionally on a VM player on a laptop to detect issues in a lab with 1-5 devices.

- RAM: 4GB
- Storage: 150GB
- CPU cores: 2

Notes on Minimum install network configuration:

When running the Indeni VM on a laptop (or similar general use system), it is Best Practice to use one of the following network configurations for the VM:

- 1 network interface in “bridged” mode, with the Indeni VM left with its default configuration of a single interface with DHCP address.
    - This configuration provides both outbound access from the Indeni VM to the monitored devices, and inbound access from the user’s web browser to the Indeni UI, using an IP address for the VM, separate from the host.
    - This configuration will work in most environments, except those which have restrictions on IP address assignment and/or VM network access.
- 2 network interfaces
    - 1 interface in NAT mode to provide access from the Indeni VM to the monitored devices
    - 1 interface in Host-only mode to provide access from the laptop to the Indeni UI
    - This configuration is recommended only when the single-interface configuration will not function in the test environment. Features on VM players vary, and multi-interface configurations may require additional setup for local virtual networks.

Production

Either VM or dedicated hardware, running 24x7, with the following requirements:

Devices	vCores	RAM	Storage	Speed
10-30	8	8GB	180GB	3000 IOPS

31-100	16	16GB	180GB	3000 IOPS
101-300	32	64GB	400GB	6000 IOPS
301-1000	64	96GB	400GB	8000 IOPS

For the latest information, please see the latest Indeni datasheet.

Network interface requirements

1. A network interface and IP address either with access to or on the security infrastructure management subnet.
    - Address may be dynamic (DHCP), although static IP is recommended to comply with the Best Practice configuration for devices of an ACL whitelist of authorized client IP addresses for the device's management interface.
    - This interface requires access to the following ports on devices (section 2.2):

DEVICE VENDOR	SSH PORT	HTTP PORT
Blue Coat	22	8082
Check Point	22	x
Cisco	22	x
F5	22	443
FireEye	22	x
Fortinet	22	x
Gigamon	22	x
Juniper	22	x
Palo Alto Networks	22	443
Radware	x	443
Symantec	22	x

2. Optionally a second interface and IP address for user access to the web UI.
    - A static IP address is not required, although it is recommended to simplify user access to the UI.

It is Best Practice to provide the Indeni VM with the following access:

- An NTP server (port 123)
- A DNS server (port 53)
- The Indeni Proactive Support Service at service.indeni-ops.com:80 and service.indeni-ops.com:443

Security Infrastructure Devices

An Indeni evaluation requires at least one security infrastructure device to connect for automated monitoring. If no devices are available, it is recommended to try the Indeni Test Drive, a cloud-hosted instance connected to devices in Indeni's test lab. In the Test Drive environment, users will not be able to connect to their own devices, but will be able to explore a live Indeni instance.

Device configuration features

For comprehensive testing, the Indeni evaluation should include:

1. At least one set of HA peered devices, so Indeni can detect HA failover unreadiness.
2. Vendor-provided device manager, both to provide uptime assurance for that management system, and to accelerate adding devices to Indeni.

Example Security Infrastructure devices

Firewalls

- Check Point SG and SMS
- Cisco ASA
- Fortinet Fortigate
- Juniper SRX
- Palo Alto Networks NGFW and Panorama

Load Balancers

- F5 BIG-IP
- Radware Alteon

Content Analysis

- FireEye NX
- Gigamon GigaVUE TA and HC
- Symantec Blue Coat ProxySG and CAS

Quick Start

This is a quick-start guide, with references to our user guide: https://indeni.com/docs/7-0-user-guide

Preparation

Steps:

1. Determine the resource requirements on your hypervisor according to the system requirements listed above
2. Determine which security infrastructure devices you will include in your evaluation based on the list of example devices above.
3. For each device, assure that its management interface IP address is reachable from the hypervisor where the Indeni VM will be installed. For a list of which ports are required per vendor, please see the table above.
4. For each device, assure that there is a service account which Indeni will use to connect, query, and run diagnostics. (section 2.1)

Installation

Steps (with links to the user guide):

1. Import the Indeni OVA file into your hypervisor (section 1.2)
2. The following steps will be run on the Indeni VM console:
    a. Boot the Indeni VM, connect to the console, and log in with Username: ***indeni*** and Password: ***indeni4it***
    b. The Indeni VM defaults to using DHCP for its IP address(es). To set a static IP address, use the initial setup wizard on the CLI. The setup wizard can be run at any later time by running the CLI command ***isetup***
3. The following steps will be run via the Indeni GUI via web browser:
    a. Connect to the Indeni GUI at https://[VM_eth0_address]/
    b. Since the Indeni VM uses a self-signed cert, your browser will likely display an error that the site identity cannot be authenticated. This is a normal and expected side-effect of using TLS with an IP address disconnected from PKI. Follow the steps for your browser to bypass the warning.

c. Login with Username: ***admin*** and Password: ***admin123!***

    d. (Optional but highly recommended) Configure SMTP integration (section 6)
    e. Add a device credential set to Indeni. (section 5.1)
    f. Add the device(s) to Indeni. (section 5.2)

Optional Configuration

See section 6 for integration with other monitoring and alerting systems:

- **SMTP**: email issue notifications and report exports
- **SNMP**: send traps for issue notification
- **Syslog**: stream issue notifications as log entries
- **LDAP**: external validation of user authentication and permissions

Sample Tests

Criteria

A strong SIA solution will:

- Inspect devices without needing to manually run commands
- Uncover issues missed by SNMP
- Get visibility of issues that would impact high-availability
- Know if a failover is about to happen
- Ensue we are following best practices in how my devices are deployed
- Perform first level triage without human intervention

These tests are provided as suggestions based on the following criteria:

- Straightforward setup
- Simple steps with quick results
- Valuable in production

Indeni suggests the following criteria to judge value in your environment:

- Detection: does your existing monitoring find this kind of event?
- Impact: what would the impact be to your environment if this event weren't detected?
- Remediation: using a different solution, how long would it take to determine and implement the resolution?
- Overhead: how much effort would it take to set up and maintain a different solution to get similar results?

Note:

For each of the tests which results in issue detection (and, where applicable, Auto-Triage diagnosis), additional information on the issue is available by clicking "Overview" under the issue summary in the right-column pane.

Tests

Single device

Test: Detect device reboot

Recommended devices: any, with additional features on Check Point, Palo Alto Networks
Summary: Indeni will detect that a device has rebooted, and, for certain devices*, diagnose the cause of the reboot.
Time: 5-10 minutes
Steps:

1. Connect to the device with an administrator-level account and use one of the following methods to cause a reboot.
    a. Reboot Type 1: Issue a reboot command on the unit
    b. Reboot Type 2: Overload a system/kernel process
    c. Reboot Type 3: Pull the Plug

Result:
Within 1-2 minutes, Indeni will list the alert along with the resulting triaging showcasing the method that was used.

Test: Detect device hardware redundancy failure

Recommended devices: device with multiple power supplies and/or redundant disks
Summary: Indeni will detect when single-system hardware redundancy features fail.
Time: 5-25 minutes
Steps:

1. Cause one of the following hardware redundancy failures.
    a. If the device has redundant power supplies, unplug one.
    b. If the device has redundant disks, remove one.
        i. Please follow the vendor recommendations for your device, e.g. only remove a drive while the device is powered up if the device supports hot-swapping of drives.
        ii. Note that, after the drive is re-inserted, your storage array may go into “degraded” mode while the drive contents are checked and re-synced with the rest of the array.

Result:
Within 2-20 minutes, the hardware failure will be detected and reported. To reduce the impact on the device from issue detection, the frequency varies per vendor, between 2 minutes on Check Point and 20 minutes on Fortinet.

Infrastructure connectivity

Test: Detect infrastructure service connectivity failure

Recommended devices: any, with the following additional capabilities:

- Fortinet: detect connectivity loss to Fortianalyzer and Fortimanager
- Palo Alto Network: Automatically diagnose the cause of the problem for loss of connectivity to DNS and NTP

Summary: Indeni will detect when the security infrastructure device loses connectivity to another critical part of the network infrastructure.

Time: 5 minutes to set up, detection time 5-60 minutes (does not require human presence)

Steps:

1. Configure the device to connect to at least one of the following services:
    a. DNS
    b. NTP
    c. Radius
    d. Vendor management tool
2. Block the connection between the device and the service.

Result:

Indeni detects the loss of connectivity, and for DNS and NTP on some devices, provides additional diagnosis of the failure cause. Note that organizations that rely on vendor management tools may misread a connection failure as a firewall outage.

Test: Detect infrastructure routing connectivity failure

Recommended devices:

- Blue Coat ProxySG (Static)
- Check Point (Static, BGP, OSPF)
- Juniper SRX (Static, BGP, OSPF)
- Palo Alto Networks (Static, BGP)
- Radware Alteon (BGP)

Summary: Indeni will detect when routing peers are not available, either via dynamic or static protocols.

Time: 5-15 minutes

Steps:

1. Set a static route or a neighbor or peering relationship to another router
2. Disconnect the next-hop router. Note that blocking IP connectivity is insufficient, as the static connection relies on L2 resolution, and OSPF relies on multicast.

Result:

Indeni detects the loss of connectivity to the router. While dynamic routing will usually provide an alternate path to a destination, that alternate next hop may be on a different interface, which, depending on the vendor device and configuration, may be in a different zone, thus covered under a different part of the security policy, and therefore likely to be blocked.

HA peers

Test: Detect HA sync errors

Summary: Indeni will detect issues in the connection between HA devices or the failure of a passive device

Time: 5-10 minutes

Steps:

1. Connect to the passive device in an HA pair and cause a specific failure. While Indeni will detect each of these failure types, it is recommended that the first time you run this test, you only cause a single failure type, so you can more easily validate the correlation between your action and Indeni's discovery of the issue.
    a. HA Failure Type 1: Remove Sync Cable between Active & Passive
    b. HA Failure Type 2: Disable Sync Port on Active or Passive
    c. HA Failure Type 3: Reboot Passive Device
    d. HA Failure Type 4: Add rule or modify existing to ignore heartbeat
2. Within 1-2 minutes, Indeni will list the alert along with corresponding information describing the issue and remedy.

Result:

HA sync failure will quickly result in state skew between HA peers, which will cause sessions to be dropped during failover. Extended sync failure may result in configuration skew, which may lead to unexpected traffic handling in the event of failover.

Test: Detect HA configuration skew

Summary: Indeni will detect configuration drift between cluster members to prevent issues, failures or outages when a failover occurs.

Time: 10-20 minutes

Steps:

1. Connect to either Active or Passive Device and change part of the configuration. This can be adding a route from a non-existent source or other non-destructive change that is not mirrored in its cluster pair. Note that, while most vendors sync most configuration elements, there are elements which are not synced. Examples of this include:
    a. Static routes
    b. DNS or NTP servers
2. Within 1-2 minutes, Indeni will list the alert along with corresponding information describing the issue including the specific lines that are different between the devices.

Result:

HA configuration skew will result in non-identical handling of traffic in the event of failover. For vendors which have configuration elements that are not synchronized between peers, there is also not detection of non-synchronization in the vendor's management tool.

Configuration Management and Compliance

Test: Detect configuration skew

Summary: Indeni will detect configuration drift between device configuration and a designated Golden Master configuration.

Time: 10-20 minutes

Steps:

1. Connect to one of your active devices and take a number of lines (usually three to five) that you can easily change and copy them to a text file.
2. On the Indeni instance, go to Alerts -> Indeni Rules. In there you will find the Configuration Mismatch rule.
3. Click to the Configurations tab of the Configuration Mismatch rule and click “+New” to create a new configuration.
4. Paste the lines into the box and select the box you’d like to check from the Devices menu.
5. Change the configuration on the box and watch as Indeni shows you what is different on that box from what you input.

Result:

As the configuration of a device changes away from the snippets you provide, Indeni will notify you about the changes. Users can apply these configurations to multiple devices by including wildcards to indicate expected differences between devices.

Test: Configuration backup

Summary: Indeni can take periodic backups of device configuration.

Time: 5 minutes to set up

Steps:

1. Click on the Devices icon in the left nav bar 
2. Choose a device. For help in choosing a device, select the device in the list, and click “More Device Info” at the bottom of the right-side device info pane.
3. Select the “Backup” tab.
4. Click the “+” icon at the top of the list.
5. Complete the configuration for the scheduled backup:
    a. Recurrence rule
    b. Device selection, by device and/or by label
    c. Click “Save”
6. After a backup has run, information about the most recent backup for each device will be listed in the device info pane.
7. To retrieve backup for a device:
    a. View backup results by selecting the Backup from the list on the Backup tab.
    b. In the top-right corner, click “Output”. Note that it may take a few seconds for the page to draw over the default “No jobs” message.
    c. Click the download icon next to the backup for the device and time you wish to download.

Result:

Indeni can be configured to create periodic backups of device configurations, which it will retain over multiple instances in case recent changes need to be rolled back.

Test: Report of non-compliance

Summary: Indeni can create reports of detected issues, targeted to multiple use cases.
Time: 5+ minutes
Steps:

1. Run any test to ensure that Indeni has discovered issues on at least one device.
2. Click on the Analysis icon in the left nav bar 
3. (Optional) On the Query tab, click “Add New Graph” and select a metric to show a KPI graph. Time range can be adjusted with the timeline on the top, and additional metrics can be added to show KPIs on the same or different devices for the same time range.
4. Click the “Custom Report” tab. In the list, select “+New”. In the right panel, click the “Add Widget” button.
5. In the list of templates, select “Regulatory Compliance and Security Risks”.
6. (Optional) Click “Add Widget” to add another widget, e.g. High Risk Devices.
7. Widget filters can be adjusted using the 3-dot icon menu in the top right corner.
8. Save the Report by clicking the “Save” button.
9. (Optional) set a schedule to generate and export the Report using the “Email Report” icon, available once the Report has been saved.

Result:
Indeni provides report formatted output to visualize its findings, based on common and/or custom use cases. Report generation is rapid, and reports can be exported and scheduled via email.

Conclusion

The purpose of this Guide is to provide a method of evaluating the value of Indeni, yielding useful results in a short period of time, which is consistent with Indeni's goal of reducing the time and effort requirements for teams to operate and maintain security infrastructure equipment. To ensure that your evaluation has actionable results, we encourage you to use similar methodology in comparing our solution to other options, even if that is just your current workflow and toolkit.

For more information about Indeni's Automation Modules used to detect and triage issues, please see our Automation Explorer at https://community.indeni.com/c/knowledge

During your evaluation, you want support from Indeni, feel free to contact us directly at info@indeni.com, or post on our community forum at https://community.indeni.com/

Corporate Headquarters
San Francisco, CA USA
Tel: +1-877-778-8991
Email: info@indeni.com

European Headquarters
Tel Aviv, Israel
Tel: +1-809-494-190
Email: info@indeni.com