# Introduction

## spOT Overview

Standalone, ruggedized

Scan an asset for vulnerabilities before deployment to factory-floor

Built-in Policies – threat intel list of vulnerabilities

Check for vulnerabilities, misconfigurations, sensitive data, credentials, policy violations

Threat Intel – Otorio research team – DB of vulnerabilities -

Generate report, calculate Risk & Compliance Score

Maintain history of scans to build trend analysis

# Setup

Simple setup. Configure details for device to be tested. Connect to device over network port..

## Configure the device to be tested

Name, vendor, IP Address

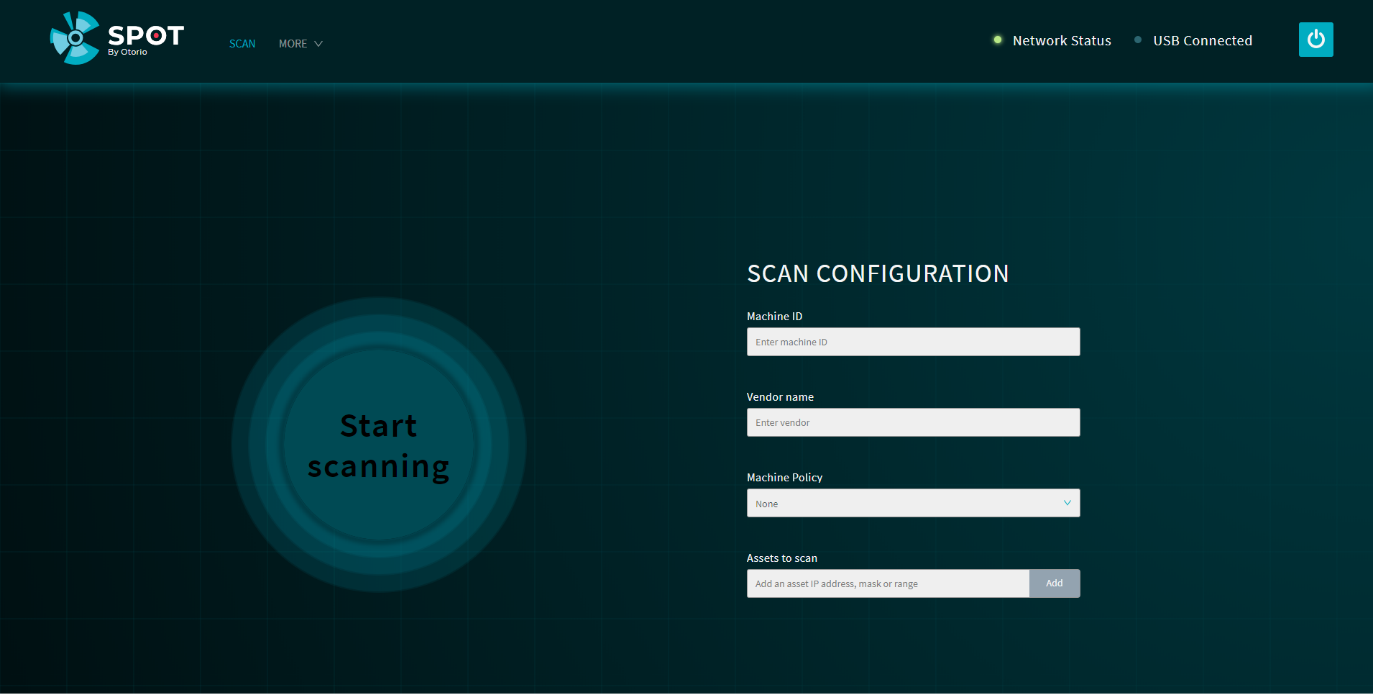
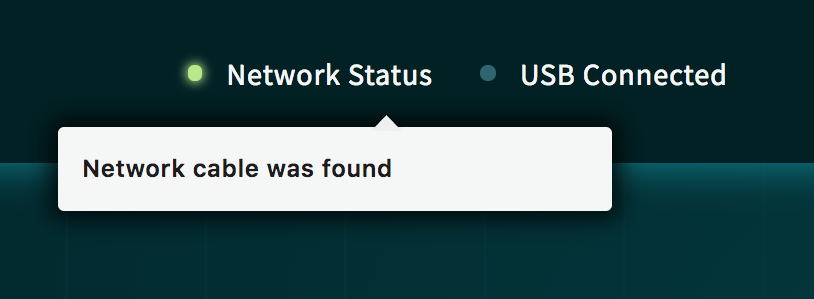


Figure Configure scan

Network status



# Scan

Single, simple operation.

## Start scan

Press Start scanning to start the scan. The scan typically takes a few minutes.

The scan progresses in a series of steps. The status of the scan as it progresses is shown on the screen.

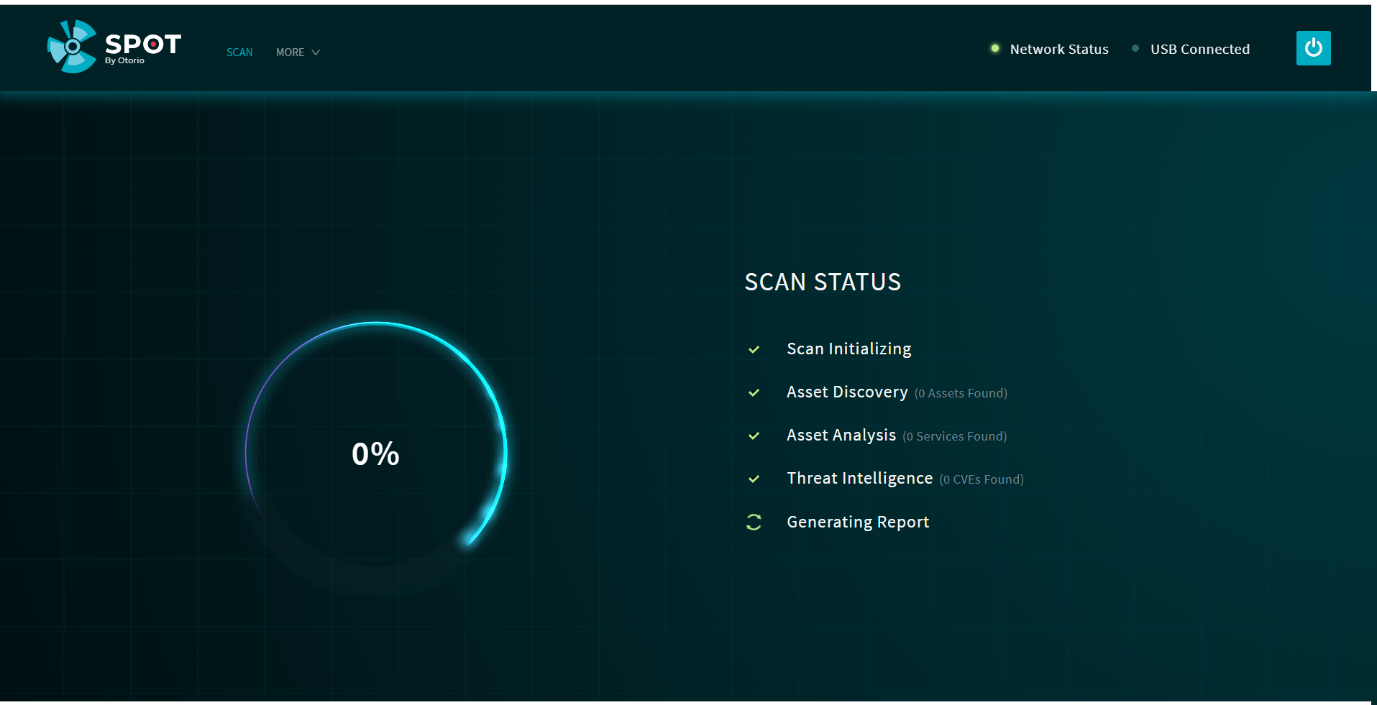


Figure Start scan

Phases of the scan

* Initiation
* Discovery
* Analysis
* Threat Intel
* Report

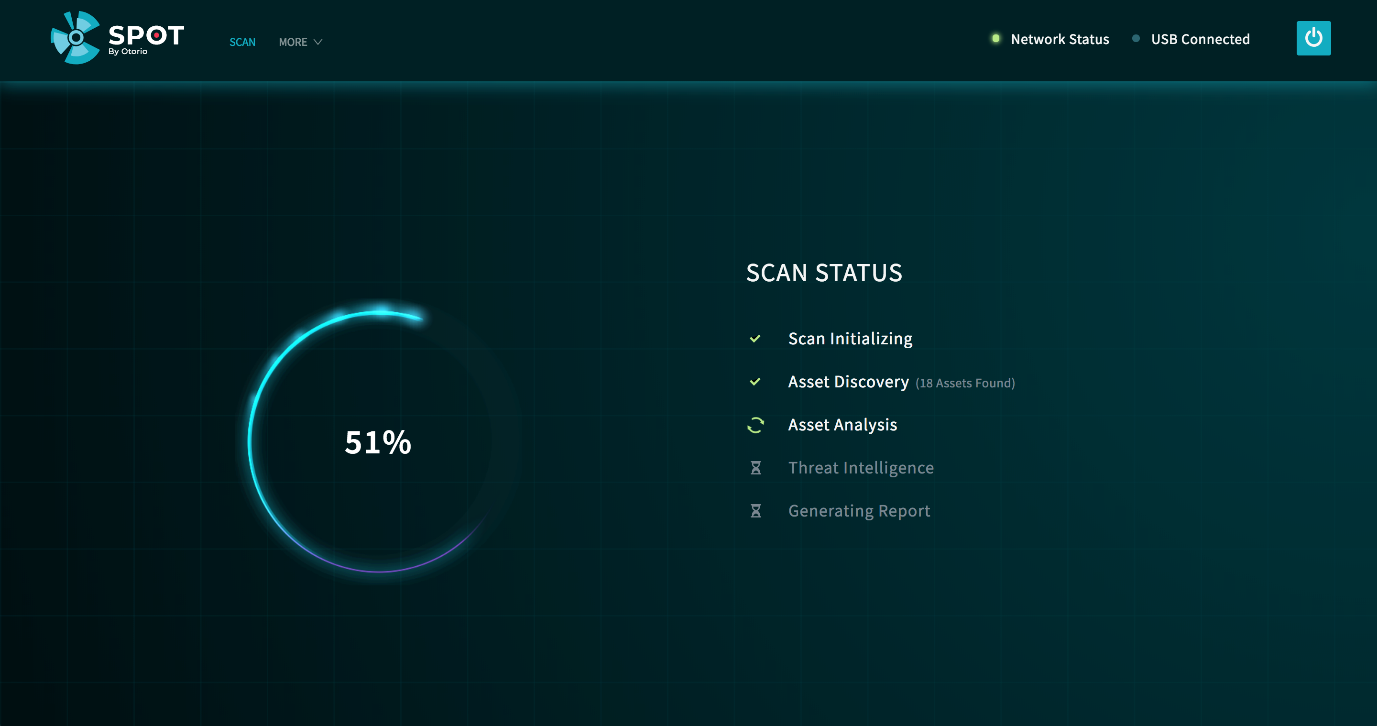


Figure Scan progress

### Asset discovery

### Asset analysis

Check credentials, configurations, policies

### Threat Intel

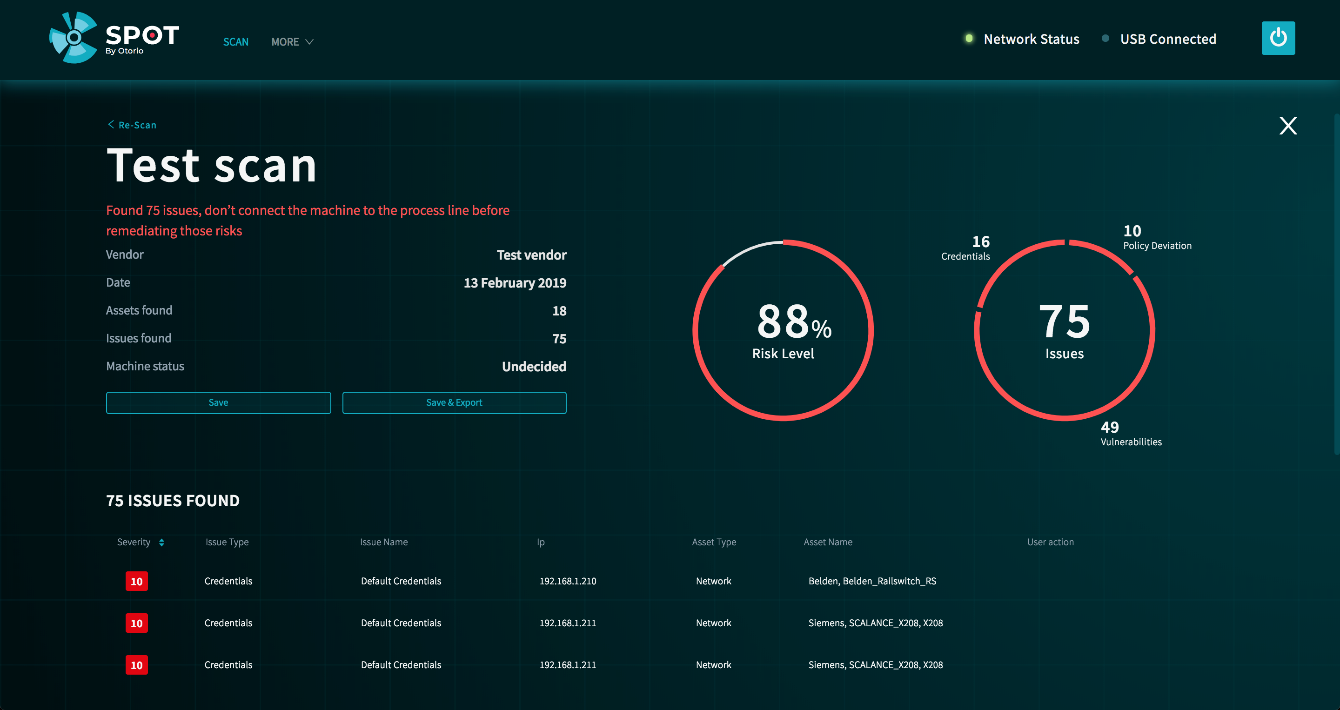
vulnerability assessment

Calculate risk, compliance score

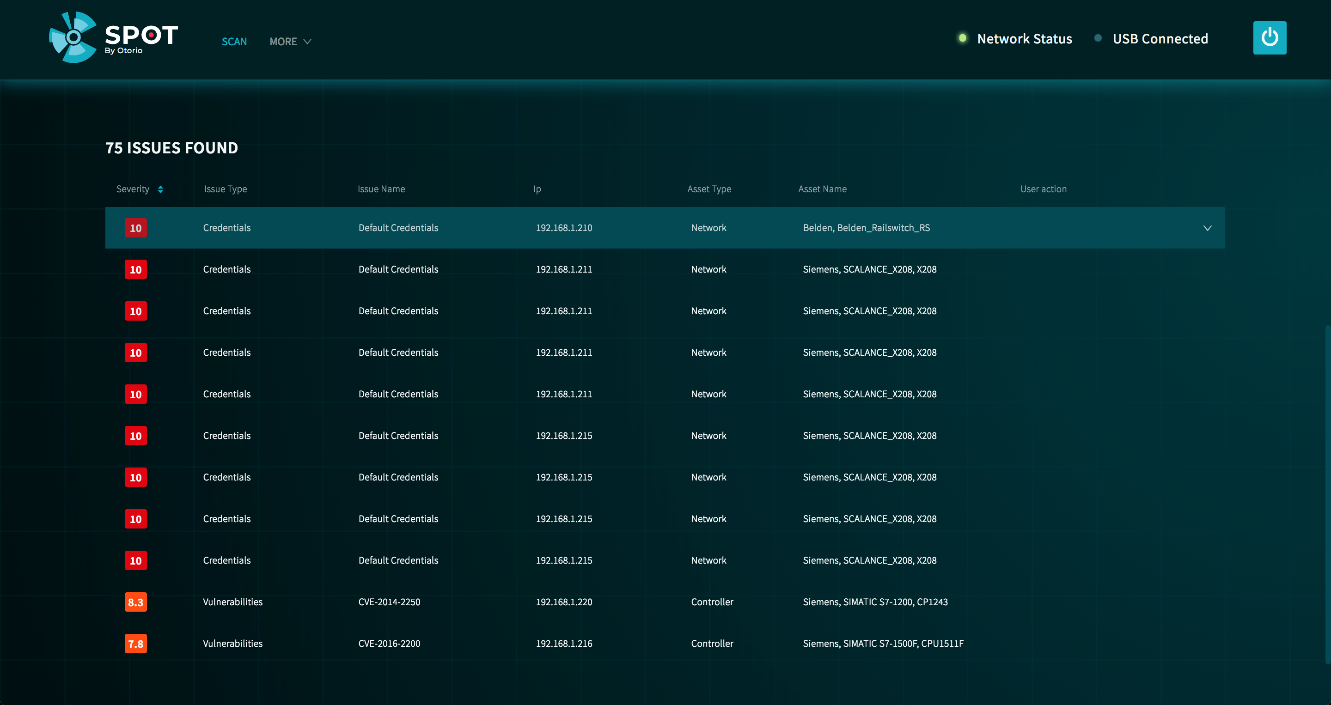
## View scan results

When the scan concludes, press  to view the results. Alternatively, press Re-scan to perform the scan again, with the same configuration.

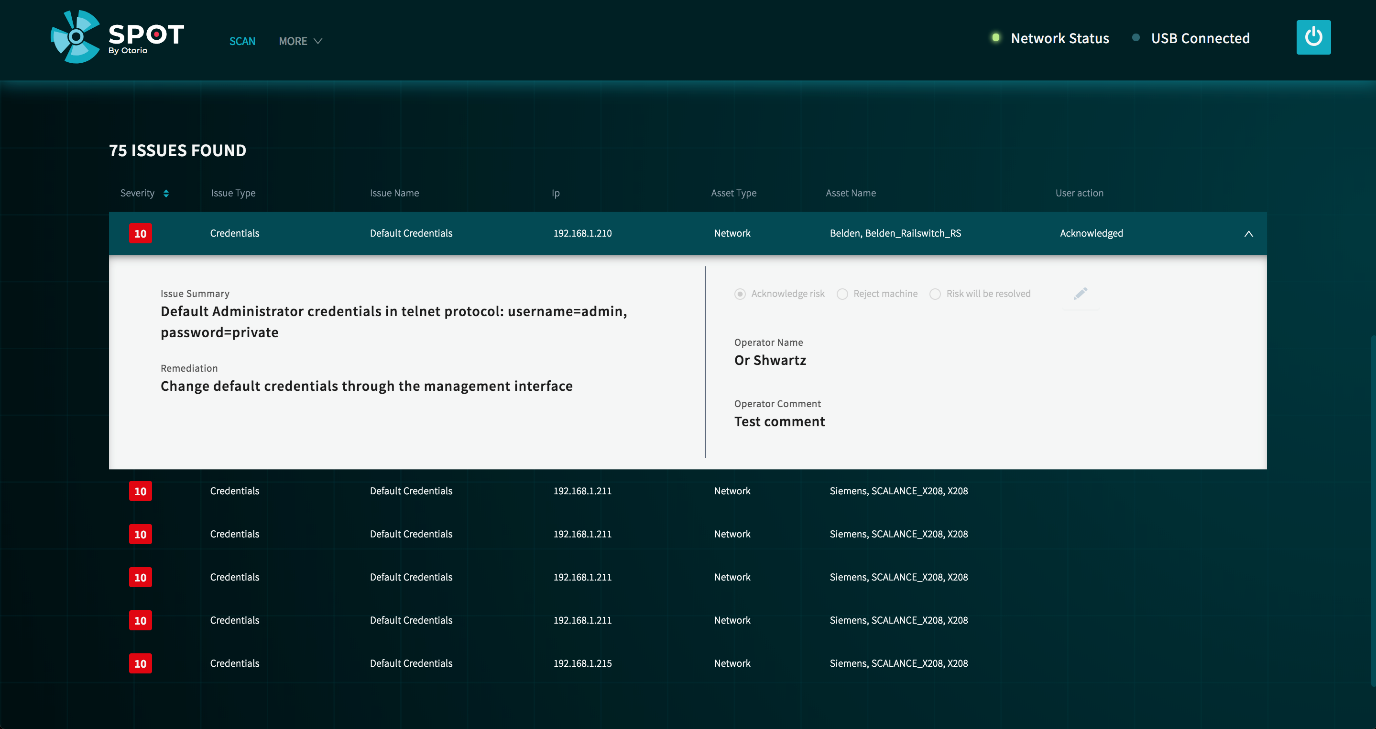
The results are shown on the screen.



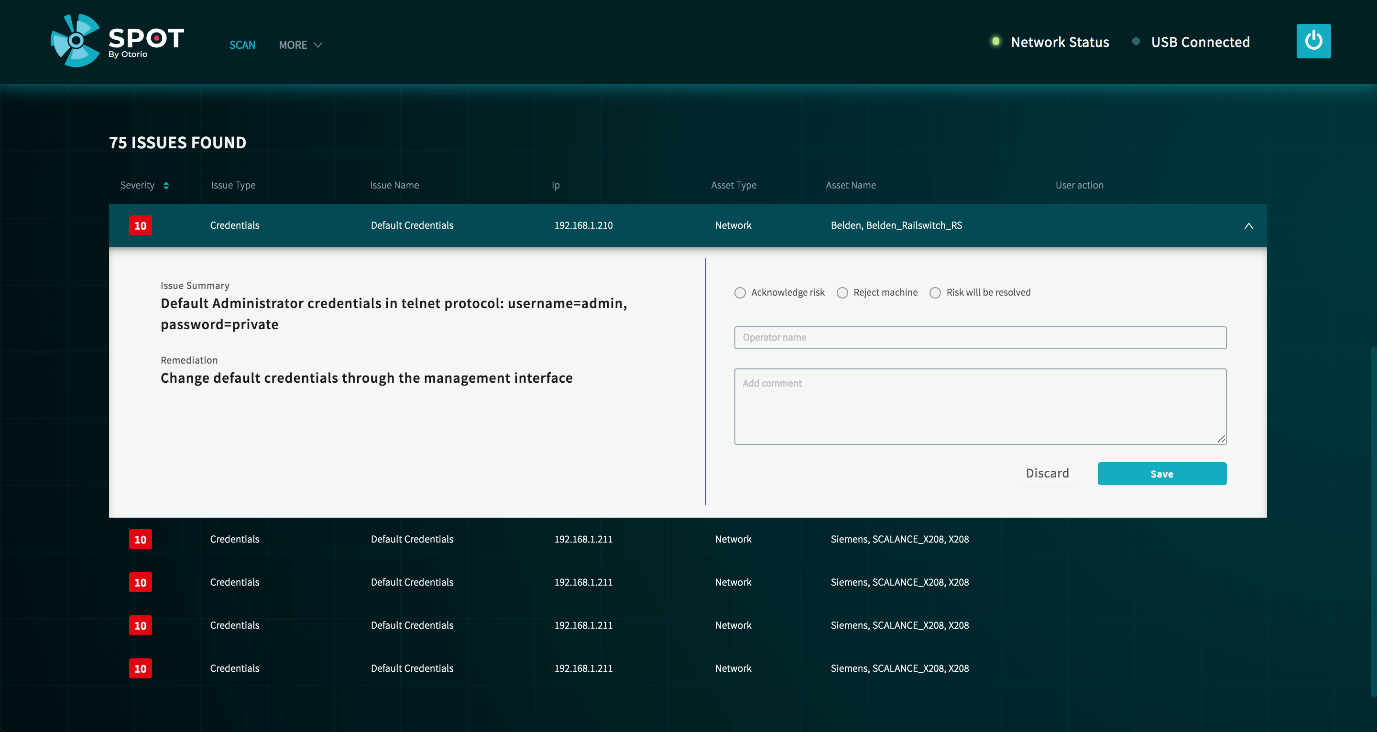
### Scan issues



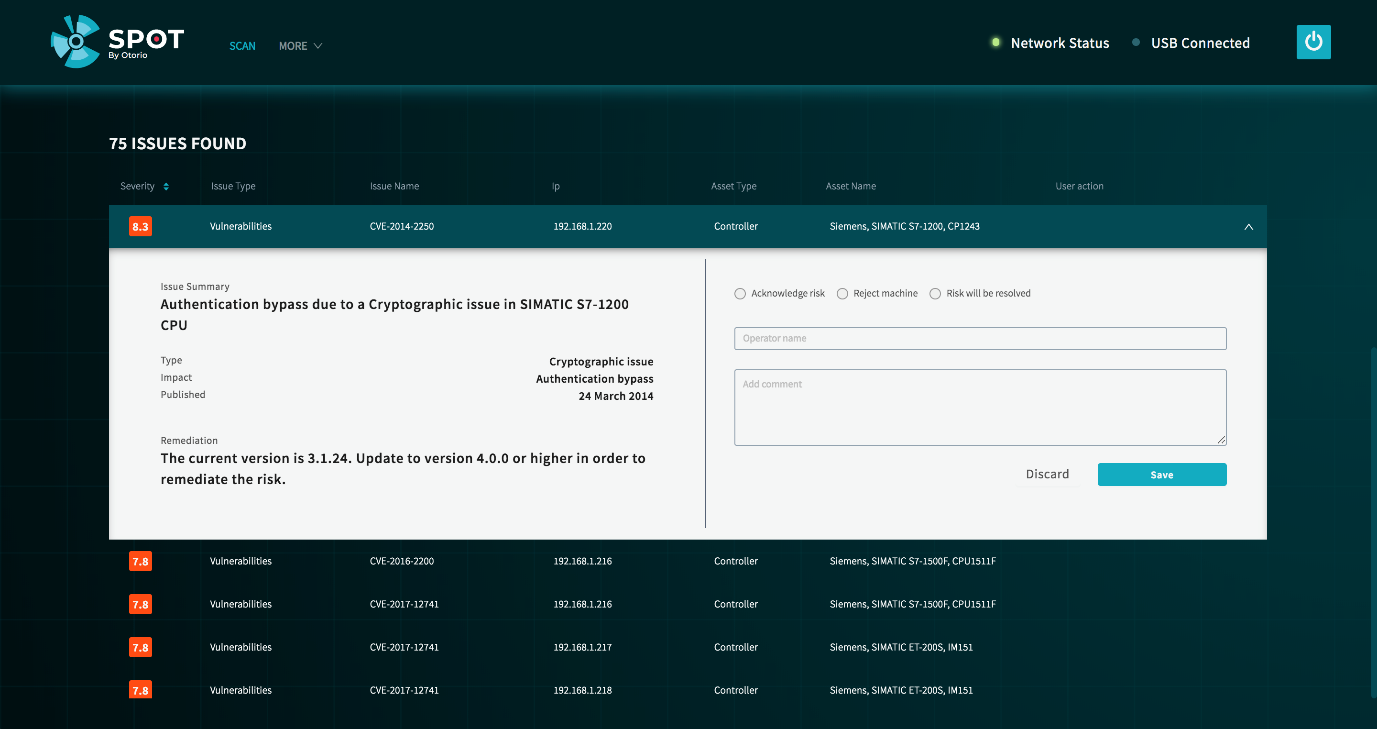
Detail



### Add comments



### Acknowledge an issue



## Save report

## Export report to PDF

# Scan History

## Trends

# Settings

## Network settings

## Analyzers configuration