

NextGen Redesign 2019

Unified Security Metrics needed a facelift. Below are the overview page, and FAQ before and after. (INTERNAL to Cisco)

OVERVIEW BEFORE

The screenshot shows the 'Unified Security Metrics NG' community page on Cisco Employee Communities. The page features a blue header with navigation links: 'Employee Communities', 'Home', 'Communities', 'People', and 'Activities'. Below the header, the community name 'Unified Security Metrics NG' is displayed with '3 Subcommunities'. A navigation bar includes 'Overview', 'Recent Updates', 'Status Updates', 'Members', 'Ask Us Anything (Q&A)', 'Wiki', 'Forums', 'Bookmarks', and 'Metrics'. A secondary bar on the right says 'Stop Following this Community' and 'Community Actions'. The main content area has a large blue graphic with a padlock and circuit patterns. Below the graphic is a paragraph of text: 'The Unified Security Metrics Next Generation (NG) deployment, based on the OpenView Security Risk (OSR) framework, will help you to proactively monitor the vulnerabilities of the network, software, and devices.' Below this text are five buttons: 'Overview' (blue), 'Change Management' (green), 'Training and Resources' (grey), 'About USM Next Gen' (yellow), and 'Support' (orange). At the bottom, there are three sections: 'Ask Us Anything (Q&A)' with a list of questions, 'Rich Content' with text about the OSR framework, and 'Members' with a grid of member avatars.

OVERVIEW AFTER:

Cisco
Employee Communities
Home
Communities ▾
People ▾
Activities

Communities

Overview ▾

Subcommunities ▾

OVERVIEW ...

- ABOUT USM NEXT GEN
- SUPPORT
- TRAINING AND RESOURCES
- FAQ
- SECURITY PULSE with INFOSEC

Members ...

Christian Wil...

Hessel Heer...

...

Unified Security Metrics NG

USM NG OVERVIEW

Unified Security Metrics Next Generation is the successor of the multi-award winning USM program which now offers continuous, prioritized, and risk-based views into the most critical vulnerabilities within the Enterprise.

CURRENT UPDATES AND KNOWN ISSUES	
ISSUE	STATUS
Closed CASPR issues are showing as closed in USM NG. Current CASPR query is returning duplicate items for the same issue.	Work in progress to identify the root cause and resolve the issue.
Tableau -- multiple login issue still unresolved	Working with Tier 2 support, multiple login issue still unresolved.
AVID vulnerabilities showing old application name after the app_name is updated in ESP.	Working with AVID teams respectively to use app sys_id in JIRA issues instead of application name. TIP will then match on app sys_id instead of app name.

RESOLVED ISSUES		
ISSUE	STATUS	RESOLVE DATE
Approved Exceptions via STO exception Tracker not reflected in USM NG reports	Resolved	4/11/19
DAVA vulnerabilities showing old application name after the app_name is updated in ESP.	Resolved. We are now matching on sys_id and application name.	4/2/19
Default impact values for app vulns are set to C1/P1/	Resolved	3/26/19
Open Date and SLA end date for BAVA Certs are being re-set every day making it a rolling	Resolved. The fix has been deployed and the	3/18/19

FAQ BEFORE:

The 'before' was just a word document attached to the community platform that had to be checked in and checked out. I created a page in the community and created jump links for ease of use and editing.

About Unified Security Metrics Next Generation FAQ

What is Unified Security Metrics Next Generation?

A: Unified Security Metrics Next Generation is risk based reporting tool, fully digitized.

USM NG provides daily reports, SLAs that help to prioritize the remediation of the riskiest vulnerabilities.

USM NG is now composed of 2 scores (Application Risk and On Time Closure Score) in addition to Risk Acceptance view to represent the security posture of your service/portfolio.

What is USM Next Generation URL?

A: <https://usm.cisco.com/usm/>

How do I know if USM applies, or will apply, to my service?

A: USM applies to any service that is listed within the IT Service Portfolio.

One of my applications is mapped to the wrong service – what should I do?

A: **Mis** mappings are not uncommon. Be sure you check and validate that your applications are mapped to the correct service in the Application Portfolio before USM pulls the data at the end of a given quarter.

A: There are 5 areas that USM currently measures with respect to IT security metrics, which are briefly described below.

- **Stack Compliance.** Measures TCP/IP stack vulnerabilities with severity levels of 3, 4, and 5, or low, medium and high, respectively, which are identified via **Qualys** scans.
- **Anti-Virus Compliance.** Measures if anti-virus software is installed and if definition files are current.

FAQ AFTER:

The screenshot displays the Cisco Employee Communities interface. The top navigation bar includes the Cisco logo and links for Home, Communities, People, and Activities. The left sidebar features a 'Communities' section with a profile picture and navigation options for Overview and FAQ. Below this are five buttons: ABOUT USM NEXT GEN, SUPPORT, TRAINING AND RESOURCES, F.A.Q., and SECURITY PULSE with INFOSEC. The main content area shows the breadcrumb 'Unified Security Metrics NG > Unified Security Metrics NG FAQ' and a title 'Unified Security Metrics NG FAQ'. The content is organized into several sections: 'What is Unified Security Metrics Next Generation?' with four sub-questions; 'Scoring FAQs' with a bolded introductory sentence and four sub-questions; 'Qualys / Stack Compliance' with one sub-question; 'Anti-Virus Compliance'; 'Infosec Policy Enforcement' with seven sub-questions; and 'BAVA (Baseline Application Vulnerability Assessment)' with five sub-questions.

Communities

Unified Security Metrics NG > Unified Security Metrics NG FAQ

Unified Security Metrics NG FAQ

What is Unified Security Metrics Next Generation?
What is USM Next Generation URL?
How do I know if USM applies, or will apply, to my service?
What gets measured in Unified Security Metrics?

Scoring FAQs
This section provides basic information on questions relating to USM scoring.
What are the scoring definitions for services under USM?
What do the percentages mean for OTC for identified vulnerabilities?
USM NG OTC scores and Risk Score Impact?
How do I find out what the SLA time frame is to remediate and close a reported vulnerability?

Qualys / Stack Compliance
Vulnerabilities were identified through a Qualys scan. How do I remediate these vulnerabilities?

Anti-Virus Compliance

Infosec Policy Enforcement
What is the scope for Policy Enforcement?
What if my application is not applicable for BAVA? Will SCAVA be used for enforcement?
What is the trigger for running a BAVA Scan?
How can I enable BAVA for my application?
How often do I run BAVA scan?
Do I need a new scan for every release, if I have a clean old scan, will that work?
What vulnerabilities are in scope for gating?
Can I deploy if I have an overdue vulnerability?
Can I request an exception?

BAVA (Baseline Application Vulnerability Assessment)
How do I begin the process for a required BAVA or DAVA scan?
I have an application in the app portfolio that will be EOL'd in the next quarter. Do I still need to have BAVA and/or DAVA scans performed?
I need to update the BAVA fields in the Application Portfolio- How can I do this?
If BAVA is certified but still showing up on my report as open-late or open-on time?
I've certified my BAVA/DAVA but I am still seeing open issues...why?