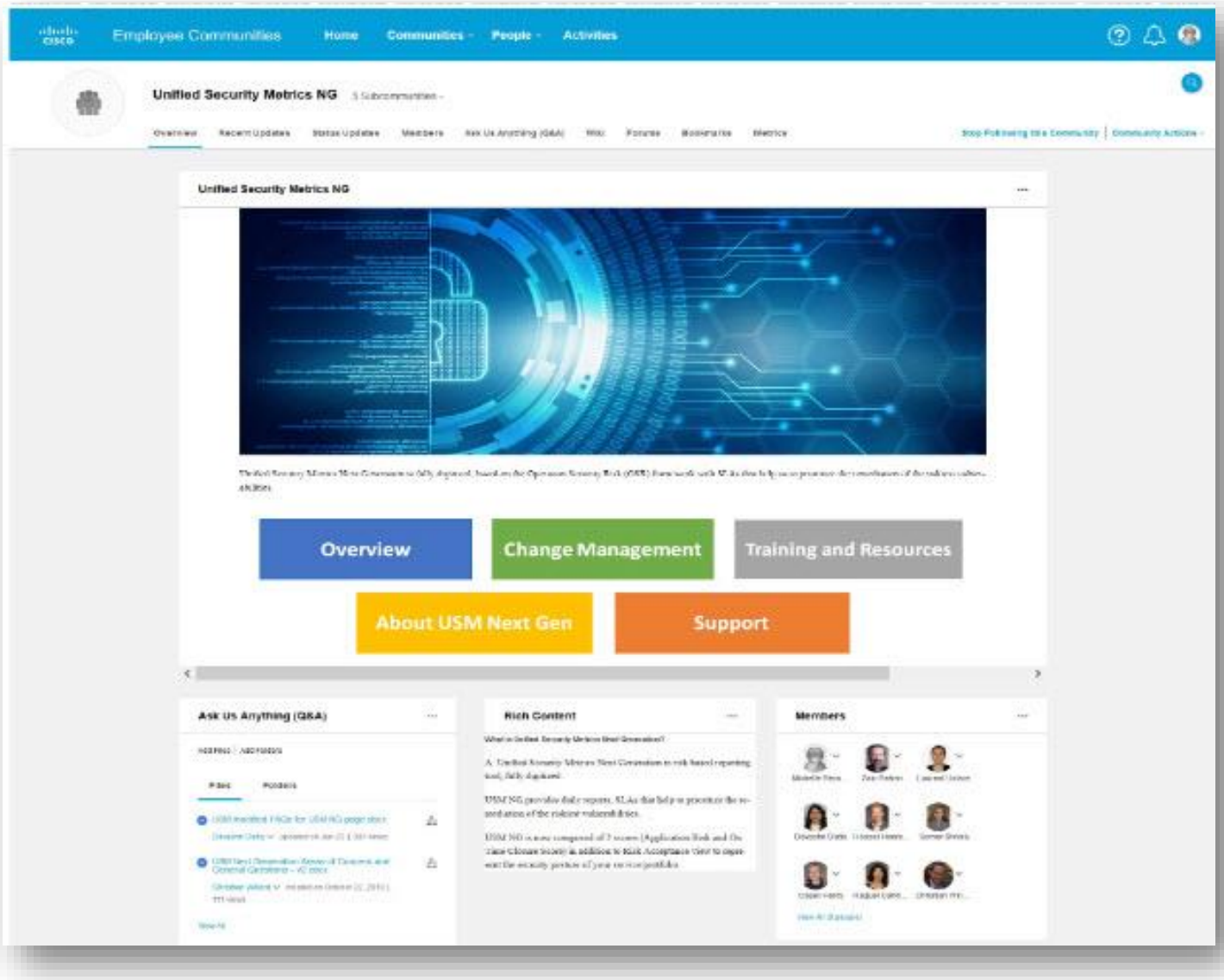
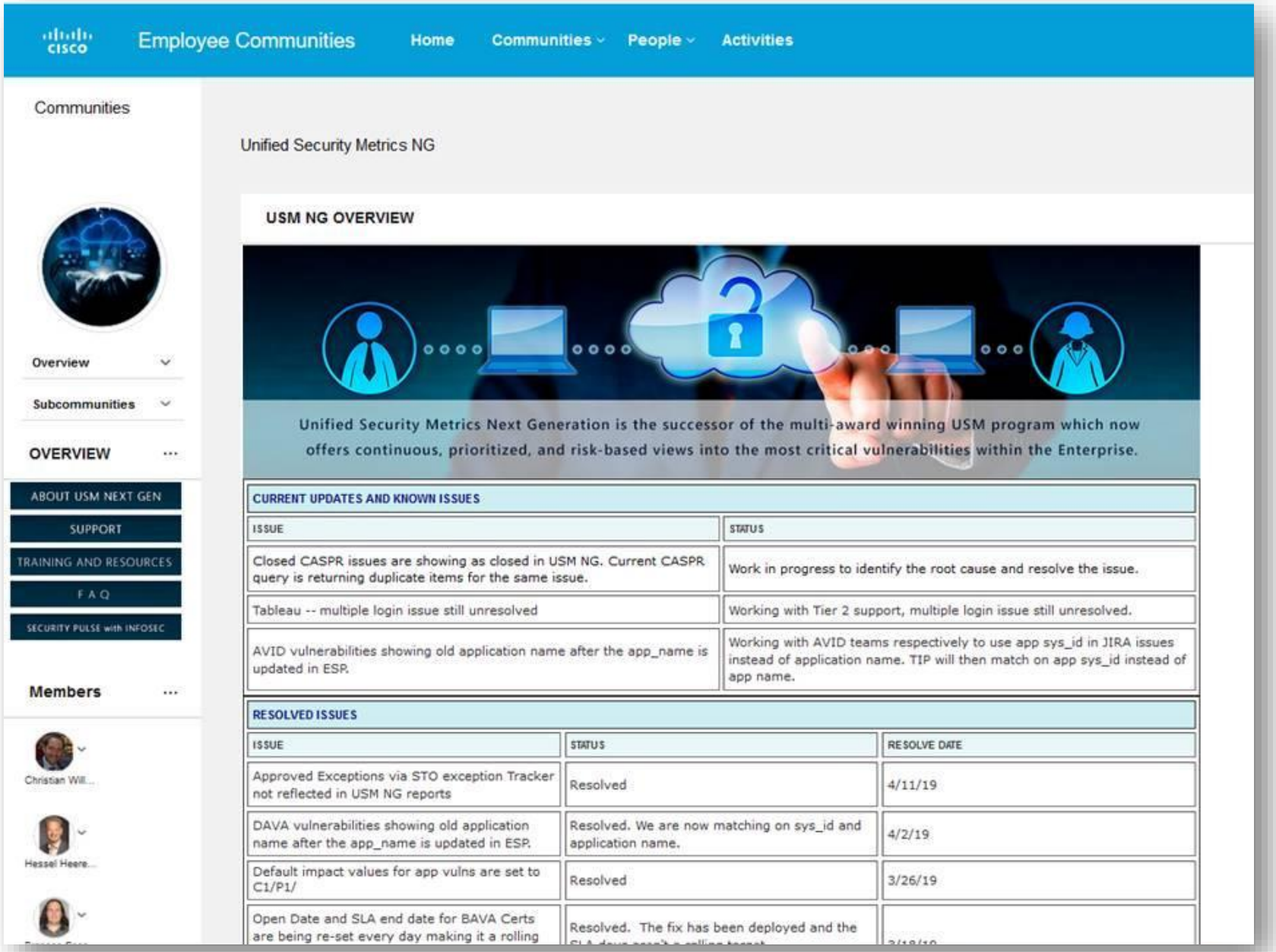
NextGen Redesign 2019

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

OVERVIEW BEFORE

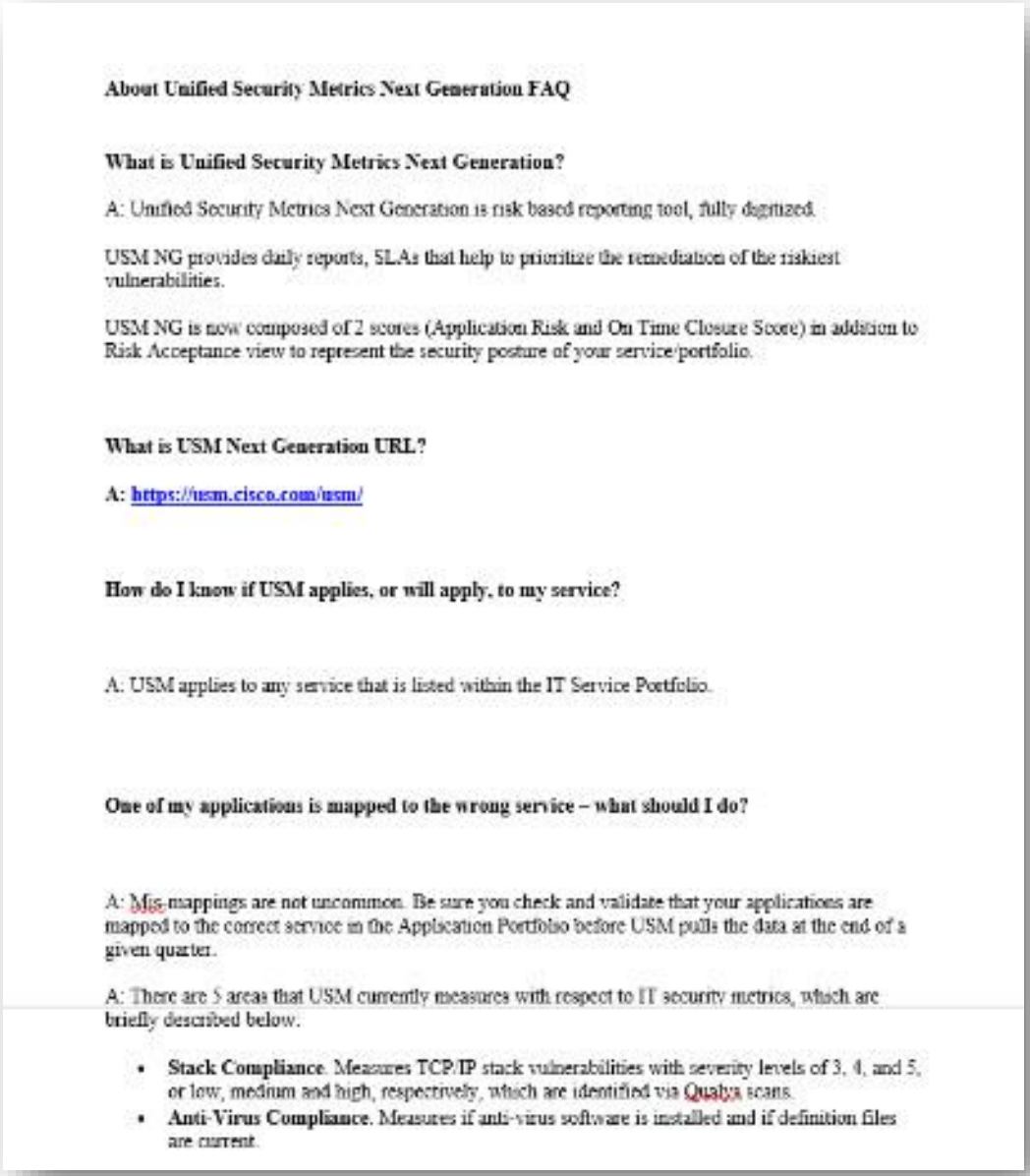


OVERVIEW AFTER:



FAQ BEFORE:

The ‘before’ was just a word document attached to the community platform that had to be checked in and checked out. Icreated 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.

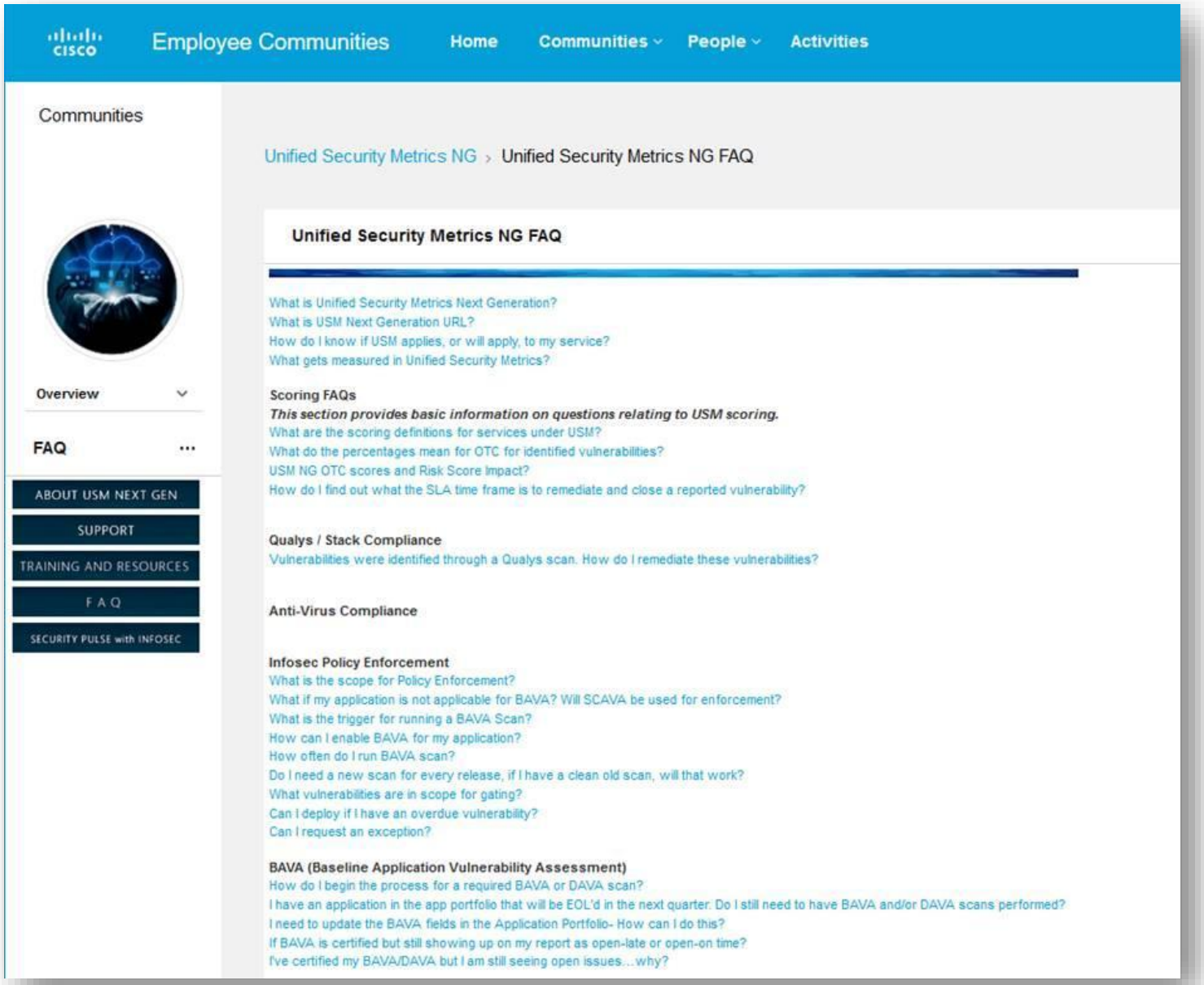
One of my applications is mapped to the wrong service – what should I do?

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:


Employee Communities
Home
Communities
People
Activities
Communities
Unified Security Metrics NG › Unified Security Metrics NG FAQ
Overview
FAQ
ABOUT USM NEXT GEN
SUPPORT
TRAINING AND RESOURCES
F A Q
SECURITY PULSE with INFOSEC
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?