Vulnerability Management Service SC

Service	Vulnerability Management Service
Service Manager	Ben Hartung, Manager of Residential Technology and Security Systems
Department	Information Security Office
Contact	McGinnies Hall Rm 154 ResNet Office, (716) 673-3668, resnet@fredonia.edu
Service Owner	AVP/CIO - Stephen Rieks
Description	The Vulnerability Management Service, utilizing Nexpose', is a service that scans and assesses network connected devices to determine vulnerabilities and remediation plans to mitigate risks. It provides a unified security and compliance assessment for the campus physical, virtual, mobile, and cloud environments which improves the performance of the campus security program by giving a complete risk and compliance posture. The service is a component of the State University of New York Security Operations Center. The service includes the following: • Scan Engine Administration: Integrates with the existing infrastructure to instantly identify and assess vulnerabilities as attack surface changes for scanned hosts. • Scan Template Design & Testing: Custom scan templates are designed based on the type of asset (host), prioritization, and services provided in accordance with minimizing impact on performance. • Asset Inventory Management: Comprehensive inventory of university server assets with assigned prioritization with risk scoring. Provides contextual business intelligence to allow the focus to be on the highest risks through automated asset classification and risk prioritization. • Vulnerability Validation: Exploits that are validated are automatically pushed to scan engine for prioritization and remediation. • Recommends Security Controls: It identifies gaps in defenses and provides a prioritized list of security controls to deploy on endpoints and servers. • Remediation Plans & Reports: Delivers impactful, actionable remediation plans and reports to systems administrators and management to effectively address exploits, efficiently leverage staffing capacity and mitigate risk. • Compliance Management: Enables the university to help address compliance with PCI DSS, NERC CIP, FISMA (USGCB/FDCC), HIPAA/HITECH, SANS Top 20 CSC, DISA STIGS, and CIS standards for risk, vulnerability, and configuration management.
Service Users	• ITS systems administrators • CIS systems administrators
User Services	• Scan template design, testing and automation • Remediation plans and reports • Scan scheduling and alert management
Business Services	The services are only provided to the current list of service users due to security protocol and staffing limitation.
Technical Services	The services listed include all of the primary technical services.
Requirements	The requirements for using this service included the following: • current systems administrator for internal or external facing server
Rates / Cost of Use	The cost of the service is split between university division based on the field device utilization percentage (e.g. residential vs. academic). There are licensing costs for servers and system users. The service cost is currently covered under SUNY SOC PIA.
Getting Started	FredQuest - ITS Incident Management System
Availability	Hours: Monday - Friday 8:30am - 5:00pm Summer: Monday - Friday 8:00 am - 4:00 pm Emergencies - 24/7 based on the availability of support staff
Getting Help	By email: resnet@fredonia.edu By phone: (716) 673-3668 In person: 154 McGinnies (Near the loading dock rear entrance) All requests for assistance are completed using FredQuest: https://fredquest.fredonia.edu/
SLA Notes	• Users with emergency systems infrastructure issues can expect a response within 4 hours and should expect a resolution within 48 business hours of entering a ticket. • Change or new installation requests can expect a response within 36 hours and the resolution will depend on the scope of the request.

<table>
<tr><td>Business Procedures</td><td>Systems fredshare</td></tr>
<tr><td>Change Procedures</td><td>Changes to the service (transition, additions, and discontinuations) must be reviewed by TAC and approved by the Service Manager (CIO) and Cabinet. Changes to the configurations, software, hardware or business procedures are reviewed monthly by the campus Security Systems Team.</td></tr>
<tr><td>Assigned Primary Support</td><td></td></tr>
<tr><td>Assigned Secondary Support</td><td></td></tr>
<tr><td>RACI Chart</td><td>Name: Vulnerability Management Service

Description: see above

<table>
<tr><th>Level</th><th>Responsible</th><th>Accountable</th><th>Consulted</th><th>Informed</th></tr>
<tr><td>Primary</td><td>Ben Hartung</td><td>Ben Hartung</td><td>Systems Administrators</td><td>User</td></tr>
<tr><td>Secondary</td><td>Fred Ullman</td><td>CIO</td><td>Systems Administrators</td><td>User</td></tr>
<tr><td>Tertiary</td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Date Last Modified</td><td>Nov 30, 2017</td></tr>
</table>

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()