VITAL CYBER

Managed Endpoint Protection

MCNC's Managed Endpoint Protection service is built to solve your toughest cybersecurity challenges.

Powered by CROWDSTRIKE

Welcome & Intros

MCNC®

Ruthy Mabe
Manager, Security Services
MCNC

Steven Walton
Cybersecurity Engineer
MCNC

CROWDSTRIKE

David Bill, CISSP
Sales Engineer
CrowdStrike

1. **Service Offering Overview**

   - NCDPI's Announcement

   - Security Protection

   - Device Hygiene

   - Managed Service Offering

2. **How to Enroll**

3. **Onboarding Schedule**

4. **Q&A**

Offering Summary

Announced April 19, 2022

VITAL CYBER

NCDPI has procured two years of our Managed Endpoint Protection service for all North Carolina Public School Units

(Initial Service Term: May 1, 2022 – April 30, 2024)

This service is <u>*available at no cost*</u> to the PSUs!

Service includes licenses for PSU managed *servers, staff devices,* and *other PSU managed non-student* devices*

Eligible Device Types:

- Windows
- Mac
- Linux (*Long Term Support Kernels*)
- Currently supported OS
    - *Windows 7 and Server 2008 R2 require additional paperwork*

*A PSU can purchase licenses for their student devices separately directly from MCNC (note: no Chromebook agent)

Security Protection

Advanced Security Protection

PREVENT

INSIGHT

- Next-Gen AV + Detection & Response
- MCNC handles these blinking lights
- MCNC contacts you only when needed

- MCNC requires a off-hours contact for response to the rare Critical Detection alerts
- MCNC will provide summary of detection, related information, and suggested actions will get emailed to you
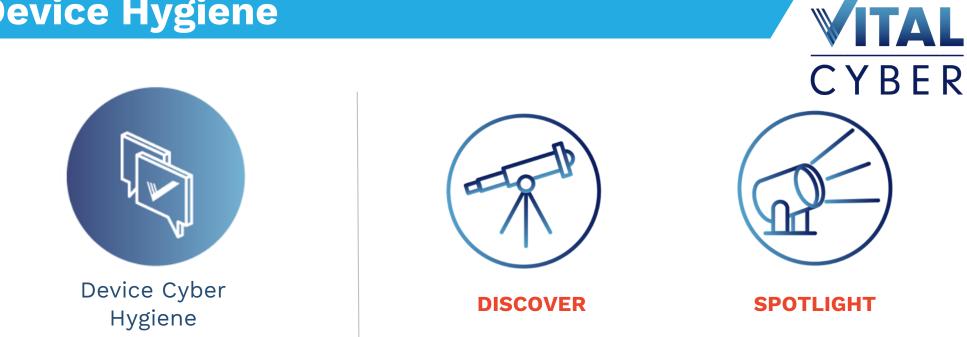
Device Hygiene

Device Cyber Hygiene

DISCOVER

SPOTLIGHT

Discover

- Visibility and awareness of your environment
  - Network neighbors
  - User Account information
  - Device Hardware Information

Spotlight

- Vulnerability Management
  - ExPRT Rating prioritizes
  - Get consolidated remediations of MANY vulnerabilities
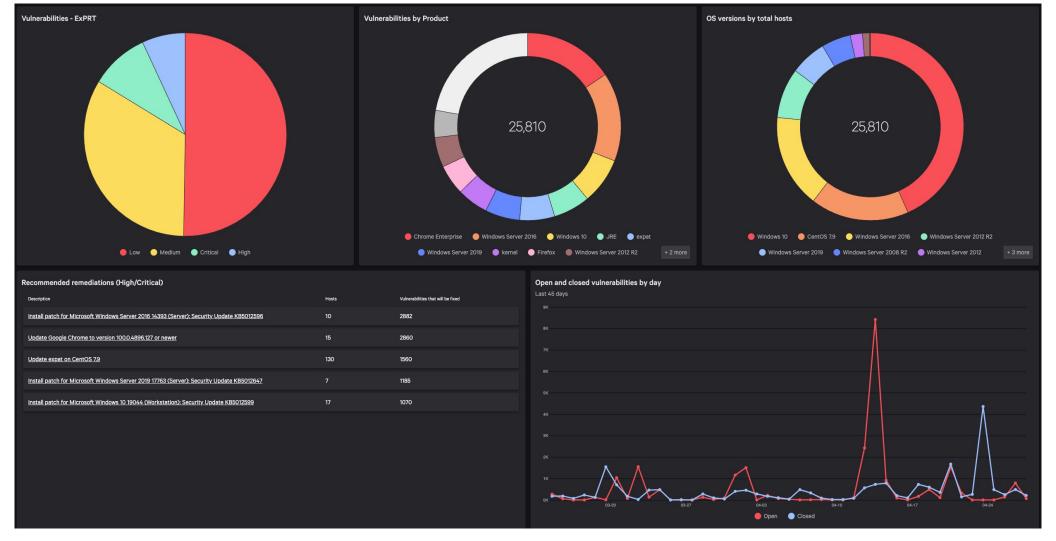 - Easily sort by device, product, or vulnerability

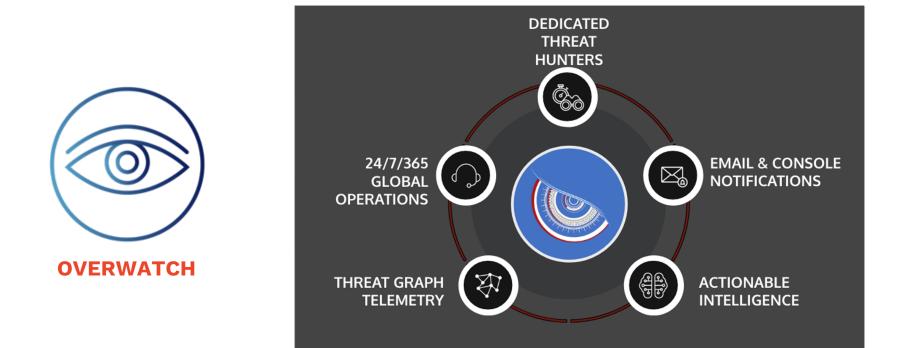# Custom Discover Dashboard

Custom Spotlight Dashboard

Vulnerabilities - ExPRT

● Low ● Medium ● Critical ● High

Vulnerabilities by Product

25,810

● Chrome Enterprise ● Windows Server 2016 ● Windows 10 ● JRE ● expat
● Windows Server 2019 ● kernel ● Firefox ● Windows Server 2012 R2 + 2 more

OS versions by total hosts

25,810

● Windows 10 ● CentOS 7.9 ● Windows Server 2016 ● Windows Server 2012 R2
● Windows Server 2019 ● Windows Server 2008 R2 ● Windows Server 2012 + 3 more

Recommended remediations (High/Critical)

Description	Hosts	Vulnerabilities that will be fixed
Install patch for Microsoft Windows Server 2016 14393 (Server): Security Update KB5012596	10	2882
Update Google Chrome to version 100.0.4896.127 or newer	15	2860
Update expat on CentOS 7.9	130	1560
Install patch for Microsoft Windows Server 2019 17763 (Server): Security Update KB5012647	7	1185
Install patch for Microsoft Windows 10 19044 (Workstation): Security Update KB5012599	17	1070

Open and closed vulnerabilities by day

Last 45 days

● Open ● Closed

Managed Endpoint Protection

Security Operations Monitoring & Response

OVERWATCH

SLAs (*Support & Security*)

Service Support Requests

Priority Level	SLA Response Time
Critical	2 Hours (24/7/365) (must be called in)
High	4 Hours (24/7/365) (must be called in)
(Critical/High SLA require a client resource available)	
Medium	4 Business Hours
Low	Next Business Day
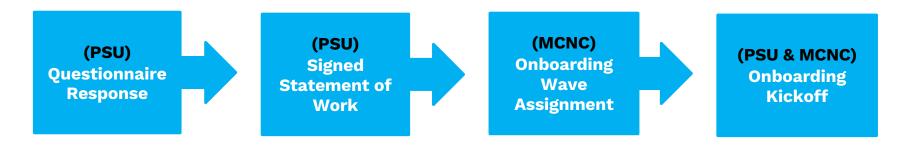
Security Alert Response

Alert Severity Levels	SLA Response Time
Critical:	4 Hours (24/7/365) WE WILL CALL YOU no matter the day or time Very rare 1-2% of ALL Detections
High	1 Business Day
Medium	1 Business Day
Low	1 Week

How to Enroll

Enrollment Flow Chart

VITAL CYBER

```
(PSU)                (PSU)                (MCNC)               (PSU & MCNC)
Questionnaire   →    Signed          →    Onboarding      →   Onboarding
Response             Statement of         Wave                 Kickoff
                     Work                 Assignment
```

- **Step 1:** PSU completes enrollment questionnaire
  - https://forms.gle/b5qQ4BnJKrpWshSq8
  - Sign up linked on MCNC landing page: https://www.mcnc.org/who-we-serve/k-12-schools/managed-endpoint-protection-k12-onboarding-landing-page
- **Step 2:** Upon receipt of PSU questionnaire response, MCNC will send a no-cost Statement of Work (SOW)
- **Step 3:** Upon receipt of signed SOW, MCNC will assign PSU to upcoming onboarding wave.
- **Step 4:** On boarding begins with scheduled wave.

Onboarding Scheduling Details

- PSU onboarding will be performed in waves
- PSUs in the same wave go through the **6-week** onboarding schedule together
- Each phase will have 1 mandatory onboarding call and MCNC office hours

Onboarding Wave Phase Summary

Phase 1	**Objective**: PSU has <u>portal access</u>, sensor is installed on at least 50% of **ALL** target devices.	2 Weeks
Phase 2	**Objective:** MCNC moves PSUs to <u>training policy</u>, MCNC further presents Spotlight and Discover, PSU begin uninstalling their existing A/V. Sensor is installed on 100% of **ALL** target devices.	+2 Weeks
Phase 3	**Objective:** PSUs confirm existing A/V is uninstalled, MCNC review general process, Discover, and Spotlight once again, MCNC moves PSUs to <u>baseline</u> policy	+1 Week
Phase 4	**Objective:** Wrap up to provide overview and ensure PSUs are <u>fully onboarded</u>	+1 Week
Office Hours: MCNC will hold office hours during each wave on Friday mornings and on the off Tuesdays in Phase 1 & 2		

Wave	Kick Off Week	Registration
Wave 1	May 23, 2022	Open – Limited availability*
Wave 2	July 11, 2022	Open – Target 50 PSUs
Wave 3	Early Fall 2022	Open
Wave 4	TBD	-

*Due to limited availability in Wave 1, we will assign PSUs to Wave 1 based on availability and need. To be considered to be included in Wave 1, questionnaire must be received by no later than <u>May 6th</u>

Questions?

Contact Us:
securityservices@mcnc.org

Ruthy Mabe
rmabe@mcnc.org

Steven Walton
swalton@mcnc.org

Managed Endpoint Protection K12 Landing Page

https://www.mcnc.org/who-we-serve/k-12-schools/managed-endpoint-protection-k12-onboarding-landing-page