“Tech Upgrades “2025”

Information Technology Presentation
October 20,2025
Lemont High School
Wesley Rozanski, IT Director

Infrastructure

Network Layer3 / Layer2 / Servers – Wireless APs

Infrastructure & Network Enhancements

•Server Upgrades:
New servers brought online in January 2024 were upgraded to **Windows Server OS 2022** in June 2024 and have now been further upgraded to **Server OS 2025** running **VMware v8.0** for enhanced virtualization performance.

•Core Network Expansion:
The **Layer 3 Core (Core Router)** has been expanded and now features **fully redundant copper and fiber ports**, ensuring improved reliability and high availability.

•Primary & Backup Internet Connections:
***The primary internet connection, provided through the State of Illinois operates at 10Gb (TEN) capacity.
***The backup is a 1Gb fiber-optic connection via **Comcast** has been implemented and configured for automatic failover for both data and voice, ensuring uninterrupted connectivity. – “Fully redundant connections along with path & CO (Central Office)”

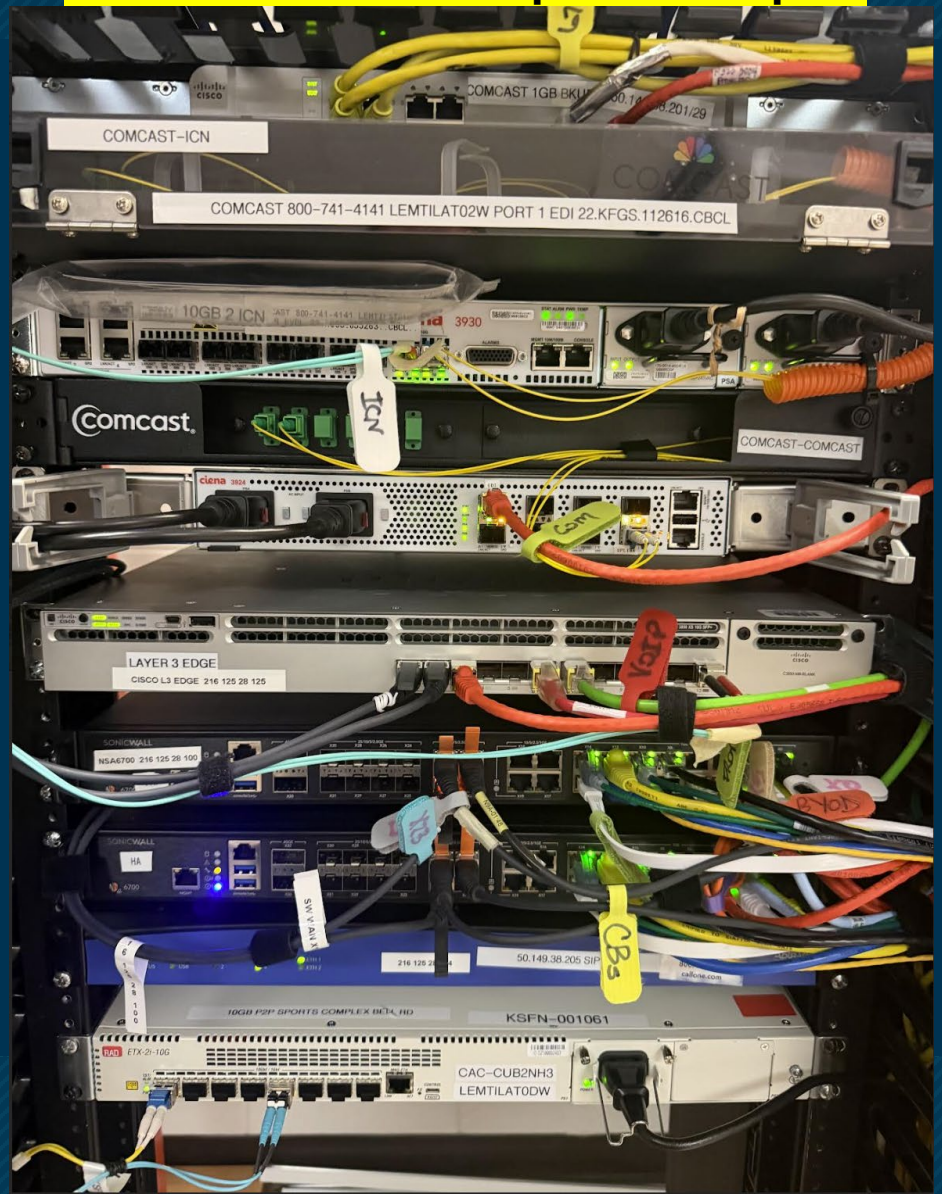
•Wireless Network Upgrade:
The local wireless network has been upgraded to **Wi-Fi 6**, improving bandwidth and performance **(from “60 mph, 3 lanes” to “80 mph, 5 lanes”).** The deployment now includes **802.1x authentication**, the strongest standard for wireless security.

•Sports Complex Connectivity:
The **Sports Complex** is now connected to the high school via a **10Gb fiber-optic link** provided at no cost through the **State of IL Wireless and wired internet** access is now available at the **Concession Stand** and **Varsity Soccer, Baseball, and Softball fields**. Students can connect their Chromebooks, staff have access, and **HUDL cameras** can be brought online seamlessly.

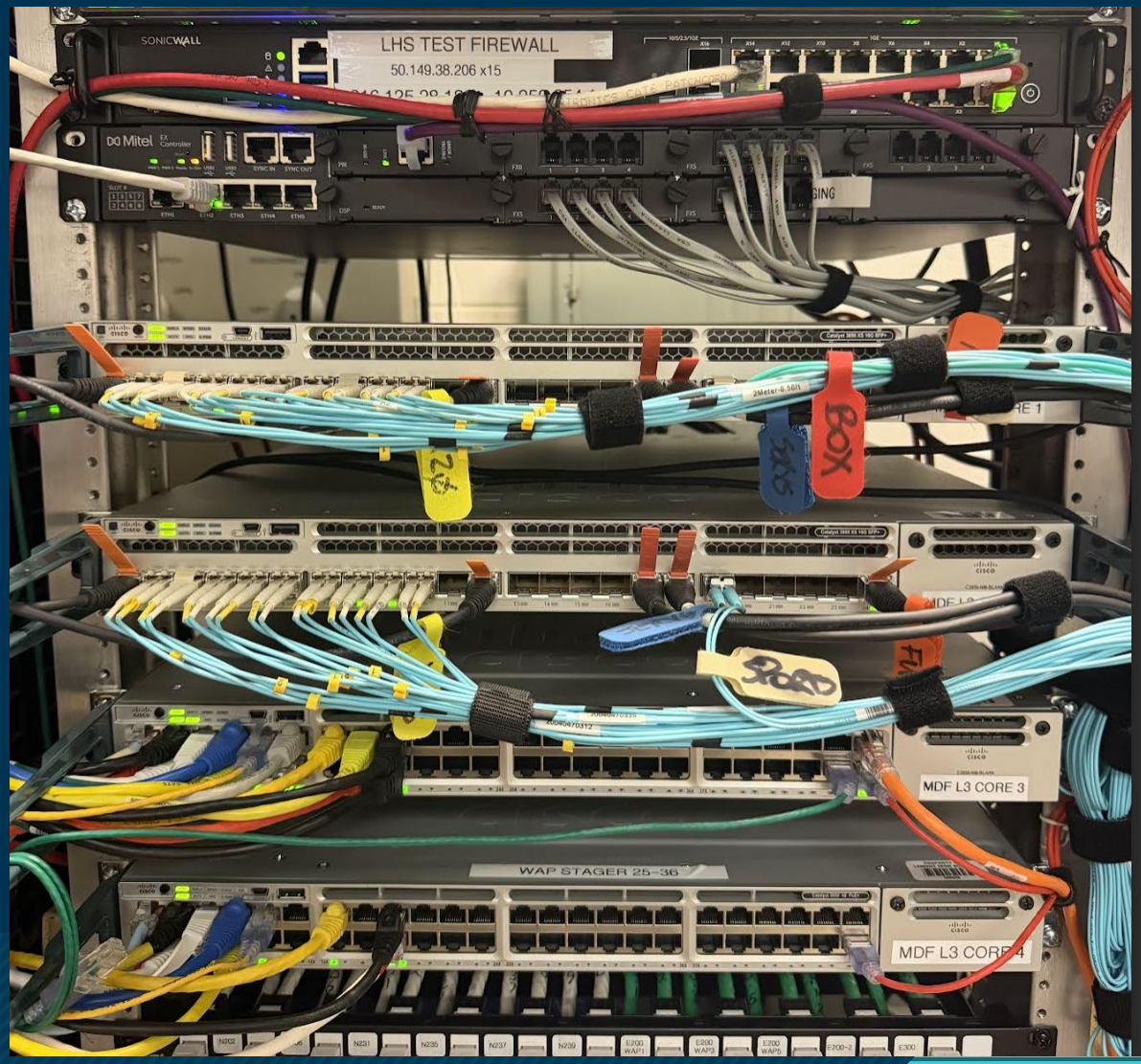
•Disaster Recovery Site (is now the SPORTS COMPLEX): The **LHS IT Department** is now backing up all **servers** to the designated **disaster recovery site**, ensuring data protection and business continuity.

Location: MDF Main Data Closet

Layer 3 Edge Primary 10GB Internet
Firewall(s) in HA Mode
Comcast Fiber 1GB Backup
10GB "P2P" to the Sports Complex



Layer 3 Core "Router"



Cybersecurity

Segment / **Secure** and **“proactively”** scan

Cybersecurity Updates…

- Network Segmentation “VLANs/Networks/Segments” are a happy place – we currently have 25 “VLANs” are in place
- Abnormal Security used for Email Security (2nd / 3rd Layers)
- District Wide Phishing Campaigns via KnowBe4 (monthly) along with Cyber-Pools via Insurance Company (quarterly) - ongoing

• What's New this Year:

- CrowdStrike: Complete Endpoint Protection along with SIEM***
- Lightspeed – Digital Alerts & Digital Insight
- Managed Methods
- Class LINK Identity Management “Rostering”
- Incident IQ – Realtime ticketing system – please send your request to (**lhshelpdesk@lhs210.net**)
- **CISA -** Cybersecurity and Infrastructure Security Agency, is a U.S. Department of Homeland Security (DHS) agency responsible for defending critical infrastructure against cyber and physical threats – CISA scans the LHS Network Perimeter on a bi-weekly basis
- **Internal active scanning (these are real-time) are performed by CrowdStrike while CISA scans the perimeter on a bi-weekly basis (from the outside)**

Instructional Technology Hardware

Instructional Technology Upgrades/Staff Devices updated
--Windows 11 has been deployed throughout the School District--

- Student Computer Lab Upgrades “Windows 11”
  - N211 – Fine Arts Lab - Graphics
  - N221 – Business Lab/Programming
  - Robotics
  - CAD LAB
  - Woodshop

- New LAB Rooms will be brought online – they are W200 & W202 with updated computer models

- **NEW for Staff ThinkPad X1 2-in-1 Gen 9 Intel (14″) – Grey – Windows 11 Enterprise for EDU along with Office 365 / Office Pro Plus 2024**

What's Next?

What's Next – The Future at LHS IT Department

*******Work in Progress: Ongoing initiatives across the LHS IT Department.*******

- **Hyper-V Evaluation**: Testing continues and may replace VMware as our primary virtualization platform.
- **Microsoft 365 Transition**: Migration to Microsoft 365 licensing is planned, including OneDrive, Office, Intune remote management, and enhanced security features.
- **Verizon Wireless MiFi (Hotspots)**: Devices will be upgraded to **5G Ultra Wideband (UW)** for improved connectivity.
- **Continuous Improvement**: We remain committed to enhancing and optimizing all systems deployed throughout 2025 and beyond.
- **& Finally "Microsoft Windows 12"**: Incoming release — testing phase to begin soon.

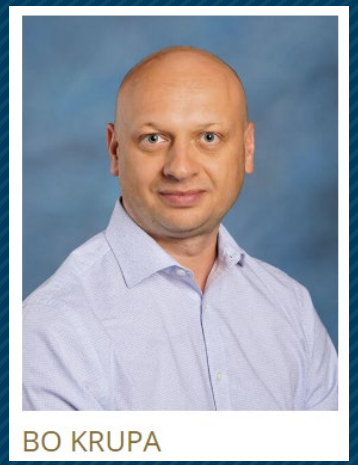
IT Department Mission Statement:

Our mission is to empower our organization through **robust and secure network infrastructure that enables seamless connectivity, collaboration, and innovation**. We are dedicated to providing reliable technology solutions that support our EDUCATION goals and enhance user experience. By prioritizing network resilience, security, and scalability, we ensure that our digital environment fosters productivity and growth. We strive to anticipate and respond to the evolving needs of our users, driving operational excellence and creating a foundation for future advancements. Together, we build a connected community that thrives on technology.

One word SUMMARY: We are here to build an AUTOBAHN for Lemont HD SD210

IT STAFF

Our "Conduit" to the Educators



BO KRUPA

Cybersecurity / Server Engineer

JAKE VONDRAK

Google Workspace Admin

LAWRENCE LORENZO

Technology Support Specialist
Help Desk Admin

ERIN HITCHCOCK

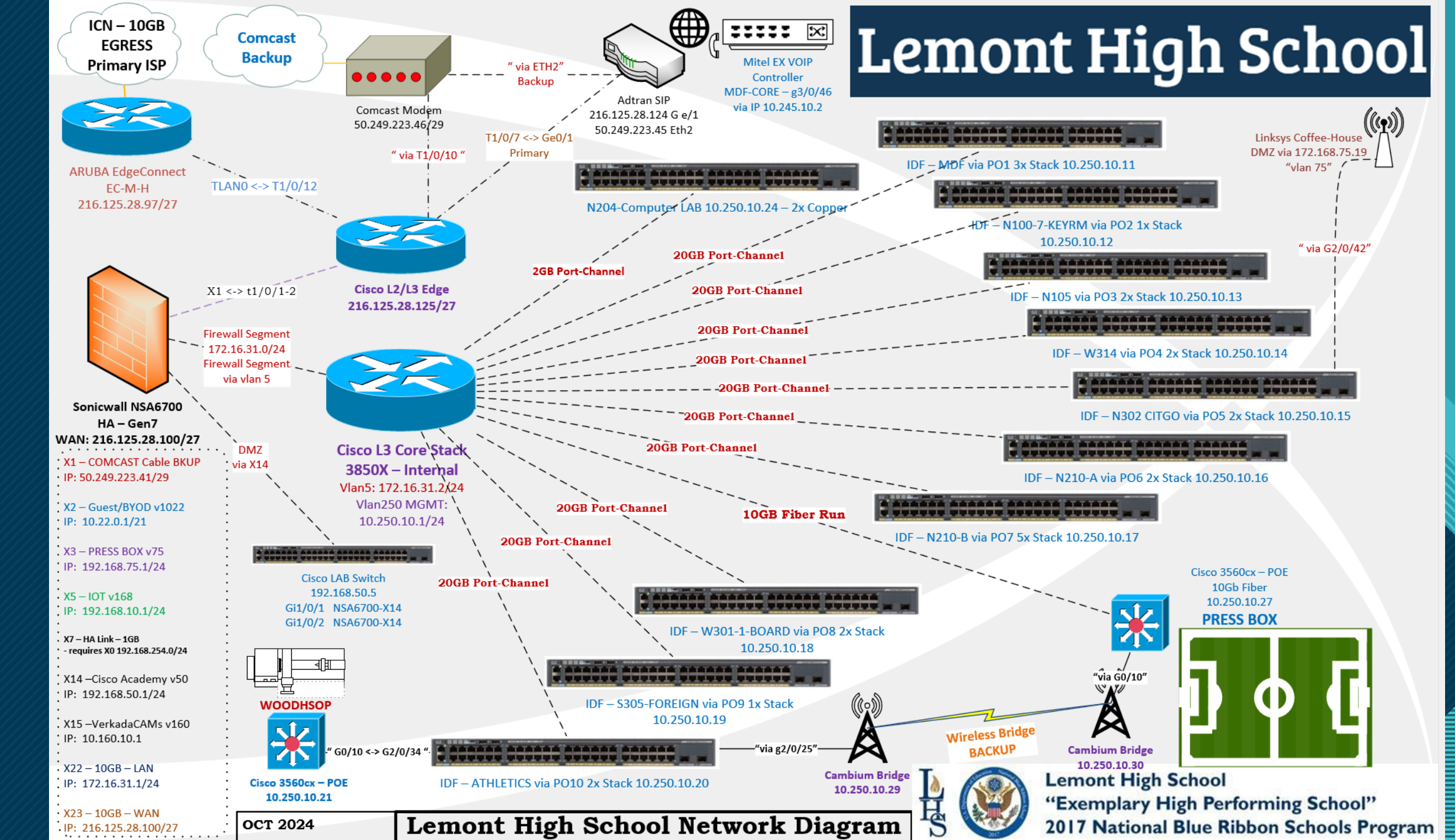
Technology Integration Specialist

Thank You!

Session is now open

for Q & A

Lemont High School



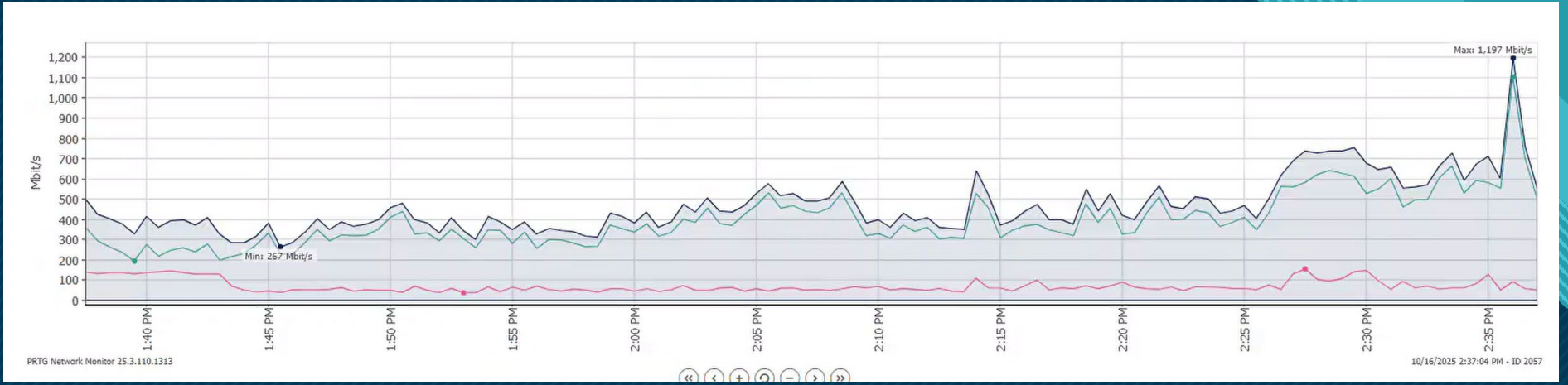
OCT 2024

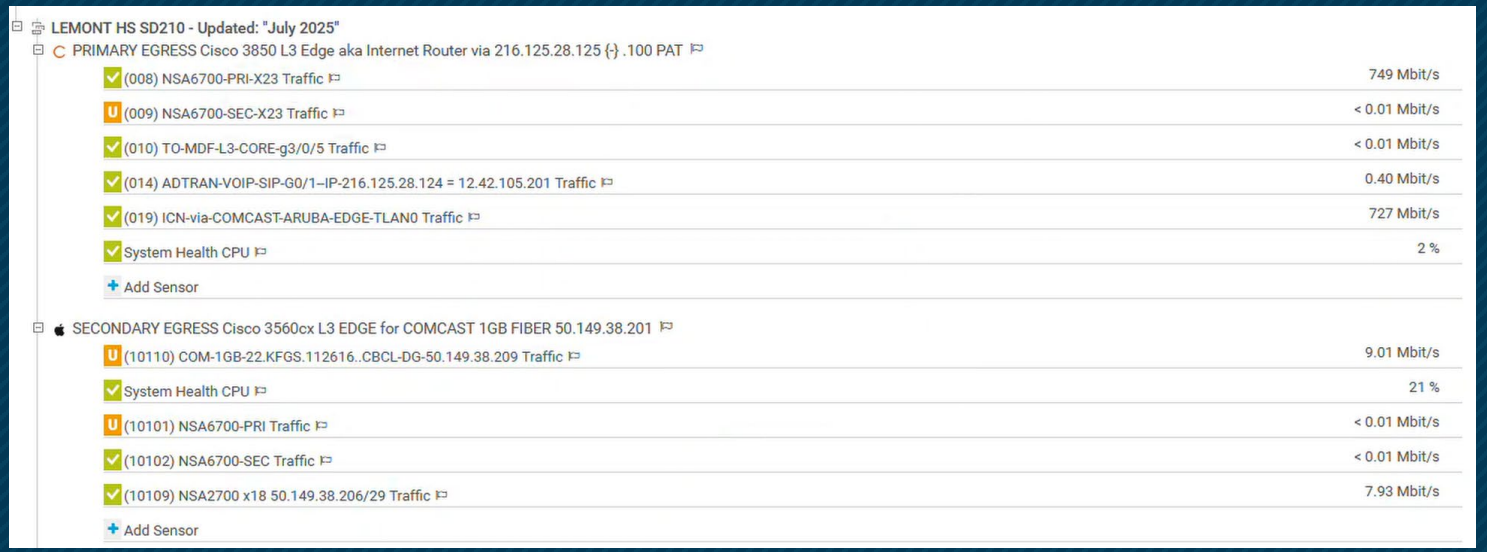
Lemont High School Network Diagram

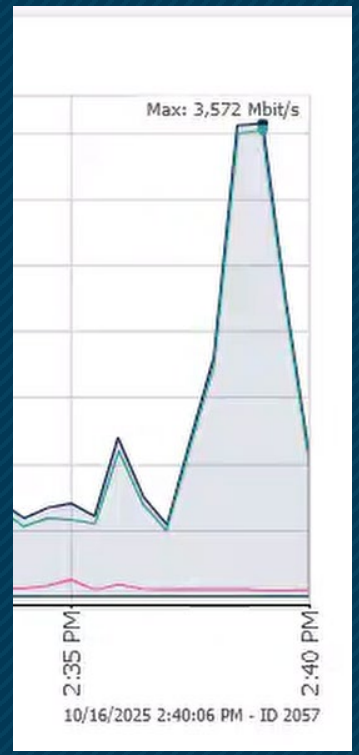
Lemont High School
"Exemplary High Performing School"
2017 National Blue Ribbon Schools Program

PAESSLER PRTG

SecureCRT for Secure Remote Access to the Network Infrastructure







- 1 EDGE 10gb ICN 216.125.28.125
- 1 EDGE 1GB COMCAST 50.149.38.201
- 2-L3-CORE-MDF 10.250.10.1
- CISCO ACA - DMZ 192.168.50.5
- Garage Cisco 3560cx 10.250.10.25
- IDF ATHLETICS - PO#10 10.250.10.20
- IDF N100-KEYRM - PO#02 10.250.10.12
- IDF N105 - PO#03 10.250.10.13
- IDF N210-A - PO#06 10.250.10.16 - 2x
- IDF N210-B - PO#07 10.250.10.17 - 4x
- IDF N302 - PO#05 10.250.10.15
- IDF S305-LANG - PO#09 10.250.10.19
- IDF W301 PO#08 10.250.10.18
- IDF W314 - PO#04 10.250.10.14
- MDF L2 STACK N227 PO#1 10.250.10.11
- PAC 3560cx Control Room 10.250.10.28
- Press-BOX-3560cx-10GB via 10.250.10.27
- Single LAB Switch 10.250.10.24 (offline)
- Sports Complex 10GB L3 10.250.10.26
- Sports Complex BASEBALL 10.250.10.36
- Sports Complex SOCCER 10.250.10.35
- Sports Complex SOFTBALL10.250.10.37
- WOODSHOP-3560cx 10.250.10.21

&

This concludes our presentation for tonight!

ClassLink: Identity & Access Management

Classlink Launchpad is a single sign-on (SSO) platform designed for education that gives users one-click access to all their digital learning tools and apps with a single password. “It provides a personalized portal for students, teachers, and staff to access school-approved applications, websites for Lemont HS – we now have a single password for Windows Server AD and Google Authentication – **additional features**

***Key features include multi-factor authentication (MFA) for security and the ability for users to customize their Launchpad by adding approved apps from a library.

How it works:

Single sign-on: Users log in once with one username and password to get instant access to all their assigned applications, eliminating the need to remember multiple credentials.

Personalized portal: The Launchpad displays a personalized homepage with a user's assigned apps, which can be customized with different themes or icons.

Secure access: It uses secure Multi-Factor Authentication (MFA) to protect sensitive data and ensure secure access from any device.

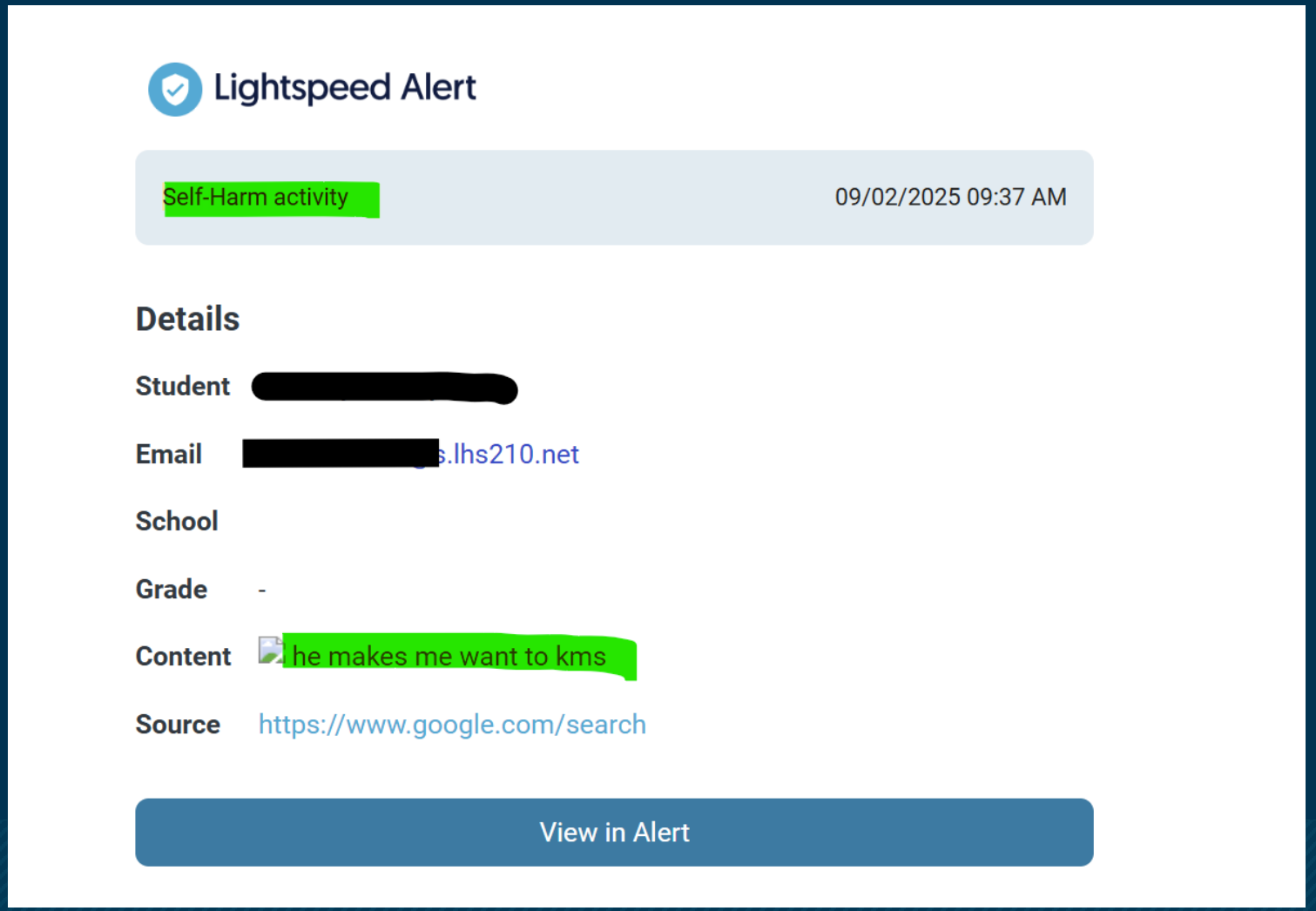
Centralized access: It provides a central place to access various resources, including cloud drives (Google Drive, OneDrive), school-specific software, and other web-based tools.

Customization and flexibility: Users can add additional approved apps from the school's application library to personalize their Launchpad.

Access from anywhere: Launchpad is accessible from any device with an internet connection, making it ideal for both in-school and at-home learning.

https://www.classlink.com/#start

Lightspeed Alert (integrated with LightSpeed Filtering) is an early-warning threat detection system for schools that monitors students' online activity for signs of self-harm, violence, bullying, and other dangerous behaviors. It uses artificial intelligence (AI) and human review to identify, analyze, and escalate potential risks, upon detection administrative is notified – an example seen below

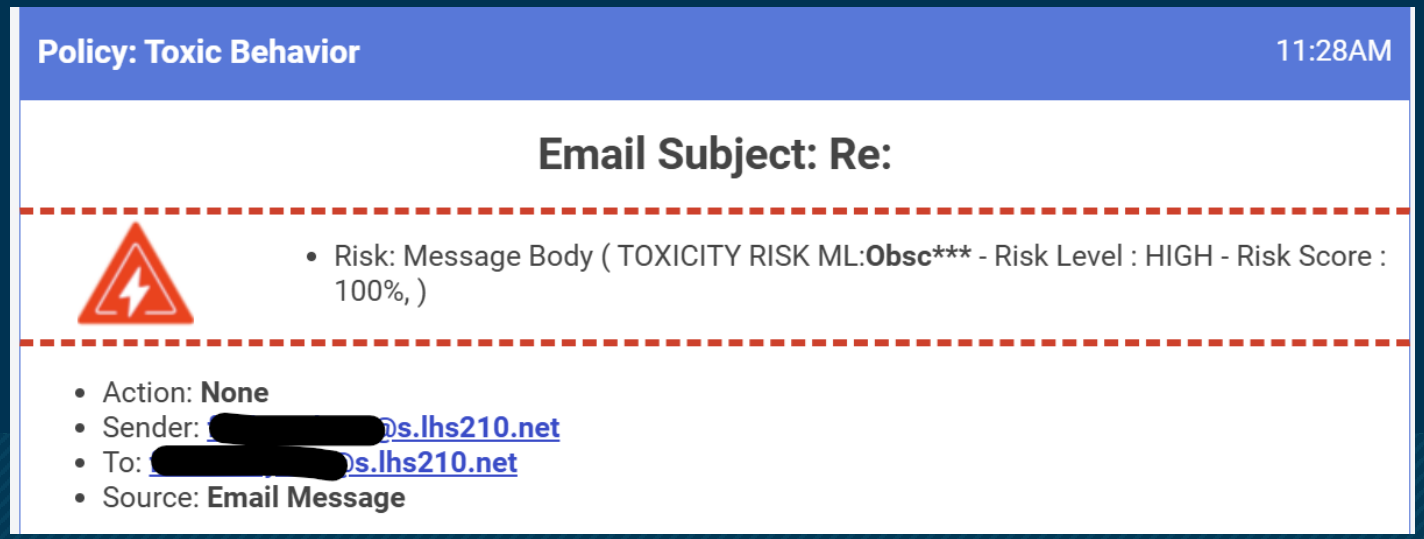


ManagedMethods is a cloud security platform used by K-12 school districts to protect student data and ensure online safety in Google Workspace and Microsoft 365 environments. It provides features for threat protection, risk detection, and data security, allowing schools to use cloud applications securely. Key functions include scanning for phishing and malware, identifying risky third-party apps, blocking unauthorized data sharing, and detecting explicit images.

***Actual Event:**

Subject: Security Monitoring System – Successful Incident Detection

The monitoring application performed as intended during a recent incident. The system automatically flagged inappropriate content sent between email accounts (personal and LHS), alerting IT and applicable staff. Appropriate actions were taken promptly, and the issue was resolved following internal review and follow-up with the involved student.



Server Virtualization Explained:

Server virtualization is the process of using software to create multiple virtual servers, or virtual machines (VMs), on a single **physical server**. This is achieved with a software layer called a hypervisor that abstracts the physical hardware and allows each VM to run its own operating system and applications independently. The benefits include improved hardware utilization, cost savings, increased flexibility, and easier management. "Server virtualization is **the process of dividing a physical server into multiple unique and isolated virtual servers** by means of a software application."

The 2 most popular are VMWare and Microsoft's Hyper-V

CrowdSTRIKE “SIEM” ***SIEM by CrowdStrike, which stands for Security Information and Event Management, is a cybersecurity solution that collects and analyzes log and event data from across an organization's IT environment in real-time. By centralizing this information, SIEM systems correlate events to detect threats, provide visibility into security incidents, and enable faster response through automated alerts and reporting for compliance

CrowdStrike Activity - Security Incident Observed

In the email shown below, we can see CrowdStrike effectively doing its job. A student attempted to download a malicious file, which was successfully blocked by CrowdStrike. When Bo initiated a remote session to investigate, he observed the student searching on Google for ways to remove CrowdStrike.

as per BO, as he setup a remote session to the student's computer - the student was searching google "how to remove crowdstrike" - it appears to be more than just an accident

"Hi Eddie "Computer Science Teacher"

[redacted] using computer number 20, has downloaded a zip file containing a bunch of malware. I need you to shut down the computer and instruct the student to use a different computer and discourage him from doing so in the future.

ALERT: [High] Malicious activity detected on N204-20

CROWDSTRIKE

SEVERITY:	High
TACTICS & TECHNIQUES:	• Machine Learning via Cloud-based ML
TIME:	17:26:09 on Wednesday, Sep 17 2025 UTC

OPEN DETECTION

A VLAN, or Virtual Local Area Network Detailed Overview

“is a logical grouping of devices on a network that allows them to communicate as if they are on the same physical network, even if they are not.”

Key benefits of VLANs include:

1. **Improved Security:** By isolating sensitive data traffic, VLANs limit access to specific users or devices.

2. **Reduced Broadcasts:** VLANs help minimize broadcast traffic, improving overall network performance.

3. **Simplified Management:** They allow for easier network management and configuration changes without physical re-cabling.

4. **Flexibility:** Devices can be grouped based on function or department, regardless of their physical location.

Overall, VLANs are an essential tool for creating organized, efficient, and secure networks.

Bi-Weekly from CISA

Greetings Lemont Township Highschool (LTSHSDIL),

The Cyber Hygiene scan results are attached for your review.

Note: CISA has the following information listed as the Technical Points of Contact for LTSHSDIL:

Name: Bo Krupa
Email: bkrupa@lhs210.net

Name: Wesley Rozanski
Email: wrozanski@lhs210.net

Please request the report password from a Technical Point of Contact and route all other requests through a Technical POC. Should a Technical Point of Contact listed above no longer be with LTSHSDIL, please contact vulnerability@cisa.dhs.gov with updated information.

If you have any questions, please contact our office.

Cheers,
CISA Cyber Assessments - Cyber Hygiene
Cybersecurity and Infrastructure Security Agency
vulnerability@cisa.dhs.gov

*** 3 vulnerabilities are in regards to our Voice Mail Server this will be remedied prior to YEAR END