Keeping the Bad Guys Out

MCSD IT SECURITY DAILY PRACTICES

- ANDREW HISH – SENIOR SYSTEM ADMIN
- TONY GARCIA – SYSTEM ADMIN
- JOY NULISCH – IT DIRECTOR

MCSD Demographics

- Key West to Key Largo 104 miles
- 10 schools (6 charters)
- 9129 Students
- 1500 Staff

IT Infrastructure

- WAN
- Internet
- Devices
- Data Center/Cloud
- Focus ERP/SIS

Protecting the Infrastructure…
at all cost

- Sentinel One Singularity Complete includes full featured enterprise-grade EDR.
  - Complete includes NGAV and behavioral AI to stop known and unknown threats.
  - Complete includes suite features like network control, USB device control, and Bluetooth device control.
  - Complete includes Rogue identification and can be instrumented for full network attack surface protection.
- Palo Alto Networks firewalls. Model 3410 and 3260 50-70%. IOT+DNS sub.
- Microsoft 365 A5 Advance Threat protection.
- Desktop Central Patching.
- Dell Encryption data.
- IBoss Content filter solution.

Protecting the Infrastructure…
On the cheap…

- CISA.GOV- Cybersecurity & Infrastructure Security Agency
- https://www.cisa.gov/uscert
- MS-ISAC-Multi State Information Sharing and Analysis Center.
- https://www.cisecurity.org/advisory
- Unit 42 Palo Alto Networks security intelligence team.
- https://unit42.paloaltonetworks.com/category/threat-briefs-assessments/
- Virus Total Great site to check URL, Files, Geo information etc.
- https://www.virustotal.com/gui/home/search
- IBM –XFORCE- Great threat intelligence website.
- https://exchange.xforce.ibmcloud.com/
- ALIENVAULT OTX-Open Threat Exchange.
- https://otx.alienvault.com/
- Internet Storm Center-SANS Great Windows patch detail.
- https://isc.sans.edu/

Daily Routine

- Layered Scheduled approach, system admins overlap morning checks and arrival time in a staggered way to check each other's work.
- Communication between admins when threats are found within one system and can be mitigated within multiple systems, Asking each other about processes that are being run.
- Network Infrastructure check. WAN, sites ,APs, switches and routers.
- Firewall check VPN usage, overnight attacks, dynamic updates notes, Wildfire and logs, along with any anomalies.
- Sentinel One check for activity and threats, based on threats and Indicators of compromise found in the wild new rules are created if needed
- Threat Intelligence and Hunting. We use various website and automated alert emails specific to K-12. Star custom rules.
- Check Server Infrastructure

Security Awareness…
Help us Keep the Bad Guys Out

- KnowBe4
- Keep it on the Agenda
- Industry Standard Controls and Practices