StingBox HoneyPot

Simple Honeypot Detection for Schools and Universities

A Different Detection Model for Education Environments

Stingbox deception-based detection is built on a simple principle: where deployed, Stingbox presents selected network services that attackers commonly probe, allowing each interaction to trigger a detection event. Because a Stingbox honeypot has no operational role and no legitimate users in the school environment, any attempted access to it is inherently suspicious.

This model is particularly effective in K-12 and university networks, where attackers moving toward high-value systems such as student information systems, payroll platforms, or administrative services must traverse shared network segments. In these environments, reconnaissance and lateral movement activity often occurs long before a disruptive event such as ransomware encryption is launched. Incident response research shows that attackers frequently remain inside networks for extended periods while expanding access and preparing attacks. Mandiant's M-Trends 2024 estimates a global median dwell time of approximately 16 days, while IBM X-Force investigations show ransomware actors commonly operating inside networks for 30–60 days before detonation. In poorly monitored environments, investigations regularly find attacker activity lasting several weeks before discovery.

The signal produced by deception detection is simple: either nothing happens, or someone is probing the network. Deception does not rely on behavioural baselines, signatures, or traffic thresholds. For education IT teams with limited staffing and limited monitoring coverage, that clarity reduces investigation overhead and enables faster response when attacker activity appears.

Stingbox presents realistic service responses when scanned, turning commonly targeted network ports into tripwire detection points. These responses appear legitimate to an attacker but serve no operational purpose in the school network. Decoy services may include:

- A file server share
- An administrative network share
- A network printer or device management interface

These services should never be accessed by students, staff, applications, or systems during normal operations. Any interaction therefore provides a high-confidence indicator of reconnaissance or lateral movement activity.

The Problem

K–12 districts and universities carry one of the most demanding cybersecurity responsibilities of any sector while operating with far fewer resources than a comparable enterprise environment.

The challenge is not the absence of tools; it is the structure of the environment itself:

- Small teams managing large environments. *Only 19–21%* of districts maintain a dedicated cybersecurity role or full-time security staff member (CoSN State of EdTech District Leadership Report, 2024).
- Open network architecture. School networks must support thousands of users, personal devices, unmanaged IoT equipment, and cloud learning platforms (Cybernut; Check Point Research).
- Monitoring limitations. Most districts and universities do not operate a dedicated security operations centre, leaving monitoring responsibilities to small IT teams that also manage infrastructure and user support (IBM Security reporting).

In this environment, increasing alert volume does not improve security outcomes. It increases the likelihood that early warning signals are missed.

Effective cyber protection in education therefore depends on detecting the right signal early—clearly and with enough confidence that action can be taken even when staff are not actively monitoring systems.

Why Education Is a Target

K-12 districts and universities experience sustained cyberattack activity, with ransomware now representing a recurring operational risk rather than an isolated event. According to Sophos' State of Ransomware in Education 2025, *63%* of K-12 organisations and *66%* of higher-education institutions reported being hit by ransomware during the previous year. Children are our most precious and vulnerable asset and represent the deepest pocket for a cybercriminal to target.

Education networks hold highly monetizable data, including student records, staff personal information, financial aid data, health records, and credentials.

At the same time, the architecture of education networks favours the tactic most commonly used by attackers after initial compromise: lateral movement. Flat VLANs, limited segmentation, shared devices, unmanaged IoT systems, and aging infrastructure all allow attackers to expand their reach once inside the network.

Sophos reports that *40%* of ransomware attacks involve exploited vulnerabilities and *37%* involve compromised credentials. Additional research shows persistent exposure of remote access services: UpGuard found that *10%* of universities—and *23%* of the top 500 institutions—expose RDP services to the internet, while the FBI estimates that *70–80%* of ransomware infections begin through exposed RDP access.

Traditional Detection Methods

Miss the Early Signal

Traditional detection tools typically prioritise alerts by identifying behaviour that deviates from historical baselines. In education networks, however, constant activity from students, staff, and connected devices generates high volumes of ambiguous signals that require expert interpretation and ongoing tuning.

As a result, early attacker activity—such as reconnaissance scanning, credential harvesting, and lateral movement—often blends into normal network activity. By the time a disruptive event such as ransomware encryption occurs, attackers may have already spent weeks exploring the environment, identifying critical systems, and escalating privileges.

Industry investigations consistently show that intruders often remain inside networks for extended periods before detection. Global incident response reporting places median dwell times in the multi-week range, with ransomware operators frequently maintaining access for several weeks while expanding their reach across the network.

The longer attackers remain undetected, the more systems they compromise, the more credentials they harvest, and the greater the operational disruption when the attack is executed.

Stingbox Deception in Education Environments

Education networks are large and access-first by design. Check Point Research reports that school and university environments often include thousands of connected devices and endpoints, many of which are unmanaged or difficult to monitor.

At the same time, device inventory visibility can be incomplete at scale, with large districts reporting gaps in tracking student devices deployed in one-to-one computing programs (EdCircuit). Aging infrastructure further complicates network security: the Consortium for School Networking reports that 45% of districts replace core network switches only after six years or more, while 58% maintain similarly extended refresh cycles for network-connected cameras (CoSN).

In this environment, deception-based detection provides a practical way to highlight surface attacker activity that would otherwise remain hidden within normal network traffic. By monitoring interactions with services that have no legitimate users, Stingbox reveals reconnaissance and lateral movement activity early in the attack lifecycle.

Key Outcomes for Education

Research and incident reporting show that earlier detection directly reduces the scale and cost of cyber incidents.

- Shorter attacker dwell time limits lateral movement and reduces the number of compromised systems.
- Earlier containment reduces operational disruption and recovery timelines.
- High-confidence alerts reduce investigation overhead for small IT teams.
- Smaller incidents reduce the scope and cost of incident response and rebuild activities.

Independent research summarised by Intelligent CISO and Enterprise Management Associates indicates that organisations using deception technologies report attacker dwell times as low as approximately 5.5 days, compared with 78–100+ days commonly cited in environments without deception controls.

Education-specific reporting from Sophos shows ransomware recovery costs averaging $2.28M for lower education and $0.90M for higher education, demonstrating the financial impact when incidents expand before detection.

Summary and Conclusions

K–12 districts and universities operate cybersecurity environments defined by open networks, limited security staffing, and constant attack pressure. Schools and universities face threats from organised attackers, opportunistic activity, automated scanning, and internal misuse by students and staff.. Traditional detection approaches that rely on large volumes of behavioural alerts frequently fail to identify early attacker activity in these environments.

Industry investigations consistently show that attackers often remain inside networks for weeks while expanding access and positioning ransomware or data theft operations. During this period, reconnaissance and lateral movement activity occurs across the network but frequently goes unnoticed.

Stingbox addresses this challenge by monitoring attacker-targeted network services that have no legitimate users. Because these services exist solely as detection tripwires, any interaction provides a clear signal of malicious activity.

By revealing reconnaissance and lateral movement early, Stingbox allows education institutions to detect attackers during the extended dwell time that typically precedes ransomware deployment. This enables faster containment, reduces the number of affected systems, shortens operational disruption, and lowers the cost of incident response.

For schools and universities operating with constrained security resources, Stingbox Honeypot's provides a practical cybersecurity control aligned with the realities of education networks.

References

1. Sophos. *The State of Ransomware in Education 2025*. Sophos Ltd., 2025.
2. Sophos. *The State of Ransomware 2022*. Sophos Ltd., 2022.
3. Palo Alto Networks Unit 42. *Vice Society Targets the Education Sector*. Unit 42 Threat Intelligence Report, 2022.
4. Palo Alto Networks Unit 42. 2024 *Global Incident Response Report*. Palo Alto Networks, 2024.
5. Mandiant (Google Cloud). M-Trends 2024: *Global Incident Response Report*. Mandiant, 2024.
6. IBM Security. *Cost of a Data Breach Report 2024*. IBM Corporation, 2024.
7. IBM Security X-Force. *Threat Intelligence Index 2024*. IBM Corporation, 2024.
8. CrowdStrike. *2024 Global Threat Report*. CrowdStrike Holdings, 2024.
9. Consortium for School Networking (CoSN). *2024 State of EdTech District Leadership Report*. CoSN, 2024.
10. Check Point Research. *Cyber Security Report: Education Sector Insights*. Check Point Software Technologies, 2025.
11. EdCircuit. *K–12 Device Inventory and Asset Management Challenges*. EdCircuit, 2025.
12. UpGuard. *University Network Exposure Report*. UpGuard, 2023.
13. Federal Bureau of Investigation (FBI). *Internet Crime Report 2023*. U.S. Department of Justice, 2024.
14. Cybersecurity and Infrastructure Security Agency (CISA). *Ransomware Guide*. U.S. Department of Homeland Security, 2023.
15. Cybersecurity and Infrastructure Security Agency (CISA). *Pre-Ransomware Notifications*. U.S. Department of Homeland Security, 2023.
16. Enterprise Management Associates (EMA). *Deception Technology Research Survey*. EMA Research, 2023.
17. Cybernut. *Education Cybersecurity Landscape Report*. Cybernut, 2025.

For further information regarding this Document or StingBox products, please contact us at:

- Email: support@stingbox.com
- Phone: (561) 203-8594
- Website: www.stingbox.com
- Mailing Address: StingBox LLC 7190
  SE Federal Hwy Ste 3 Stuart, FL 34997-8693, USA