Customer Story

Penfield Central School District

K-12 school system maximizes network visibility and improves threat coverage while avoiding alert fatigue

When thinking of potential attack targets, a small suburban school district may not be the first that comes to mind. The reality, however, is that these school districts are common targets for threat actors.

One group in particular, Russian-based Vice Society, is dedicated solely to attacking K-12 schools. This is because these schools often have small security teams and limited resources, making them easy targets for ransomware.

Additionally, a shift back into in-person learning after the Covid-19 remote learning strategy has led to an increased usage in technology as an integral part of the teaching strategy. This means that there are a lot of endpoints without much staff to manage them.

The key to keeping both students and staff protected from cyber threats is maintaining heightened visibility into network traffic and user activity. This is why Penfield Central School District in New York uses the Stamus Security Platform to provide additional layers of threat detection to their existing strategy.

SNAPSHOT

Organization type: K12 public school system

Location: Monroe County, NY

Organization size: 6000 students, 1000 staff

Challenge: The IT team lacked visibility into network traffic activity and believed they were vulnerable to attacks that were not detectable via their endpoint/antivirus system.

Solution: The school district deployed Stamus Security Platform to dramatically increase their network visibility while minimizing alert fatigue and improving their overall security posture.

Outcome: After implementing SSP, Penfield school district has an added layer of detection that gives them confidence in their ability to keep their students and staff protected from cyber threats.

Penfield Central School District uses Stamus Security Platform to:

Maximize Visibility: by identifying previously unknown threats and unauthorized network activity, capturing extensive metadata along with detailed forensic evidence, and making it readily available through an intuitive user interface, the team from Penfield Central School District is able to know more and respond sooner.

Avoid Alert Fatigue: through its ability to sift through millions of individual detection events and identify only serious and imminent threats, Stamus Security Platform drastically reduces alert fatigue and has nearly eliminated false positives while still logging all data needed for proactive threat hunting and incident investigation.

Improve Detection Confidence: Stamus Security Platform is straightforward to operate and requires very little maintenance, enabling one employee to effectively monitor the activity of a 6000+ device network with the confidence that he will be able to detect and respond to threats.

BACKGROUND

Penfield Central School District is a public school system located in Monroe County, NY – about 15 minutes outside the city of Rochester, covering sections of six towns: Penfield, Pittsford, Walworth, Macedon, Brighton, and Perinton.

They have 1000 staff members overseeing the education of approximately 6000 students in Kindergarten through 12th grade with four elementary schools, one middle school, and one high school.

The Penfield IT department manages several different types of technology assets, chiefly a one-to-one device program for their middle and high school students as well as laptop carts in the lower grades. According to senior network technician Mike DiLalla, the district uses a variety of educational services and programs that primarily function in the cloud such as Microsoft Office 365.

TECH STACK

Microsoft Windows environment with 5000+ endpoints and 40+ on-premise servers

Numerous cloud-based applications, including Microsoft Office 365

Antivirus software

Network detection and response (NDR) by Stamus Networks

DiLalla is one of only nine IT employees, and he is the primary senior security manager, with the other IT team members working in support roles. This means that DiLalla is solely responsible for managing the security of 5000+ endpoints and 40+ on-premise servers.

Before coming to Stamus Networks, Penfield primarily used a SIEM, an application blocker, and antivirus software to protect their network. They found success with these tools, but the district wanted to increase their network visibility. By collecting as much information as possible, they would not only see the threats they were facing, but also better support hunting and investigations into the threats stopped by their antivirus software.

CHALLENGES

As previously mentioned, the greatest threat facing Penfield was ransomware. They were very confident in their antivirus software's ability to handle these types of attacks, but they wanted to see a more thorough incident timeline and have more comprehensive investigative abilities.

Additionally, they wanted the ability to monitor compliance with their policies and uncover violations. With 6000 students using computers and most of them taking those computers home everyday, they needed additional internal controls to ensure proper usage outside of their on-prem app blocker.

Penfield had a number of technical requirements for a new network detection system. First, they needed something that functioned well in a Microsoft Windows environment. All 6000+ endpoints are windows-based. Second, they wanted something that used passive monitoring for detection, like a classic network-based intrusion detection system (IDS). But they wanted the system to more intelligently generate a security event stream that did not produce an overwhelming number of IDS false alarms and would likely produce the inevitable alert fatigue.

SUMMARY OF CHALLENGES

Ransomware specifically targeting K-12 schools

A lack of visibility into network traffic

Needed to identify policy violations

IT team only uses windows

Wanted IDS-like data without IDS noise

Had to support their virtualization environment

Only one network technician for 5000+ devices

DiLalla is the only member of the IT team managing security events, but he also has many other responsibilities. He needed a system that could automatically triage the security event data and notify him only of the most serious and imminent threats.

It was also important that the system support their virtualization environment. Penfield uses VMware, so any appliances they chose needed to function in that environment.

These challenges led DiLalla and Penfield to search for a virtualized network-based threat detection solution that was optimized for detection in a Windows environment and could provide maximum visibility, identify and act on policy violations, and could be tailored to uncover the specific threats they believed were targeting them without additional nois

SOLUTION

Penfield selected the Stamus Security Platform (SSP) with the NDR license tier. SSP is an advanced network-based detection and response (NDR) solution that exposes serious and imminent threats against critical assets, enables rapid response, and may be deployed on-premise, in the cloud, or in a hybrid environment.

> SSP answered the organization’s challenges by increasing visibility into their Windows-based environment using their network traffic with the extensibility that allowed them to tailor the system to their detection needs.

When evaluating potential solutions, DiLalla was evaluating traditional IDS-based network threat detection solutions. He was familiar with SNORT and liked the visibility IDS gave into network data, but SNORT is open-source and has a number of limitations. Further review led him to evaluate Suricata, which he liked because it was more modern than SNORT. Ultimately, he found Stamus Networks, and he appreciated that SSP was built on top of the Suricata engine and came as a complete turnkey system with many powerful additions.

They ended up choosing SSP because it gave them exactly what they were looking for: increased visibility, low noise and false positives, and turnkey support. And it fit well with their virtual deployment model.

Penfield deployed two virtual appliances in the VMware environment, with a Stamus Networks probe inspecting and analyzing north-south network traffic on a 10 Gbps link and the Stamus Central Server on the front-end, managing probe data and providing the user interface.

Even after deploying SSP, Penfield relies heavily on the capabilities of their antivirus software as a first line of defense and threat detection. However, they use Stamus Security Platform capabilities on a regular basis. The first feature regularly used is the Kibana integration. With Kibana, Penfield can troubleshoot and view vast amounts of protocol transactions and flow data generated by the probe. DiLalla also uses the guided threat hunting feature to search for specific threat types and to identify policy violations.

For Penfield School District, they really wanted to pare down detections to focus only on specific threats they knew they would face, such as ransomware and command and control behaviors.

With SSP, DiLalla is able to specifically filter for these types of threats and view the Malware category in the Declaration of Compromise™ (DoC) covered threats. DoCs are high-fidelity, response-ready, and prioritized alert notifications with correlated evidence signaling only the most serious and imminent threats. This drastically reduces the amount of noise caused by network-based threat detection solutions and virtually eliminates false positives.

SOLUTION SUMMARY

Implemented Stamus Security Platform to increase visibility into their network

Deployed two virtual Stamus Networks appliances

Regularly uses SSP to view protocol logs and flow data, hunt for threats, and identify policy violations

Configured detections to focus on malware, drastically reducing noise

OUTCOME

The Stamus Security Platform gives Penfield Central School District maximum visibility into network traffic across 5000+ endpoints, enables thorough investigation into policy violations and user behaviors, and minimizes false positives and alert fatigue — all while functioning in their preferred environment and without requiring their continuous maintenance or support.

SSP gives Penfield a detailed view of their network activity with more data points, more information, and helpful forensic and investigative tools.

> *Stamus Security Platform is easy to run compared to other IDS-like solutions. It requires very little support to maintain and operate. If you are looking for network-based threat detection, then SSP should be on your radar.*
>
> - Mike DiLalla, Sr. Network Technician, Penfield Central School District

With the Stamus Security Platform (SSP), Penfield has added another critical layer of detection and visibility that they didn't have before. To Penfield Central School District, the inclusion of SSP in their security strategy provides additional confidence in their ability to protect their students, staff, and data from cyber threats.

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As organizations face threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. The global leader in Suricata-based network security solutions, Stamus Networks helps enterprise security teams know more, respond sooner and mitigate their risk with insights gathered from cloud and on-premise network activity. Our Stamus Security Platform combines the best of intrusion detection (IDS), network security monitoring (NSM), and network detection and response (NDR) systems into a single solution that exposes serious and imminent threats to critical assets and empowers rapid response.

STAMVS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

✉ contact@stamus-networks.com
www.stamus-networks.com