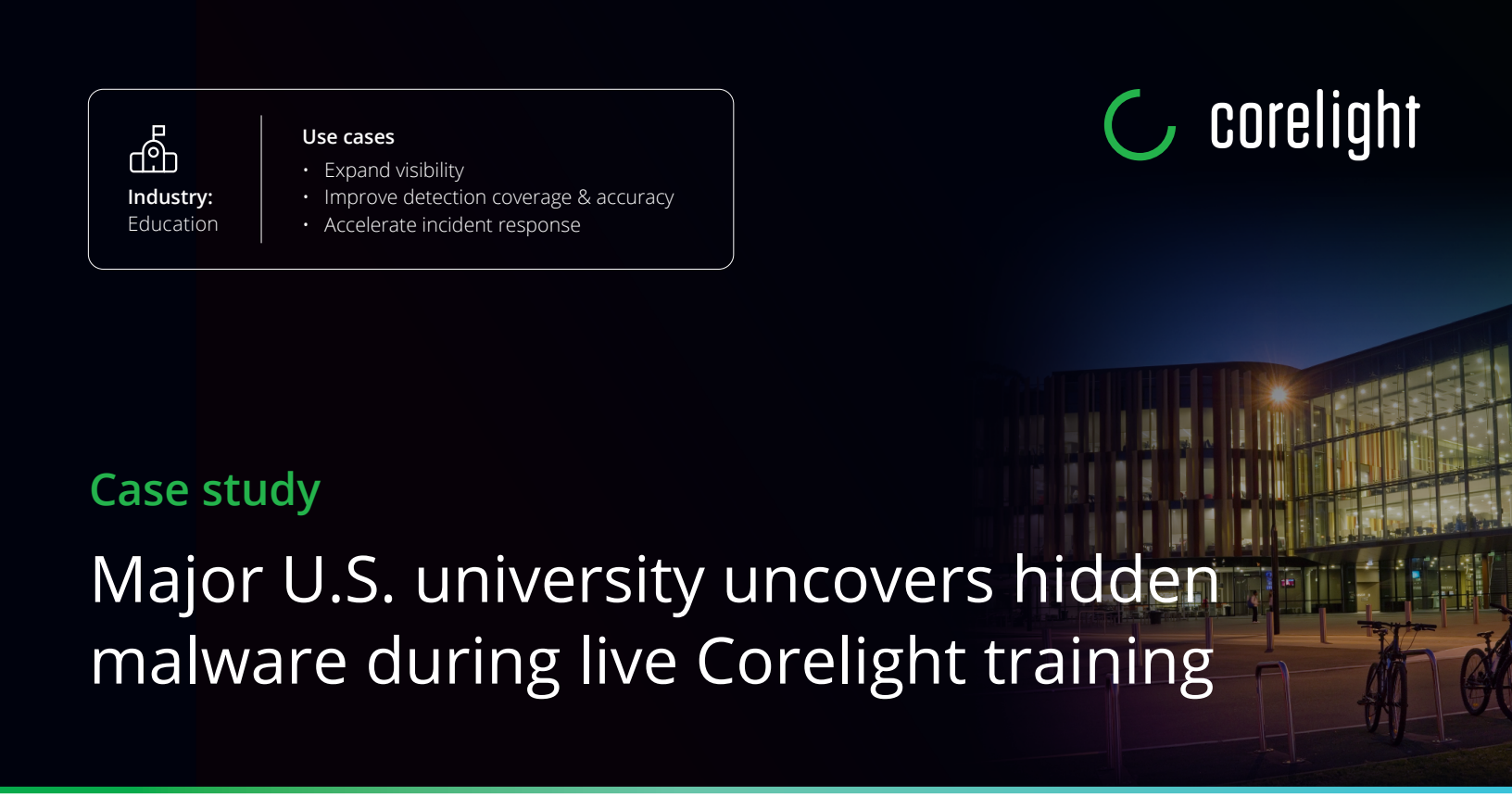
**Industry:**
Education

**Use cases**

- Expand visibility
- Improve detection coverage & accuracy
- Accelerate incident response

corelight



## Case study

# Major U.S. university uncovers hidden malware during live Corelight training

### SITUATION

A major U.S. research university's security team is responsible for protecting a vast and diverse digital environment. While equipped with an enterprise SIEM and endpoint security, the team knew they had significant visibility gaps, especially concerning the thousands of unmanaged student and personal devices on their network. They needed to move from a reactive security posture to a proactive one but required richer network evidence and the skills to use it effectively against today's advanced and evasive threats.

### SOLUTION

The university deployed Corelight to generate comprehensive, protocol-rich network evidence. To accelerate their team's capabilities, they engaged Corelight for a three-day, hands-on virtual training course focused on practical threat hunting within their own environment and using their own data.

### FINDING ACTIVE THREATS ON DAY ONE

During a live threat-hunting exercise in the training, the Corelight instructor guided the university's team to query their new network data against known malware indicators. The results were immediate and impactful:

1. **URSNIF malware correlation:** Corelight's detailed DNS logs flagged a query often associated with **URSNIF** (also known as Gozi), a notorious banking trojan. The evidence allowed the team to begin tracing the infection back to the source endpoint, an evasive threat that had gone undetected by their existing security stack.

   This discovery highlighted a critical security gap inherent in endpoint-only security models. After the team confirmed the threat was not present in their EDR logs, they concluded the source was likely an unmanaged student device using the university's network. Since the university's EDR agent was not on the machine, the threat was completely invisible to their endpoint security, but perfectly visible to Corelight on the network.

2. **Suspicious iPhone uncovered:** Corelight flagged potential **ICMP tunneling** from a staff member's iPhone. This sophisticated technique, often used by evasive threats for covert data exfiltration, would have been invisible without the network-level visibility Corelight provided.

ICMP (Internet Control Message Protocol) is used to exchange control messages between devices, most commonly through Ping (Echo Request and Echo Reply) messages. Because Ping traffic is routinely allowed through firewalls, attackers using a living-off-the-land (LotL) tactic (using authorized tools with malicious intent), sometimes hide their communications inside these payloads—a technique known as ICMP tunneling. Corelight's detailed ICMP logs exposed this covert channel from a staff iPhone, something endpoint or SIEM tools would likely overlook.

**IMMEDIATE ROI AND AN EMPOWERED SECURITY TEAM**

The training session delivered far more than just knowledge—it delivered tangible security wins.

- **Uncovered hidden and evasive threats:** The team found two active, high-fidelity threats that were invisible to their other tools.
- **Accelerated incident response:** They immediately opened incidents to isolate and remediate the compromised devices.
- **Empowered analysts:** The hands-on victory gave the team the practical skills and confidence to hunt for threats independently. The team now integrates **Corelight's rich network evidence** into every investigation. As one engineer confirmed, this new capability has "closed a big visibility gap for us."

By leveraging Corelight's evidence and expert training, the university not only validated its investment in the early days of their deployment but also fundamentally leveled up its ability to defend the campus network.

corelight

To learn more about uncovering hidden malware , request a demo at

**https://corelight.com/contact**

info@corelight.com | 888-547-9497