CYBRAICS

Endpoint devices bypass security tools with peer-to-peer software

Situation

Signature-based endpoint protection tools fail to see the threat.

As a large hospital district specializing in cutting-edge care, our customer knew that their extensive network of healthcare providers made it impossible to control what was running on each system. They invested heavily in endpoint protection tools and restricted peer-to-peer (P2P) software to combat this challenge. However, even with these tools in place, they were unable to detect several instances of P2P software running in their network.

Solution

Multiple P2P services that bypassed endpoint tools are immediately identified.

Cybraics' nLighten immediately detected several instances of P2P downloads and uploads from the 3rd party networks that had gained access to the healthcare provider's primary network. Some users had also changed their default settings in an attempt to hide their use of P2P software and bypass network security. However, nLighten provided a clear view of which devices were using the P2P services, how much data they transferred, and pinpointed the external host machines. In one case, the user was a doctor on a tenant network who had installed a torrent app on his phone.

Success

Security gaps closed and network protected.

The nLighten platform's behavioral detection capabilities proved more than capable by immediately identifying the unauthorized P2P software and correlating the network activity. Then, with clear cases to remediate, the hospital shut down the offending systems and stopped the risky actions by a few that exposed the entire district to potential threats.

> *The thing that really stands out for me and my team is the dashboards. Very nice. It weeds out the noise and goes right to the crux of the issue.*

Filter out the noise with nLighten™ — the fully autonomous SIEM and MDR platform that turns scattered data into powerful, actionable insights

Visit Cybraics.com to Schedule a Demo