GREYNOISE | corelight

Joint Solution

How Corelight and GreyNoise Find Threats Before They Have a Name

Stop emerging attacks as they

Security Operations Centers (SOCs) are caught in a crossfire. On one side, they are inundated with a massive volume of "internet noise"—benign scanners, misconfigured services, and research bots that trigger thousands of low-value alerts, consuming valuable analyst time. This continuous alert storm makes it easy to miss the real, targeted threats.

On the other side, attackers are moving faster than ever, exploiting zero-day vulnerabilities in critical edge devices before a patch or indicator of compromise or attack is ever published. Adversaries hunt for exposed management interfaces, exploit specific vulnerabilities, and compromise systems weeks before a threat is ever officially known, leaving teams who rely on traditional threat intelligence completely blind until it's too late.

Noise hides the signal, leaving critical vulnerabilities exposed.

Seeing the Attack Before the IOC

Corelight and GreyNoise are addressing this head-on by combining to provide a comprehensive, two-layered defense that empowers security teams to solve both challenges.

The solution's foundational layer is Corelight's Open NDR Platform, which establishes a digital tripwire for the entire network. It operates by capturing what it calls "ground-truth network evidence"—a complete and detailed record of all network traffic, which is then processed into high-fidelity Zeek logs. This rich data is subsequently fused with an integrated high-fidelity threat intelligence feed, powered by CrowdStrike. This potent combination of raw evidence and curated intelligence allows Corelight to deploy a sophisticated, multi-layered detection engine, leveraging artificial intelligence, behavioral analysis, and traditional signature matching to identify both known and novel threats with significant precision.

The second layer comes from GreyNoise, which provides global context by analyzing internet-wide scanning traffic. It sifts through billions of daily connection attempts to determine the intent behind an IP address. GreyNoise separates the benign "noise"—like research scanners and common cloud services—from actual threats, such as opportunistic attackers or targeted campaigns scanning for a new vulnerability. This filters out distractions and provides an essential early warning for emerging attacks.

When integrated into CrowdStrike's Falcon Next-Gen SIEM, this solution provides unparalleled visibility. Analysts see Corelight's rich network evidence automatically enriched with GreyNoise's context in a single pane of glass. This fusion allows them to instantly distinguish ignorable noise from a rising zero-day threat, enabling them to stop attackers before the breach.

Use Case: Hunting the F5 Threat Before the IOC

The F5 BIG-IP breach was a perfect example of attackers exploiting the management plane before defenders had a "Proof of Concept" (PoC) or signature. Here is how the joint solution turns the tables.

1. The Early Warning (GreyNoise): GreyNoise observes a sudden, anomalous spike in scanning activity targeting F5 BIG-IP management interfaces across the internet. It tags this activity as malicious and opportunistic, not a known benign scanner.

2. The Investigation (Corelight): An analyst in the CrowdStrike SIEM sees the GreyNoise alert. They immediately pivot to their Corelight data to ask: "Are any of those scanning IPs talking to my F5 devices?"

3. The Ground Truth (Corelight): The analyst finds a match. Corelight's conn.log shows one of the malicious IPs connected to their BIG-IP device, and the ssh.log shows an unusual successful login from that IP to the management interface.

4. The Result: The SOC identifies and isolates the compromised device days or weeks before an official IOC is released, preventing the attacker from gaining a foothold. They successfully hunted an unknown threat by correlating global context with on-prem evidence.

Stop reacting and start defending. See how Corelight's ground-truth evidence at corelight.com and GreyNoise's internet-wide context at greynoise.io can help you find threats before they have a name.