Use Cases

|  |  |  |
| --- | --- | --- |
| **Incident Response & Forensics** | **Security Visibility & Threat Hunting** | **Networking Monitoring & Troubleshooting** |
| **Malware**  Quickly pinpoint the impact of a  malware attack by searching the network  logs for file hashes and then pivoting on  connections to see all hosts and connections that interacted with the malware.. | **Rare Certificates Visibility:**  Import the network logs to a SIEM and monitor the top rare certificates in the network in real-time to find unique certs that can signal an attack in progress. | **Load Balancer Troubleshooting:**  Use the network logs to diagnose and prove an A10 load balancer performance problem that can’t be replicated in a lab environment. |
| **DDoS Attack**:  Using network logs to detect the origin and directionality of a DDoS attack and the affected endpoints where other security tools missed the attack and/or got the directionality wrong (internal systems hijacked to talk \*out\* to China). | **PCAP Investigations:**  Running Corelight alongside PCAP capture and using the network logs to identify interesting/risky network logs and pivoting to the associated PCAP to obtain and investigate the full payload. | **Application Monitoring:**  Import the network logs to a SIEM and monitor the applications running in the environment to understand when new software is introduced by different business units and/or by employees. |
|  | **DNS Visibility:**  Import the network DNS logs to a SIEM to to be able to quickly search, summarize, and identify DNS anomalies. |  |
|  | **Web Server Vulnerability Management:**  Use network logs to gain visibility into thousands of internal and external web servers and their software versions for vulnerability visibility and management. |  |