



10-10-2026

Zeek

Zeek (formerly Bro) is a powerful open-source network analysis framework that provides a comprehensive platform for security monitoring, intrusion detection, and network forensics.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for [Splunk Enterprise](#), [Splunk Cloud Platform](#) or [Splunk Observability Cloud](#).

Getting data in

Source	Add-ons and Apps	Guidance
Zeek Zeek sits on a hardware, software, virtual, or cloud platform that observes network traffic and generates high-fidelity logs, extracting critical information such as connection records, DNS queries, HTTP requests, and file transfers, which are invaluable for security analysts. Software administrators use Zeek data in a Splunk deployment to analyze packet capture data directly or use it as a contextual data feed to correlate with other vulnerability related data in the Splunk platform. In the Common Information Model, Zeek data can be mapped to multiple data models, such as Certificates or Network Resolution, depending on the field.	Splunk platform Technical Add-on for Zeek	Splunk Lantern Articles • Detecting software supply chain attacks • Monitoring a network for DNS exfiltration • Detecting Supernova web shell malware • Monitoring ingress and egress

Source	Add-ons and Apps	Guidance
		traffic across Operational Technology perimeters • Monitoring common Operational Technology protocol ports