corelight

Zeek* logs

50+ data types and protocols.

If your typical response to alerts involves digging through piles of PCAP files or trying to piece together data through thin NetFlow records, there's a better way. It's Zeek. Zeek generates a wide range of rich network information, including logs for:

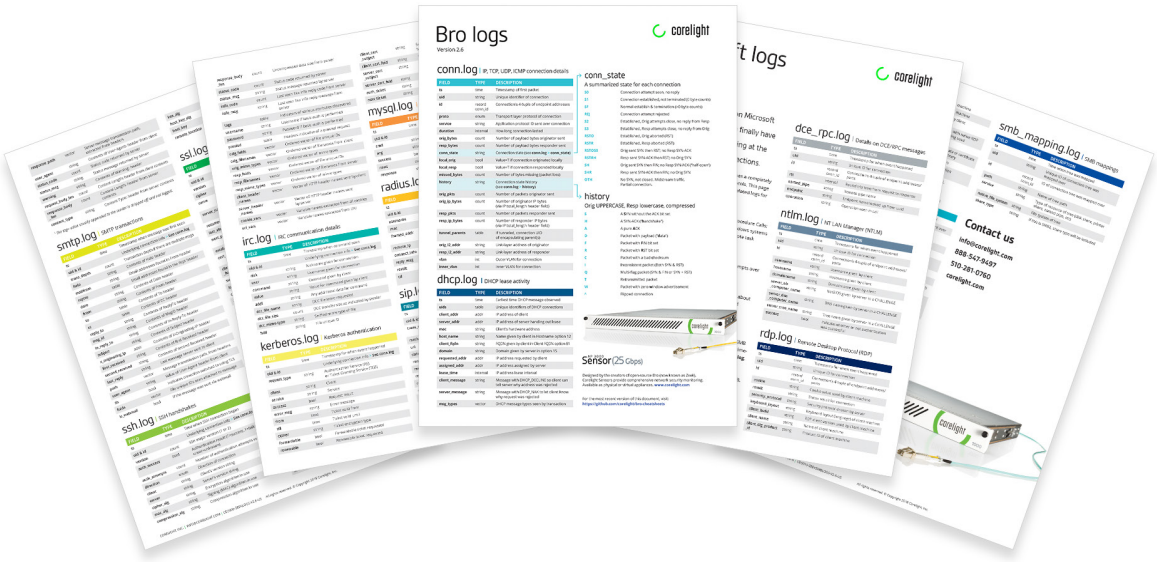
- barnyard2
- broker
- capture loss
- cluster
- config
- conn
- conn history
- conn state
- dce rpc
- dhcp
- dnp3
- dns
- dpd
- files
- ftp
- http
- intel
- irc
- kerberos
- known certs
- known hosts
- known modbus
- known services
- loaded scripts
- modbus
- modbus register change
- mysql
- netcontrol
- netcontrol catch release
- netcontrol drop
- netcontrol shunt
- notice
- notice alarm
- ntlm
- ocsp
- openflow
- packet filter
- pe
- radius
- rdp
- reporter
- rfb
- signatures
- sip
- smb cmd
- smb files
- smb mapping
- smtp
- snmp
- socks
- software
- ssh
- ssl
- stats
- syslog
- traceroute
- tunnel
- unified2
- weird
- weird stats
- x509

*Formerly known as Bro.

Better network security starts with better data.

Zeek (formerly known as Bro) is the world's most powerful framework for transforming network traffic into actionable data for analysis, forensics, and real-time response. Tens of thousands of organizations, including some of the largest enterprises in the world, rely on Zeek to protect their systems and networks. Zeek logs give you the best view of your network, telling you exactly what's happening in one structured and organized place.

Free cheatsheets for release 2.6 include 18 of the most popular logs, with more DHCP fields and updated descriptions, plus five logs for Microsoft® SMB:



Download yours at: https://github.com/corelight/bro-cheatsheets

corelight

Corelight was founded by the creators and core technologists behind Zeek, and we aim to build exceptional tools for network monitoring and cybersecurity. Our products come from the same people who create features, commit changes, and fix bugs in the open-source Zeek codebase.

We make the **world's networks safer.**

Contact us

For more information or to schedule an evaluation:

info@corelight.com

888-547-9497

510-281-0760

corelight.com