corelight | Tor

Joint solution

Corelight integration for the Tor Network Exit List Service

Continuous, bidirectional Tor visibility for enhanced threat investigation and compliance

Security teams often lack visibility into network connections and the IP addresses originating from Tor exit nodes, a blind spot that carries real consequences. For one, compliance frameworks, such as PCI-DSS, SOC 2, FedRAMP, and CMMC, increasingly require organizations to demonstrate effective monitoring of anonymization network usage. Failing to meet that standard is not only a compliance risk, it's also a signal that your defenses have a visibility gap adversaries can exploit.

Compounding the problem is that the Tor Exit List of IP addresses contains well over 1,000 IP addresses that rotate daily as Tor exit nodes join and leave the network. Static block lists go stale within days, so without an auto-updating feed, even the best-intentioned security teams are working with outdated intelligence.

Corelight provides continuous, bidirectional Tor visibility

Built on the design patterns of elite defenders, Corelight's Open NDR Platform provides SOC teams with visibility and ground-truth network evidence to accelerate threat investigations and address regulatory compliance requirements. This integration extends that capability to one of the most commonly abused network anonymization vectors in use today.

SOLUTION HIGHLIGHTS

Bidirectional Tor connection visibility with detection of inbound and outbound Tor connections

Auto-update of Tor bulk exit IP list ensures intelligence stays current without manual intervention or static list management

Compliance-ready evidence to show auditors that Tor network usage is being actively monitored

In addition to monitoring for outbound connections to the Tor network, support for the Tor Exit List Service enables Corelight customers to identify and log all inbound connections from Tor exit nodes hitting your infrastructure. Here, Corelight automatically and continuously fetches the Tor Exit List of IP addresses directly to the sensor, giving SOC teams immediate, actionable intelligence without adding operational complexity. The result is clear bidirectional visibility for all Tor connections. No manual updating or stale data.

For organizations that need to adhere to regulatory requirements and regular compliance audits, Corelight's integration with the Tor network provides the documented, evidence-backed awareness that auditors require.

For threat responders, it provides the context needed to identify malicious activity initiated via Tor exit nodes, which are frequently used as entry points for cyberattacks or unauthorized data access.

corelight

To learn more about the Corelight integration for Tor, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497

All rights reserved. © Copyright 2026 Corelight, Inc.