White Paper

Corelight Cybersecurity Solutions and Trusted Internet Connection (TIC) 3.0

Introduction

The Trusted Internet Connection (TIC) initiative was implemented in 2007 with the aim of helping federal agencies consolidate networks and standardize perimeter security defenses. The rise in federal cloud adoption and proliferation of end-user mobile and cloud applications, however, substantially degraded the effectiveness of the traditional network perimeter defense model. The updated TIC 3.0 guidance gives federal agencies a much more adaptable framework designed to keep pace with emerging threats and new technologies.

How Corelight Supports Modernizing Federal Networks

Corelight's Open Network Detection & Response (NDR) platform supports federal entities in achieving the following TIC 3.0 security objectives:

- Manage Traffic
- Protect Traffic Confidentiality
- Ensure Service Resiliency
- Ensure Effective Response

Corelight delivers comprehensive network evidence and analytical insight that gives organizations powerful network visibility and the rich network evidence needed to inform effective response actions and policy enforcement capabilities across on-premise, cloud, and hybrid environments.

Corelight's open NDR platform merges Zeek network security monitoring with a Suricata intrusion detection (IDS) and proprietary network security analytics and packet capture technology (Smart PCAP). Our customers use the platform to make fast sense of traffic on-premise and in the cloud, dramatically accelerating incident response, increasing analyst effectiveness and unlocking powerful threat hunting and detection capabilities. Notably, Corelight can also deliver critical security operations capabilities in Zero Trust environments such as continuous verification.

Taking Federal Networks from TIC 2.2 to TIC 3.0

The TIC 2.2 network security architecture called for backhauling all traffic through an agency's TIC to create a centralized enforcement and monitoring point. The TIC 3.0[1] architecture expanded the scope to accommodate modern cloud and hybrid environments where traffic lives outside the traditional network perimeter. The TIC 3.0 Security Capabilities Catalog[2] provides an index of security capabilities which are categorized as:

- **Universal Security Capabilities:** Enterprise-level security capabilities that outline guiding principles for TIC use cases.
- **Policy Enforcement Point Security Capabilities:** Network-level security capabilities that inform technical implementation for relevant use cases.

Corelight data addresses these security capabilities by providing network evidence allowing organizations to audit trust levels of their distributed, networked environments to successfully apply the commensurate security policy. Fundamentally, Corelight can help organizations transition from 2.2 to 3.0 TIC architectures by:

- Providing comprehensive and consistent traffic visibility across on-premise, cloud, and hybrid deployments to facilitate TIC 3.0 security objectives.
- Providing rich network evidence to inform response capabilities and extend the dimensions of playbook creation.
- Supporting ongoing verification of TIC 3.0 policy enforcement points providing security teams with evidence of compliance, or non-compliance.

The table that follows highlights a few of the capabilities and use cases where Corelight can deliver network evidence. For a complete list of Corelight's security capabilities mapped to TIC 3.0, please contact a sales representative.

[1] The TIC 3.0 program defines five standalone security objectives that are designed to guide network architectures and implementations. See the appendix to highlight Corelight's open NDR platform relevant capabilities.

[2] https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Security%20Capabilities%20Catalog%20v2.0_0.pdf

Table 3: A Sample of Corelight Security Capabilities

TIC Capability	Description	Corelight Security Capabilities & Use Cases
Universal security capabilities		
Intrusion Detection and Prevention Systems	Intrusion detection systems detect and report malicious activity. Intrusion prevention systems attempt to stop the activity	- Suricata IDS - IDS ruleset optimization - 3rd party intel integration Sample use case A Corelight customer implemented a new IDS ruleset update to detect active exploits of a newly identified zero-day vulnerability to understand if the organization is currently under attack.
Central Log Management with Analysis	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and where the security analysis aids in discovery and response to malicious activity.	- Log storage & analysis via multiple SIEMs - Custom Corelight analytical content - Corelight machine learning Sample use case Corelight customers stream network evidence and alerts to Splunk, Elastic, and other SIEMs, using a SIEM compliant information model (e.g.,CIM, ECS) to accelerate IR investigations or feed machine learning algorithms.
Vulnerability Management	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	- Software version visibility and inventory - Out-of-the-box integration vulnerability management tools Sample use case A customer integrated Corelight's software logging capabilities with a vulnerability database to automatically flag vulnerable systems seen communicating on the network.

TIC Capability	Description	Corelight Security Capabilities
Policy Enforcement Point Capabilities		
Data Loss Prevention (DLP)	Data loss prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	- Corelight's network monitoring and custom analytic scripting capabilities can help verify that PII is not exiting the network - Protocol visibility Sample use case A Corelight customer deployed a community-developed script to automatically detect when unencrypted Social Security numbers were exiting their network.
Encryption for Email Transmission	Email services are configured to use encrypted connections, when possible, for communications between clients and other email servers.	- Email protocol visibility to ensure compliance Sample use case: A Corelight customer leveraged Corelight's encrypted traffic analysis and email protocol visibility to ensure ongoing compliance with email encryption policies.
Certificate Transparency Log Monitoring	Certificate transparency log monitoring allows agencies to discover when new certificates are issued for agency domains.	- Certificate inventory - Certificate analytics Sample use case A customer used Corelight's certificate visibility capabilities to discover when new or expired certificates were observed on their network.

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497