Corelight Investigator Security Measures

These Corelight Investigator Security Measures ("**Security Measures**") set forth the administrative, physical and technical security measures that Corelight implements and maintains to protect Customer Data in Corelight Investigator. As security threats change over time, Corelight continues to update its security program and strategy to protect Customer Data and its Cloud Products in accordance with industry standard practices. As such, Corelight reserves the right to update these Security Measures from time to time; provided, however, any update will not materially reduce the overall protections set forth in this document. The then-current Security Measures are available at www.corelight.com/legal/security-measures. These Security Measures does not apply to any (a) Products and/or features that are identified as No-Charge Offerings, or any similar Products and/or features offered by Corelight or (b) on-premise component(s).

Capitalized terms used and not defined in these Security Measures have the meanings given to them in the Corelight Customer Agreement located at https://www.corelight.com/legal/agreements (or such successor URL as may be designated by Corelight).

1. **ARCHITECTURE & DEPLOYMENT MODEL**.

   1.1. **Overview**. The Corelight Investigator platform ("**Investigator**") is delivered using a hosted, software-as-a-service ("**SaaS**") model. Investigator operates on a cloud-native platform that is built on Amazon Web Services ("**AWS**"). Under the AWS "shared responsibility model", AWS provides physical and network security while Corelight is responsible for building and running a secure and highly-available application.

   1.2. **Hosting Regions**. Investigator offers a number of supported regions ("**Investigator Regions**") that consist of AWS Regions. Each AWS Region contains multiple Availability Zones ("**AZs**") consisting of one or more individual data centers, each with redundant power, networking, and connectivity, and housed in separate facilities. Corelight deploys Investigator in multiple AZs to provide seamless high availability and disaster recovery capabilities.

   1.3. **Hosting Location of Customer Data**. Customer Data is hosted in the Investigator Region that Customer selects when its instance is provisioned, but note that Customer's Users may access Customer's Investigator instance from anywhere in the world. As of the publication date of these Security Measures, the following Investigator Regions are available:

Investigator Region	AWS Region
EU	Germany
UAE	United Arab Emirates
USA	US West

   1.4. **Web Application Security**. Investigator leverages AWS Shield and AWS WAF together to provide layered web application security. AWS Shield protects against DDoS attacks whereas AWS WAF protects against exploits on web applications (such as SQL injection or XSS).

   1.5. **Application Architecture**. The Investigator application is deployed in an AWS Virtual Private Cloud ("**VPC**"). Investigator's VPC security infrastructure ensures data never co-mingles across tenants and customers.

      (a) **Multi-Tenant**. Investigator separates Customer Data using logical identifiers. Customer Data is tagged with a unique customer identifier that is assigned to segregate Customer Data ownership. Investigator is designed and built to identify and allow authorized access only to and from Customer Data identified with customer-specific tags. These controls prevent other customers from having access to Customer Data.

2. **SECURITY AUDITS & CERTIFICATIONS**.

   2.1. Corelight uses independent third-party auditors to assess Investigator at least annually, as described in the following audits and certifications ("**Third-Party Audits**"):

      (a) SOC 2 Type II

   2.2. For additional information relating to Investigator's Third-Party Audits and other-related security documentation, please visit https://corelight-inc.trustshare.com/home.

2.3. To the extent Corelight decides to discontinue a Third-Party Audit, Corelight will adopt or maintain an equivalent, industry-recognized framework.

3. **ENCRYPTION**.

3.1. **Encryption in Transit**. Customer Data is encrypted when in transit using TLS v1.2.

3.2. **Encryption at Rest**. Customer Data is encrypted at rest in AWS using the 256-bit Advanced Encryption Standard algorithm ("**AES-256**"). AWS does not have access to unencrypted Customer Data. Investigator uses AWS Key Management Service ("**KMS**") to manage encryption keys for data at rest. Investigator's encryption key management involves regular rotation of encryption keys.

4. **ACCESS CONTROLS**.

4.1. **Provisioning Access**. Corelight follows the principles of least privilege through a role-based access control mechanism when provisioning system access. Corelight personnel access to Customer Data is restricted based on if their job role or job responsibilities specifically require it. Access to Customer Data is promptly removed upon termination of employment. In order to access Investigator's production environment, an authorized user must have a unique username and password and multi-factor authentication enabled. Access rights to Investigator's production environment are reviewed at least quarterly. Before an authorized user is granted access to Investigator's production environment, access must be approved by management.

4.2. **Password Controls**. At a minimum, Corelight's password management policy for Corelight personnel follows the NIST 800-63B guidance and requires the use of longer character lengths, special characters, and multi-factor authentication.

5. **SYSTEM & NETWORK SECURITY CONTROLS**.

5.1. **Platform Controls**.

(a) **Network Segregation**. Investigator leverages multiple layers of network security controls, including network-level isolation, for segregation between Investigator's development and production environments.

(b) **Firewalls & Security Groups**. Corelight protects the Investigator platform using industry standard firewall and/or security groups technology with deny-all default policies (i.e., resources cannot communicate with each other unless permitted).

5.2. **Monitoring & Logging**. Corelight uses its own products to monitor, detect and respond to security events.

(a) **Intrusion Detection Systems**. Investigator also leverages security capabilities provided natively by AWS for security detection.

(b) **Infrastructure Logs**. Corelight uses monitoring tools and services to log certain activities and changes within the Investigator platform. These logs are further monitored, analyzed, and are securely stored for ninety days.

5.3. **Endpoint Controls**. For access to the Investigator platform, Corelight personnel use Corelight-issued laptops which utilize full disk encryption, anti-malware software, automatic patching configurations, screen lock with automatic activation features, and periodic scanning for restricted/prohibited software.

6. **ADMINISTRATIVE CONTROLS**.

6.1. **Governance**. Corelight's chief information security officer ("**CISO**") leads Corelight's information security program and oversees a dedicated information security team. The CISO develops, reviews and approves (together with other internal stakeholders) Corelight's Security Policies (as defined below).

6.2. **Policies & Procedures**. Corelight maintains information security, use and management policies (collectively, "**Security Policies**") designed to educate employees regarding their responsibilities with respect to Corelight's information security (including imposing disciplinary measures for failure to abide by such policies). The Security Policies are evaluated and updated at least annually and are made available via the corporate intranet.

6.3. **Personnel Screening**. All Corelight personnel undergo background checks prior to onboarding (as permitted by local law), which may include, but are not limited to, criminal record checks, employment history verification,

education verification, and global sanctions and enforcement checks. Corelight uses a third-party provider to conduct screenings, which vary by jurisdiction and comply with applicable local law.

6.4. **Confidentiality Agreements**. All Corelight personnel are required to sign non-disclosure/confidentiality agreements.

6.5. **Personnel Training & Awareness**. Corelight personnel receive training on the Security Policies upon hire and refresher training annually. Employees are required to certify and agree to the Security Policies and personnel who violate the Security Policies are subject to disciplinary action, including warnings, suspension and up to (and including) termination. Corelight also conducts ongoing awareness of emerging security threats through various mechanisms, including simulated security-related incidents (e.g., phishing campaigns).

7. **PHYSICAL & ENVIRONMENTAL CONTROLS**. Customer Data is not hosted at Corelight's corporate offices. To ensure that AWS has appropriate physical and environmental controls for its data centers hosting Investigator, Corelight regularly reviews those controls as audited under AWS's third-party audits and certifications. Corelight ensures that AWS will have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, will include, but are not limited to, the following:

- Physical access to the facilities are controlled at building ingress points;
- Visitors are required to present ID and are signed in;
- Physical access privileges are reviewed regularly;
- Facilities utilize monitor and alarm response procedures;
- Use of CCTV;
- Fire detection and protection systems;
- Power back-up and redundancy systems; and
- Climate control systems.

8. **SECURE DEVELOPMENT**. Corelight applies security by design principles throughout the secure development lifecycle ("**SDLC**"). Corelight also applies the SDLC standard to perform numerous security-related activities for its software applications across different phases of the product creation lifecycle, from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before deploying new software or code, (b) open source security scans, (c) static and dynamic application security testing, (d) network vulnerability scans, and (e) external penetration testing.

8.1. **Change Management**. Corelight maintains a documented change management program for Investigator. Corelight utilizes a code versioning control system to maintain the integrity and security of Investigator's source code. Access privileges to the source code repository are reviewed periodically and limited to authorized personnel. Corelight maintains a documented change management program for Investigator. This change management program includes logically or physically separate environments from production for all development and testing.

9. **VULNERABILITY MANAGEMENT**. Corelight maintains controls and policies to mitigate the risk of security vulnerabilities in a measurable time frame that balances risk and the business and operational requirements.

9.1. **Monitoring & Detection**.

(a) Investigator's cloud environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code.

(b) Corelight uses third-party tooling to conduct vulnerability scans regularly to assess vulnerabilities in Investigator's cloud environment. Corelight also conducts regular dynamic application security tests ("**DAST**") to assess the Investigator application, including APIs, in a runtime environment to identify vulnerabilities and exploitable flaws.

(c) Corelight reviews external threat intelligence, including US-CERT vulnerability announcements and other trusted sources of vulnerability reports.

9.2. **Verification & Mitigation**. Corelight verifies identified vulnerabilities and assesses them according to industry-standard ratings systems. Corelight leverages the National Vulnerability Database's Common Vulnerability Scoring System ("**CVSS**"), or where applicable, the U.S.-Cert rating, combined with an internal analysis of contextual risk to determine criticality. Vulnerabilities meeting defined risk criteria are prioritized for remediation and/or mitigation based on their impact to Investigator in accordance with Corelight's internal criticality SLA matrix.

10. **BACKUPS, CONTINUITY, AND DISASTER RECOVERY**.

10.1. **Backups**. Investigator performs regular backups of Customer Data, which is hosted on AWS's data center infrastructure. Customer Data that is backed up is retained redundantly across multiple AZs and encrypted in transit and at rest. Investigator's backup schedule and disaster recovery program are designed to meet the recovery point objective ("**RPO**") and recovery time objective ("**RTO**") of 2 hours and 24 hours, respectively.

10.2. **SaaS Resilience & Continuity**. Since Investigator is deployed across multiple AZs in each AWS Region, Investigator can continue operating in the event a single AZ goes down. Should that occur, Corelight automatically scales resources in the still-operating AZs, and monitors overall regional capacity and utilization.

10.3. **Business Continuity and Disaster Recovery**. Corelight Business Continuity ("**BC**") and Disaster Recovery ("**DR**") plans are reviewed and tests are conducted annually.

11. **BREACH DETECTION & RESPONSE**.

11.1. **Detection**. Corelight maintains a security incident response team ("**SIRT**") to identify, report and appropriately respond to security incidents. The SIRT employs an incident response framework to manage and minimize the effects of unplanned security incidents. Customers may notify Corelight of suspected vulnerability or incident by submitting a technical support case for Corelight's evaluation.

11.2. **Security Breach**. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed Security Breaches, Corelight will take appropriate, reasonable steps to minimize unauthorized disclosure. "**Security Breach**" means any breach of Corelight's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Corelight. Security Breaches will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

11.3. **Communications & Cooperation**. In the event of a Security Breach for which that Customer is impacted, Corelight will: (a) notify Customer in writing without undue delay after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Corelight will reasonably cooperate with and provide to Customer information in its possession to assist Customer in meeting Customer's obligations to report a Security Breach as required under applicable data protection laws, taking into account the nature of the processing, the information available to Corelight, and any restrictions on disclosing the information (such as confidentiality).

12. **THIRD PARTY VENDOR MANAGEMENT**. Corelight has implemented a vendor management program that applies the appropriate technical and organizational security controls that are proportional to the type of service the third-party vendor is providing and any associated security-related risks. Prospective third-party vendors are vetted through a process that ensures they comply with, and will continue to comply with, Corelight's confidentiality, security, and privacy requirements for the duration of their relationship with Corelight. Third-party vendors that process Customer Data are subject to more stringent technical and organizational security controls which are reflected in Corelight's contractual agreement with such third-party vendors. In addition, Corelight regularly reviews (a) each critical third-party vendor engaged against Corelight's security and business continuity standards; (b) each third-party vendor's access to Customer Data and its technical and organizational security controls to protect Customer Confidential Information; and (c) evolving legal or regulatory requirements that impact Corelight's security program or processing of Customer Data. Corelight's current third-party vendors that are sub-processors are available at www.corelight.com/legal/subprocessors.

13. **DATA DELETION**.

13.1. **By Customer**. By default, Investigator retains: (a) alerts and detections for a ninety-day period; and (b) Zeek and Suricata logs for a thirty-day period unless additional log retention days are purchased ((a) and (b), each a "**Retention Period**"). The respective categories of Customer Data will be erased at the end of the applicable Retention Period, and new Customer Data will be stored in its place, so that at any time during the Subscription Term, Customer Data for the most recent Retention Period will be accessible to Customer. Investigator also provides Customer controls for the deletion of Customer Data, as further described in the Documentation.

13.2. **By Corelight**. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any Subscription Term (including any applicable retrieval period) Corelight will promptly delete any remaining Customer Data.

14. **SECURITY TOOLS FOR CUSTOMERS**.

14.1. **Configurable Security Options**. Customers can configure organization-wide security policies for Investigator accounts; configuration options include:

(a) **Investigator Support for Single Sign-On (SSO)**. Investigator supports SSO capability through SAML (Security Assertion Markup Language).

(b) **If not utilizing SSO**. Investigator supports password policies, minimum password length and complexity, user lockouts after repeated failed login attempts, and disallowed password reuse; and password encryption in transit as well as at rest.

(c) **Role-Based Access Controls**. Investigator features role-based access controls to enable customers to implement fine-grained access management for users within their Investigator deployments.