Cyber Lorica™ SIEM & 24/7 Monitoring

For [Company]

Prepared for: [Manager]
[Title]
[Company]

Prepared by: Jeremy Rasmussen, CISSP, CEH, PMP
Director of Cybersecurity
Abacode, LLC
[Publish Date]
Proposal number: ****

Date: [Publish Date]

Dear [Manager],

Having visibility into your enterprise and being able to correlate security-relevant events and raise alerts for appropriate incident response is critical to network security. Abacode offers the Cyber Lorica™ solution as a subscription-based program that includes the installation and configuration of a Security Information and Event Management (SIEM) and Intrusion Detection System (IDS) platform, as well as the 24/7 monitoring service in a bundle. In addition, we provide a full spectrum of cybersecurity consulting services to help you plan and maintain governance, assess your security posture, and train your staff to create a culture of security. Our value proposition is as follows:

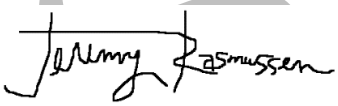
* We serve as your trusted cybersecurity advisors: To provide due diligence in defending against constant hacker attacks, a company would need to hire full-time security personnel with the background, knowledge, and training to analyze complex cyber events 24 hours a day, 7 days a week. Staffing such a team would likely require [Company] to retain a minimum-security staff of six trained personnel.

* We provide separation of duties: An organization's IT staff, third-party managed IT, and cloud services are responsible for configuration and lockdown of enterprise security. A separate entity should be responsible for the audit and monitoring of the enterprise, in order to avoid conflict of interest and ensure separation of duties consistent with governance best practice.

* We help limit your liability: The average cost per record for a data breach is more than $154.1 This stems from replacement and cleanup, legal, fines, loss of reputation and customer base, and other costs. If a company has, say, 50,000 customer records, then its potential exposure is a staggering $7.7 million. By implementing the Cyber Lorica program, we help minimize the risk of successful attacks and limit the damage from breaches so that your exposure and liability are drastically reduced.

Please contact us at jeremy.rasmussen@abacode.com or 813-321-4949 with any questions. We look forward to the opportunity to work with you.

Best Regards,



Jeremy Rasmussen, CISSP, CEH, PMP
Cybersecurity Director
jeremy.rasmussen@abacode.com
www.abacode.com

Contents

Cyber Lorica™ SIEM and 24/7 Monitoring

Having visibility into your enterprise and being able to correlate security-relevant events and raise alerts for appropriate incident response is critical to network security. Abacode offers the **Cyber Lorica™** solution as a subscription-based program that includes the installation and configuration of a Security Information and Event Management (SIEM) platform as well as 24/7 monitoring service in a bundle.

Our value proposition:

- **We serve as your trusted cybersecurity advisors**: To provide due diligence in defending against constant hacker attacks, a company would need to hire full-time security personnel with the background, knowledge, and training to analyze complex cyber events 24 hours a day, 7 days a week. Staffing such a team would entail a minimum of six personnel for your monitoring requirements. We offer our Cyber Lorica™ monitoring tailored to your company's needs.
- **We provide separation of duties**: An organization's IT staff and third-party managed IT and cloud services are responsible for configuration and lockdown of enterprise security. A separate entity should be responsible for the audit and monitoring of the enterprise to avoid conflict of interest and ensure separation of duties consistent with governance best practice.
- **We help limit your liability**: The average cost per record for a data breach is more than $154.[1] This stems from replacement and cleanup, legal, fines, loss of reputation and customer base, and other costs. If a company has, say, 50,000 customer records, then its potential exposure is a staggering $7.7 million. By implementing the Cyber Lorica™ program, we help minimize the risk of successful attacks and limit the damage from breaches so that your exposure and liability are drastically reduced.
- **We aid in forensics / incident response:** An organization can create an environment of "forensic readiness"[2] by engaging in activities to maximize an environment's ability to collect credible digital evidence and thus minimize the cost of forensics during an incident response. Cyber Lorica™ aggregates all log and alert data in a centralized location, greatly aiding in agile and effective incident response.
- **HIPAA Compliance**: Cyber Lorica helps organizations meet the HIPAA log auditing and aggregation requirements:
    - Section 164.308(a)(1)(ii)(c) – Information system activity review (required), which states organizations must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."
    - Section 164.312(1)(b) – Audit controls (required), which state organizations must "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Project Scope

The Cyber Lorica™ program is comprised of two major components:

[1] Source: 2015 Ponemon Institute Study

[2] Robert Rowlingson, Ph.D: "A Ten Step Process for Forensic Readiness" in the International Journal of Digital Evidence

- **SIEM monitoring platform** that collects, aggregates, and correlates the security information and logs from the critical devices to detect cyber-attack patterns. This SIEM component relies on a network intrusion detection system (IDS) that inspects all inbound and outbound traffic from the Internet. Additionally, this system correlates OS and application level events along with the results of host-based vulnerabilities detection to identify when hosts, applications, and services are being targeted or have been compromised.

- **Fully managed SOC**, wherein Abacode provides the AlienVault software licenses and server appliance costs as part of the monthly subscription rate. Our team of all US-citizen IT Security professionals monitor your security information 24/7 from the Abacode Security Operations Center (SOC), headquartered in Tampa, FL. This team will follow your incident response protocols and provide remediation recommendations when threats and vulnerabilities are detected.

Assumptions: for purposes of this quote, the cost of licensing, configuring, deploying, and maintaining these appliances is rolled into the overall subscription costs for the fully managed Cyber Lorica™ pricing.

Project Activities

The Cyber Lorica™ implementation steps are described below:

- Abacode meets with [Company] to jointly identify and document the network subnets, DNS servers, network devices, servers, and workstations that will be monitored. Additionally, the deployment options are evaluated with the client and either virtual or physical appliance is selected.
- Abacode develops a project plan for the Cyber Lorica™ implementation and schedules the team, date, and time for the initial implementation.
- Abacode reviews the project plan with the client and secures client support for the proposed implementation date.
- Abacode installs and configures the SIEM monitoring platform to aggregate data from the selected devices in collaboration with client personnel utilizing a web conference as detailed in the project plan.
- The Abacode SOC personnel host a web conference with [Company] to discuss the incidence response plan and escalation details. Additionally, the Abacode SOC team will setup expectations and agree on reporting and vulnerability scanning schedule and frequency.

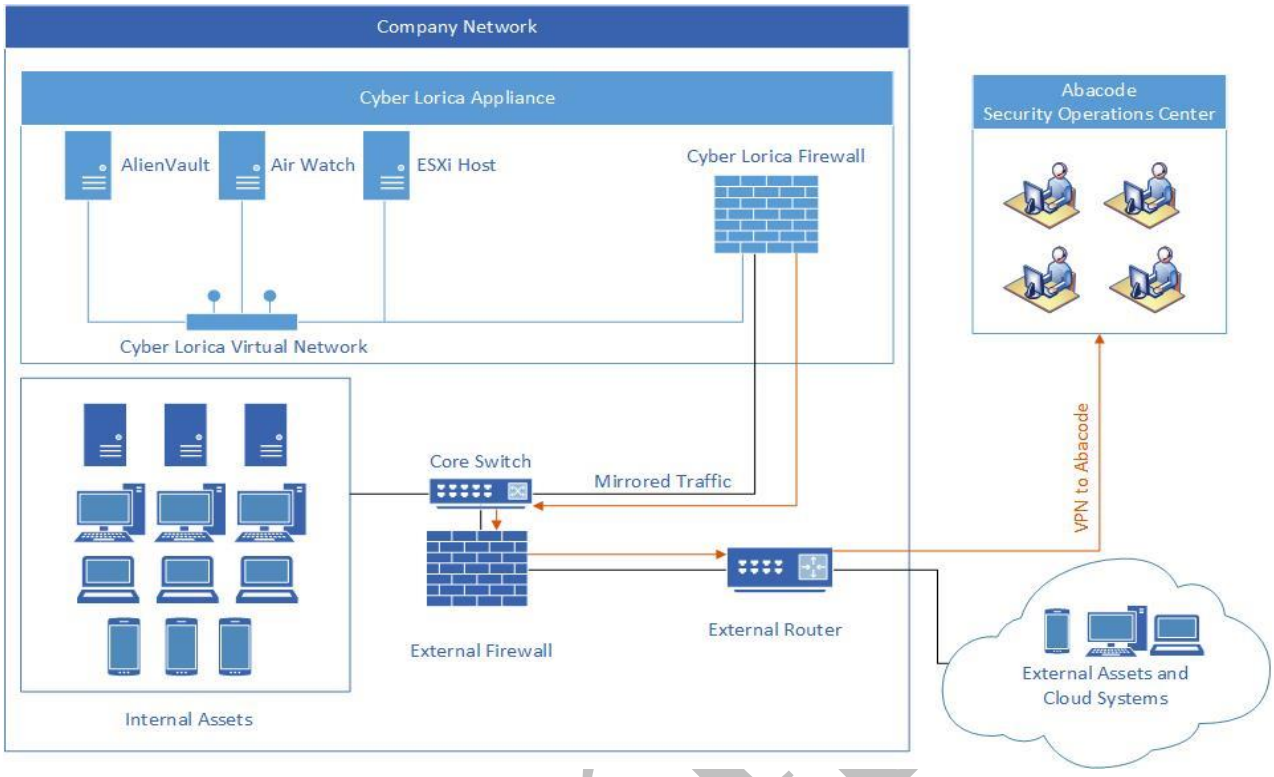


Figure 1. Cyber Lorica™ on premises deployment

Project Deliverables

- Project Plan
- 24/7 Monitoring Tier 1 support in US-based SOC with trained US-citizen IT security staff
- 24/7 Tier 2 support from Project Manager working in conjunction with your IT security staff for incident escalation
- Lab support to validate and reverse engineer serious exploits and threats for remediation
- Technical Interchange Meetings
- Fully licensed software
- Configured SIEM monitoring appliance that aggregates data from enterprise
- Deployment of the solution
- Maintenance and updates of the appliance
- Escalations as detailed in the incident response plan
- Scheduled reports

Project Assumptions

The following assumptions have been used in estimating the effort for this project, and they are critical to the success of the effort:

1. **Management Commitment** – Our experience shows that successful projects require strong management commitment. Executive sponsorship of this project is essential. It is proven that projects with strong executive involvement go more smoothly, produce expected budget results, and have strong client satisfaction.
2. **Key Contacts** - [Company] will provide a single point of contact for project coordination with Abacode. [Company] will also provide a list of key personnel for areas affected by the project to the Abacode Project Manager prior to the project kick-off including: Name, Title, Responsibility, Phone and E-mail. IT operations staff should be available for interview.
3. **Permission** - [Company] gives Abacode permission to conduct testing on its systems and on any third party hosted servers. [Company] will contact and verify complete cooperation of any external hosting agencies.
4. **Facility Access** - [Company] will ensure access to all facilities as necessary and to all documentation in a timely and reasonable manner.
5. **Availability** - [Company] understands that Abacode relies on immediate clarification and resolution regarding the integrity of data / information supplied to Abacode. [Company] will make necessary resources available to answer questions and provide additional detail as necessary.
6. **Project Start Date** - Upon delivery of an executed contract, Abacode will work with [Company] to determine a project start date that both meets your business objectives and allows us to staff the project effectively.
7. **Scheduling** - Project work will be performed during normal business hours. In the event that [Company] requires Abacode to perform work after hours, additional charges will apply.
8. **Scope** - [Company] will provide IP addresses, domain names, etc., included in project scope.

Abacode Responsibilities

1. **Key Contact -** Abacode will provide a single point of contact for project management and coordination with the [Company].
2. **Delivery -** Abacode will dedicate the necessary resources to the project to complete it in the agreed timeframe barring any change in scope or delay by the [Company] in providing information.
3. **Notification** - Abacode will promptly notify [Company] of any incomplete or inaccurate information.
4. **Confidentiality** - Abacode understands and acknowledges the confidential nature of the data and information provided and generated during this process and will protect such with all due caution.
5. **Effort -** Abacode will conduct all efforts in a professional and workmanlike manner and make every effort to ensure no systems are affected by the security testing.
6. **Change Orders -** We will work with you to execute change orders, as appropriate, to clearly communicate additional services and the related fees, which are outside the current scope of this statement of work. We will not incur time on out-of-scope items until a change order is approved by [Company].
7. **Protection of Your Information** - Client confidentiality and protection of client-provided information is a matter of great importance to our team. Clients who trust us with their most sensitive corporate information expect that information to be controlled as strictly as if still in their possession. We apply the following redundant, reinforcing practices to protect client identity and information:
    - Contract correspondence and other administrative written communications to [Company] will be maintained only with Abacode personnel associated with the project.
    - All members of our team are available to sign specific nondisclosure agreements that bind them to protect client identity and project information.
    - At [Company] discretion, our team members can be badged as, and operate as, employees of [Company].

Project Fees

For Abacode, it will be our pleasure to provide [Company] the professional services described in this proposal. We are committed to exceeding your expectations. Below are the different options that we are able to offer you based on the requirements that we have gathered.

Cyber Lorica Option Selection

Option	Device Count	Description	Fee
A	Up to ****	**Option A**-CyberLorica24/7 Security Monitoring for ***most critical device***[1] and Cybersecurity Consulting Services for **one-year contract**.	$ per month
B	Up to ****	**Option B**-CyberLorica24/7 Security Monitoring for ***most critical devices*** and Cybersecurity Consulting Services for **three-year contract**.	$ per month

Acceptance

In order to confirm acceptance of the terms of this proposal, we ask you to select the option that best suits your needs and to provide your signature below. The Statement of Work described in this proposal will be governed by the terms and conditions in the Master Service Agreement to be executed by Abacode and [Company].

☐ Cyber Lorica™ Option **A** (one-year commitment)

☐ Cyber Lorica™ Option **B** (three-year commitment)

[1] An inventory of "most critical devices" includes, but is not limited to, the following: firewalls; perimeter routers; layer 3 and layer 2 switches; other network appliances; file, email, web, database, virtualization, and/or other servers; and any other servers or endpoints deemed critical to network operations. Note that these critical devices generate the majority of security relevant events per second (EPS) in the enterprise.

Terms and Conditions

This proposal is valid for 30 days from [Publish Date]. If this Order Form is executed and/or returned to Abacode, LLC by [Company] 30 days after this date, Abacode LLC may adjust these terms, without increasing the Total Price. Following activation, any adjustments to these terms must be confirmed by [Company].

Prices provided as part of this proposal do not include any taxes that may apply. Any such taxes are the responsibility of [Company]. Abacode, LLC utilizes the SIEM software platform from AlienVault as part of the Cyber Lorica™ program. AlienVault software terms and conditions are described in the following online document: https://www.alienvault.com/eula.

Abacode, LLC may reject this Proposal if: (1) changes have been made to this Proposal (other than completion of the signature block) or (2) the requested signature is incomplete or does not match our records or the rest of this Proposal. By signing this form, you represent that you have the authority to bind such entity and its affiliates to the terms and conditions on this Order Form.

Payment terms are Net 30. Abacode, LLC's billing preferred method is via email, and billing frequency is monthly (annual up-front billing option is also available). Subscriptions are non-cancelable before their Order End Date. The Cyber Lorica™ hardware appliance is property of Abacode, LLC. [Company] is responsible for returning the hardware appliance to Abacode at the end of the contract.

Acceptance

For Abacode, it will be a pleasure to provide [Company] our professional services described in this proposal. We are committed to strive to meet and exceed your expectations. In our genuine interest of helping your organization succeed in achieving the highest levels of cybersecurity, we have applied considerable discounts.

To confirm acceptance of the terms of the proposal, we require for you to select the option that best suits your needs and to provide your signature below. The Statement of Work described in this proposal will be governed by the terms and conditions in the Master Service Agreement to be executed by Abacode and [Company].

This proposal is based on the following criteria:
# of critical devices, # of all devices, # of locations

[Company]	Abacode, LLC
[Manager]	Rolando Torres
[Title]	Director of Cybersecurity
SIGNATURE: _____	SIGNATURE: _____
DATE: _____	DATE: _____