Improving your Cybersecurity Posture with Abacode’s MSSP Services

White Paper
By Rolando Torres, BSEE, Managing Partner
Contents

Overview ................................................................. 3
Anatomy of a Cyber Attack ........................................... 4
The Strategy .............................................................. 5
Assessment and Baselining ........................................... 6
Remediation of Findings .............................................. 6
Train, Monitor, Audit, Respond ..................................... 6
Implement New Controls ............................................. 6

How to Fight Back – Monitoring is Essential .................... 7

Cyber Lorica 24/7 Monitoring Platform Explained ................ 8
Deployment and Configuration ....................................... 8
Monitoring, Analysis and Escalation Services ....................... 9
Monthly Vulnerability Scans ......................................... 9
Weekly and Monthly Reports ......................................... 9
Monthly Meeting and Consultation .................................. 9
Cyber Lorica vs. Other MSSP Competitors ......................... 10
Cyber Lorica Deployment Diagram .................................. 10

Cybersecurity Consulting Services .................................. 11
Comprehensive Cybersecurity Posture Assessment ................ 11
Penetration Testing ..................................................... 11
Website/Web App Vulnerability Assessment ....................... 12
Cybersecurity Training ............................................... 12
Information Security Governance .................................... 12
Forensics Investigations ............................................. 13
Overview

In today’s environment, no business or organization is exempt from becoming a victim of cybercrime. Much has been said about cybercriminals only focusing on large corporations and organizations that handle private personal information such as credit card or social security numbers.

In this white paper, we debunk the myth that there are organizations or individuals that are at least risk of being breached because of their size or line of business. Furthermore, this document will shed light onto how cybercriminal organizations operate; from reconnaissance and identification of vulnerable targets to exploitation of vulnerabilities that result in breach.

The new cybersecurity paradigm is the assumption of breach, as no solution can guarantee total protection from all attack vectors. Abacode demonstrates in this document that it is critical to have strategies in place to protect your data and systems, as well as to direct your response when attacked.

Abacode is a cybersecurity firm that helps growing organizations manage their cyber risk. Cyber Lorica is a monitoring program that combines best-of-breed systems such as AlienVault IDS and SIEM, AirWatch MDM, and custom built tools with monitoring provided by our cybersecurity experts 24 hours a day, seven days a week.

Abacode can also help you improve your cybersecurity stance through training, assessments, pen testing, information security governance, and forensic investigation of incidents.
Anatomy of a Cyber Attack

The steps and methodology that cybercriminal organizations utilize to prey on their prospect victims vary by the attack surfaces utilized, physical proximity to the victim, and level of sophistication of the victim’s defenses. Below are some of the most common steps utilized by cybercriminals to breach their victims:

1. **Reconnaissance and Discovery**  
The first step often consists of a variant of a reconnaissance attack. While hackers might try to qualify and quantify the value of a target organization ahead of their reconnaissance attack, most of the time they are simply scanning EVERY IP address in the target country or state. That means they are indiscriminately analyzing IP addresses that belong to small, medium, or large organizations.

2. **Identification and Documentation of Vulnerabilities**  
Once the cybercriminal is able to identify some basic information of the victim, they transition to identifying and documenting vulnerabilities to exploit. During this phase, the cybercriminal might utilize a reconnaissance attack that is tailored to the organization’s system based on the intelligence gathered during step 1.

3. **Vulnerabilities Exploitation**  
In this step, the cybercriminal will try to exploit the identified vulnerabilities to gain access to the target system. Such attacks include but are not limited to: SQL injection, brute force authentication of internet facing assets, probing of default username and passwords, accessing exposed content that should be restricted, and installation of malware.

4. **Privilege Escalation**  
Once the cybercriminal has entered or compromised the target system, they would begin to analyze the internal network to escalate privileges, identify the systems that contain the data to be stolen, and stage the final assault. In some instances, they will use the compromised system to pivot to other servers, computers, or devices until they can access the target data or system. They could also sell your device in the dark web for other cybercriminal organizations to use for their illicit activities. This is another reason why every organization is considered a target even if they don’t host personal data.

5. **Data Harvesting**  
Game over, the cybercriminal is in; they have obtained elevated privileges and setup a mechanism to harvest your data, whether that is data at rest or transactional data. This mechanism could consist of a combination of malware, root access kits (RAT), or modifications of software running in your system, among many other different techniques.
The Strategy

In the previous section, we discussed one of the many approaches commonly used by cybercriminal organizations to victimize companies and organizations. Our theoretical attack shows one of the numerous ways that organizations with some form of IT component - such as email, website, CRM or a document management system - are at risk of being breached.

For many years, organizations have followed the castle fortification approach, hoping that by increasing their defenses the cybercriminal will bypass them for easier targets. In this effort, organizations have invested heavily in firewalls, antivirus, malware detection and other security systems that, while they can be considered the technological foundation of cybersecurity, have limitations in addressing all aspects of cyber risk.

Organizations need to develop a strategy to address Cyber Risk that includes technology, processes, and the human factor. Often the question is ‘where should we start?’ Unfortunately, there is no simple answer. It is important to understand that cybersecurity is a continuous, cyclical process. The four primary components of the cybersecurity readiness cycle (CRC) are:

1. Assessment and Baselining (ANB)
2. Remediation of Findings (ROF)
3. Train, Monitor, Audit, and Respond (TMAR)
4. Implement New Controls (INC)
Assessment and Baselining
During this phase, a third party auditing firm is hired to perform a comprehensive assessment of the organization. This assessment might include: a pen test, web vulnerability assessment, policy and procedures review, information security controls check, and security technology configuration review. Once the assessment is complete, companies receive a detailed report of findings and recommendations that will help drive the next stage, Remediation of Findings.

Remediation of Findings
The findings and recommendations identified in the Assessment Report are prioritized to implement the most impactful recommendations first. Budget considerations along with internal resources constraints often play a role on how quickly findings are corrected. In many instances, the organization is required to engage a third party company to help with the remediation process. In some cases, the organization has to accept the risk posed by a finding due to a lack of resources to correct the finding.

Train, Monitor, Audit, Respond
Through monitoring, the organization stays on top of the ever changing threat landscape, identifies when it is being targeted, and enacts an articulated and timely response when attacks are confirmed. As cybercriminal activity is constant, monitoring also needs to be around the clock and provided by cybersecurity analysts that specialize in persistent threats. The organization should hire a reputable MSSP company to monitor their systems, 24 hours a day, 7 days a week. For example, Abacode collaborates with the organization’s IT team to enact a proper response when unauthorized activity is detected.

Regarding human factor controls, they should be tracked and audited in order to make sure that said controls are both being followed and are working as intended. Such controls include training, auditing to ensure that policies and procedures are followed by the staff, and validation that technological implemented controls are functioning properly.

Implement New Controls
The implementation of new controls is prioritized according to the time, personnel, and budget constraints of the organization. Some of these controls should be driven by Information Security Management (ISM) standards such as ISO 27001 or NIST Framework. Other controls might be enacted due to technical recommendations of well recognized organizations such as NIST and SANS. Lastly, new controls could be influenced by advances in current technology already in used by the organization, the replacement of aging technology, or the adoption of new technologies.
How to Fight Back – Monitoring is Essential

Cybercriminal organizations have an unfair advantage over their victims, particularly if they are not actively monitoring their IT infrastructure and network. Without monitoring, the cybercriminal is able to operate undetected as he/she makes progress towards compromising and breaching their victims’ systems.

It is important to make a differentiation between the technology that enables the detection of unauthorized activity and a full monitoring program that includes the constant intervention of cybersecurity professionals like Abacode’s Cyber Lorica. The monitoring platform is a tool that when properly configured, operated, and maintained, will enable the organization to detect attacks. Monitoring requires human intelligence and human decision making to analyze the attacks and determine the proper course of action or response that should be enacted to protect the organization.

Some organizations might attempt to acquire a monitoring solution to run by themselves and assign the responsibility of monitoring this system to an IT person as an ancillary task. In most cases, this IT person, who is not a cybersecurity professional, gets overwhelmed by false positives, alarms that make no sense, and the inability to research these alarms. The end result is that alarms tend to be ignored, neglected or not properly investigated in a timely matter. Additionally, utilizing IT personnel on a regular business schedule means that the system is not monitored at all after business hours, during weekends, holidays, or when the IT person goes on vacation or PTO.

Abacode’s Cyber Lorica combines the Intrusion Detection System (IDS), Security Incident and Event Management (SIEM), Vulnerability Scanning capabilities of AlienVault, and the Mobile Device Management (MDM) capabilities of VMWare AirWatch, along with custom built security and OpenSource solutions in a platform that is monitored 24 hours a day, 7 days a week by cybersecurity experts.
Cyber Lorica 24/7 Monitoring Platform Explained

As previously stated, Abacode’s Cyber Lorica combines AlienVault, VMWare AirWatch and custom built security and OpenSource solutions in a platform that is monitored 24 hours a day, 7 days a week by cybersecurity experts. The level of monitoring provided by Abacode is considered proactive in that we identify vulnerabilities before these are exploited by hackers and point out high risk behavior before this leads to a breach.

AlienVault is recognized as a “visionary” in the Gartner Magic Quadrant for SIEM. The AlienVault Unified Security Management (USM) solution provides: Security Incident and Event Management (SIEM), vulnerability assessment (VA), asset discovery, network and host intrusion detection (NIDS/HIDS), file integrity monitoring (FIM), Open Threat Exchange, and Threat Intelligence. AlienVault’s Open Threat Exchange community enables sharing of Internet Protocol (IP) and URL reputation information. AlienVault Labs provides an integrated threat intelligence feed to Cyber Lorica that includes updates to signature, vulnerability, correlation, reporting, and incident response content.

AirWatch is recognized as the “leader” in the Gartner Magic Quadrant for Enterprise Mobility Management. Through the integration of AirWatch into the Cyber Lorica monitoring platform, our cybersecurity professionals are able to identify security issued with your mobile device fleet.

Abacode has the expertise to develop plugins that integrate unsupported devices, systems, and applications into AlienVault. Such integration capabilities enable our cybersecurity professionals to monitor systems that are not supported out-of-the-box to identify internal and external unauthorized activity.

Deployment and Configuration

Cyber Lorica has multiple deployment options including Cloud-based, physical appliance, or virtual appliance delivered to a VMWare ESXi host. Abacode recommends the physical or virtual appliance option in most solutions as it keeps the security data and logs contained within the organization’s data center. With the Cloud-based deployment, the security data is transmitted encrypted to a Cloud server where it is stored for analysis and reporting purposes, and destroyed when no longer needed.

All available features of the network IDS are enabled by collocating the Cyber Lorica appliance with the primary firewall and core switch in the data center. In this manner, the appliance can be setup to inspect all traffic going thru the firewall in addition to having access to the firewall generated syslogs.

Network appliances and devices such as routers and switches are configured to forward their syslogs to the Cyber Lorica appliance for storage and analysis. In the case of Unix and Linux servers, host IDS and file integrity monitoring is accomplished through the installation of an agent application. This agent has a small footprint and utilizes minimal amounts of RAM and CPU cycles.
Windows server, desktops, and laptops are also required to deploy an agent for monitoring. In addition to the host IDS and file integrity monitoring, the Windows agent includes registry monitoring that allows the immediate detection of malware such as CryptoLocker.

Mobile devices and laptops are configured to use the AirWatch MDM app available in the Apple Store for iPhones, Google Play for Androids, and Microsoft Store for Windows mobile devices. The AirWatch management console is integrated into the monitoring platform to enable our cybersecurity professionals to monitor your mobile device fleet events.

Monitoring, Analysis and Escalation Services

Abacode’s Security Operations Center (SOC) team monitors the events and alarms generated by the Cyber Lorica console 24 hours a day, 7 days a week. Our TIER 1 cybersecurity professionals are constantly observing the alarms and events console to analyze alarms as soon as they arise. The Abacode team can internally escalate the alarm to the TIER 2 and/or TIER 3 support team members to decide if a client escalation is required and to determine the recommended corrective action.

If the Abacode Team decides that an alarm needs to be escalated to the client, the specific protocol established with that client is followed. The escalation protocol includes details such as contact information, SLAs, and escalation ladder. Depending on the severity and client preference, the escalation might occur via email, telephone call, and/or teleconference bridge.

Monthly Vulnerability Scans

Abacode’s Security Operations Center (SOC) team performs monthly vulnerability scans to detect issues such as missing patches, malware, enabled services that need to be disabled, open ports, and unauthorized software, among others. The outcome of these vulnerability scans is presented to the client in an actionable report that summarizes and prioritizes the findings and provide corrective recommendations.

Weekly and Monthly Reports

Abacode’s Security Operations Center (SOC) generates weekly reports summarizing the level of activity, events, and alarms addressed during the week. Additionally, there is a report of malicious IP addresses that have been targeting the organization so that those IP addresses can be blocked in the firewall. On a monthly basis, a vulnerabilities report is generated along with a report summarizing the activity of the previous month.

Monthly Meeting and Consultation

Abacode hosts a monthly meeting with each client to review the provided reports and to discuss the most important incidents and alarms. Furthermore, the client has the opportunity to discuss other cybersecurity topics or questions with the Abacode team including consultation in the acquisition of new technologies.
## Cyber Lorica vs. Other MSSP Competitors

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cyber Lorica</th>
<th>Dell SecureWorks</th>
<th>TrustWave</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS / Threat Intelligence</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>SIEM / Log Aggregation</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Vulnerabilities Detection</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Compliance Reports</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>24/7 Monitoring</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mobile Fleet Management</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Apps Support</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best Value!</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cyber Lorica Deployment Diagram

![Cyber Lorica Deployment Diagram](image)
Cybersecurity Consulting Services

Comprehensive Cybersecurity Posture Assessment

Abacode separates itself from the competition by providing the most comprehensive and thorough Cybersecurity Posture Assessment in the market. Our approach will provide you with true intelligence on your cybersecurity readiness including actionable findings and recommendations. Our team of Cybersecurity Professionals has performed hundreds of assessments and penetration tests for enterprises of all sizes, including commercial and military organizations. We pride ourselves in providing the level of expertise that not only will help you identify your vulnerabilities and areas of improvement, but also provide you guidance on best practices to correct those vulnerabilities.

The Cybersecurity Posture Assessment is tailored to the client needs utilizing the following options:

- Cybersecurity Posture Assessment
- Internal & External Network Assessment
- Phishing and/or Social Engineering test
- IDS/IPS Assessments
- Test to simulate a “rogue” or “disgruntled” employee to see if they find and crack sensitive data
- Perform a gap analysis of existing IT security policies and procedures
- Review compliance with information security standards such as HIPAA, PCI DSS, ISO 27001, etc.

Penetration Testing

A Pen Test helps the organization determine how effectively the implemented security technology, policies, and controls can prevent the intrusion of determined, ethical hackers. Organizations with the highest level of cybersecurity readiness perform pen testing exercises regularly - typically once a year - in order to assess their security in the ever changing infrastructure and threat landscape. As new devices, systems, applications, and solutions are adopted by the organization, new vulnerabilities and risks are introduced.

During the Pen Test, the Cybersecurity Firm Team can take the “red team” approach in which they operate like an outsider trying to breach the organization. In other instances, the Cybersecurity Firm Team can take the “blue team” approach and assess the vulnerabilities in collaboration with the organization’s staff. The outcome of the Pen Testing effort is a formal report of findings and recommendations generated from the exercise that will help the organization raise their readiness level.
Website/Web App Vulnerability Assessment

Similar to Pen Testing, during the Website/Web App Vulnerability Assessment a team of ethical hackers will attempt to compromise the target website or web app. Typically, the first step is to run a series of scans and tools that identify open ports, active services, and other vulnerabilities that hackers could exploit. Abacode’s ethical hackers utilize the gathered intelligence to try to compromise the website or web app. Misconfigurations, third party plugins/tools, and poorly written code could introduce vulnerabilities unperceivable to the non-cybersecurity expert but exploitable by hackers.

Abacode highly recommends that websites and web apps are assessed for cybersecurity readiness prior to going into production and with every major release, particularly when these assets handle transactional and/or sensitive data. Even informational corporate websites should be scanned and tested as any compromise of such websites poses a threat to the organization’s online brand and reputation.

Cybersecurity Training

Humans are the weakest link when it comes to cybersecurity. The most effective way to mitigate the cyber risk exposure introduced by employees, partners, and vendors is training. Abacode provides two different types of training, tailored to the leadership of the organization and the general staff.

Every member of the organization is critical to the success of the implementation of cybersecurity policies and procedures. Staff members should be empowered to fulfil their cybersecurity roles and responsibilities and to be vigilant and careful in the utilization of the organization’s assets.

Furthermore, as today’s cybersecurity paradigm is assumption of breach, it is imperative that the organization’s team members at all levels understand their responsibilities in reporting incidents and which reporting mechanisms to use.

Lastly, cybersecurity training needs to be reinforced regularly to keep the staff up-to-date on the latest threats, keep their level of awareness high, and their cybersecurity responsibilities fresh in their minds.

Information Security Governance

The implementation of an Information Security Management (ISM) program shows a high-level of commitment of the organization to keeping the top most cybersecurity readiness. Organizations in highly regulated markets are required to comply with standards such as HIPAA and PCI DSS that involve information security governance efforts.
Abacode believes that ISM programs such as the NIST Framework and ISO 27001, when properly implemented and executed, are critical in keeping an organization safe. Such programs define a set of controls that incrementally reduce the risk of breach.

Abacode can help your organization select the ISM standard that best suits your needs and work with your staff to implement the ISM controls at a pace your organization can digest.

**Forensics Investigations**

Special attention should be paid to increasing the organization’s state of cyber forensic readiness. Therefore incidents can be investigated in a timely fashion with the highest probability of finding the root cause of the event.

Abacode is prepared to help you execute your incidence response by performing a full forensic investigation following the silver platter approach required by the Department of Justice for prosecution. Our forensic investigations are performed under the directive and supervision of a licensed Private Investigator as is required by most states. If necessary, all evidence, findings, reports, and documentation could be handed over to the authorities for prosecution and will be admissible in a court of law.

Abacode can work with your legal advisors, insurance company, and executive team to assess the extent of an incidence, timing of the event, and if there are notification requirements. Abacode performs these investigations under the strictest level of confidentiality in direct and exclusive communication with the organization that contracted our services.