



**SECURELY MANAGED**  
A SECURELY YOURS LLC COMPANY

**CSI** Investigation  
Risk Management



**SECURELY MANAGED  
ENHANCING YOUR  
CYBER DEFENSE**

# Cyber Defense Strategy - Hope or Planned?



Cyber-attacks are becoming more targeted. Is your cyber defense strategy based on hope? Hope that your industry is not targeted by cyber hackers? Or hope that your company is small enough that you are not on the radars of these advanced cyber attackers? Or that you do not have sensitive data which the cyber criminals may be interested in?

You may be surprised to know that the cyber thieves have many reasons to penetrate your network and systems – besides the obvious reasons for privacy data, medical data or credit card data, the thieves may be looking at using your networks and systems as one way to get to your customers and business partners.

The truth is that the majority of the companies may already have been attacked, and they are unaware that the thieves are living in their systems for days, months or even years.

It is also possible that you have planned out your cyber defense strategy. It is possible that this strategy includes the risk assessment, appropriate security controls and the best practices as outlined by industry experts (e.g., security awareness program, incident response program and supplier management program to name a few).

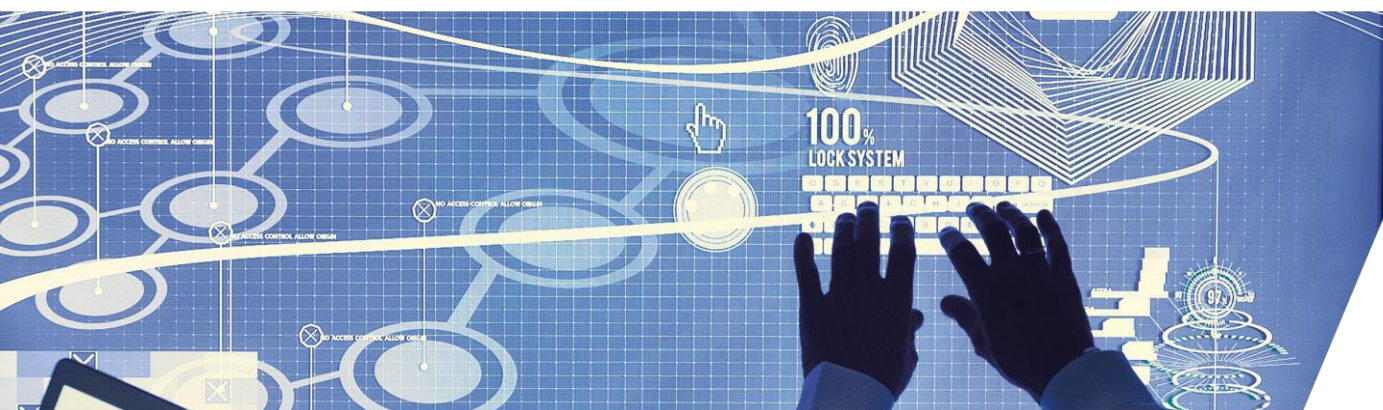


## Is Your Cyber Defense Adequate?

Most organizations, even though they have made significant progress in planning out their cyber defenses, are still behind the 8-ball. Do you still feel that your cyber defense program is occasional, or maybe periodic but not continuous? You may be aggregating your audit logs and network traffic logs with software like Security Information Event Management (SIEM), but may not have enough budget to buy adequate storage to aggregate all the logs, or you may have purchased the SIEM software for regulatory compliance reasons but is not deployed or used properly, or maybe you have enough resources to monitor the SIEM dashboard between regular work days, but not during evenings or weekends.

Do you think that cyber thieves sleep at night or weekends? Do you feel that your cyber defense strategy has holes? Is one such hole 24x7x365 continuous security monitoring?

# Proposed Solution



As an organization, you are probably in three stages of continuous security monitoring. We call it our SIEM lanes. Take our SIEM lane challenge and see which proposed solution can help you the best. Before you start, let's clear some acronyms: SIEM is the software used to aggregate and analyze network traffic and audit logs. Managed Security Service Providers or MSSP are service organizations which can provide you 24x7x365 security monitoring through their Security Operations Center or SOC.

Your organization may be at a stage where you have not purchased the SIEM software, and you do not have any current monitoring. Our solution in SIEM Lane 1 can provide you the listed services in the diagram below. Our solution includes the license to SIEM software as well as 24x7x365 monitoring for one single low price.

If you have licensed the SIEM software but are currently monitoring the SIEM dashboard yourself, we recommend SIEM LANE 2 services. We highly recommend that you make the best use of the resources who are currently monitoring the SIEM software and use those resources for actually mitigating the risks identified by our 24x7x365 SOC. See SIEM LANE 2 for further details.

If you already have a SIEM and an MSSP, we believe you have already taken the strategic step to advanced cyber defenses. If you are unsatisfied with your current MSSP provider or would like to check out our low prices (compared to your current MSSP provider), check out SIEM LANE 3.

# SIEM Lanes

## SIEM MSSP

We provide:

- 24x7x365 Monitoring
- SIEM Software
- Asset Discovery
- Vulnerability Scanning
- Network and Host Intrusion
- Endpoint Detection and Response
- File Integrity

**SIEM Lane 1**

## SIEM MSSP

We provide:

- 24x7x365 Monitoring of your SIEM
- SOC is USA based
- We monitor you remediate
- Make the best use of your resources
- Our price include Asset Discovery, Vulnerability Scanning

**SIEM Lane 2**

## SIEM MSSP

We provide:

- Lowest price point in the industry
- Best service
- Savings can assist in additional resources for remediation

**SIEM Lane 3**

## OUR MSSP SERVICES



### OUR PROPOSED SOLUTION



**SIEM**

- Log Management
- Worlds largest Repository
- OTX Threat Data
- SIEM Event Correlation
- Incident Response



**ASSET  
DISCOVERY**

- Active & Passive Network Scanning
- Asset Inventory
- Software Inventory



**VULNERABILITY  
ASSESSMENT**

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning
- Remediation Verification



**INTRUSION  
DETECTION**

- Network IDS
- Host IDS
- File Integrity Monitoring
- Endpoint Detection and Response (EDR)



**BEHAVIORAL  
MONITORING**

- Netflow Analysis
- 24/7/365 monitoring
- Service Availability Monitoring



## Benefits

- ❑ Immediate notification of a security threat – 24x7x365
- ❑ Direct Access to highly skilled security engineers monitoring the network.
- ❑ Services include not only log and SIEM monitoring but also vulnerability scanning, penetration testing, threat intelligence, Network IDS, Host IDS, File Integrity monitoring.
- ❑ 24x7x365 day access monitoring service
- ❑ Full suite of compliance, audit, and security reports

## Why Securely Yours and CSI ?

- ❑ Best research on threat Intelligence
- ❑ Experienced staff with decades of Cyber Security experience
- ❑ Complimentary services in Vulnerability Management, Incident Response and Patch Management
- ❑ Guaranteed service satisfaction
- ❑ Lowest price point in the industry

