DOES YOUR ORGANIZATION NEED CYBER MONITORING 24X7X365?

SAJAY RAI AND PHILIP CHUKWUMA

CYBER MONITORING IS LIKE GOING TO A DOCTOR?

There are those who go to the doctor and want to only know if they are dying or not. And then there are others who go to the doctor to know all the details of what is going inside their body. The latter group of individuals are the ones who really want to improve their body.

Similarly, there are those organizations who only care to know if they are under cyberattack or if they have been breached. They do not necessarily care to know the details of what is going on inside their network. These organizations compare the need to get 24x7x365 monitoring to the physical alarm system for the house. The physical alarm system notifies you and the law enforcement if there has been a physical breach. The same way, they expect their 24x7x365 monitoring service to let them know about the data breach or a cyberattack. These organizations generally do not get the maximum value from what a 24x7x365 monitoring can provide. On the other hand, the organizations who really care to understand all the activities within their network are the ones who really want to improve their IT security and reduce the possibility of cyber compromise.

SIEM AND MSSP

Let’s first understand how monitoring works: all the endpoints in the network generate logs. Windows servers, desktop and laptops generate event logs, whereas network devices (e.g. firewalls, switches, routers) generate syslog. An organization may also have Linux or Unix servers which generate syslog. All these logs are usually forwarded to a security software called SIEM, which stands for Security Information Event Management. SIEM performs correlation analysis and behavior analysis of these logs to determine if it is worthy of an alarm. For example, if a user enters a password wrong once, it could just be an event and no alarm is issued, whereas, 100 or more attempts are made to enter password within 1 s, it is assumed that a software bot or a script is trying to guess a password, and therefore these events are worthy of an alarm.

If an organization licenses a SIEM software, they probably monitor the logs between the regular office hours of 8 am to 5 pm (Monday through Friday) as they do not have the resources or the budget to staff their cyber monitoring 24x7x365. These organizations may get a false sense of security that they are regularly monitoring their logs. But as we all know the bad guys do not sleep at night. In fact, they may be more active at night. And it may be too late for an organization to review evening and night logs the next day, as the damage may have already been done.

An organization could also use MSSP, which stands for Managed Security Service Provider. MSSPs provide 24x7x365 cyber monitoring of your IT infrastructure. Majority of MSSPs provide complete package of monitoring including the use of a SIEM. But if an organization already has a SIEM, a MSSP could just provide monitoring service (although it is usually more cost-effective for an organization to get full service from MSSP). Because these MSSPs can monitor multiple clients using their resources 24x7x365, it is usually cheaper for organizations to use MSSPs to monitor their network for cyber-attacks 24x7x365.

WHETHER TO 24X7X365 OR NOT?

Your Organization Probably Fits into One of the Three Monitoring Cases:

Case 1: No SIEM, No MSSP

In this case, an organization may not understand the benefits provided by SIEM and/or MSSP. This is the organization which most likely thinks that 24x7x365 of their network is like the home security system. In their eyes, the 24x7x365 has only one benefit – it will alert them of any cyberattack or data breach.

The benefits of 24x7x365 are far greater than just the alarms for cyberattack or data breach. An organization gets to understand the details of what is going inside their network. This is analogous to a person going to the doctor and getting to know the details of what is happening inside his/her body.

These organizations, when they install the SIEM in their network may have already been breached. By installing the SIEM, they get to understand the activities which are being performed inside their network. For example, if a SIEM detects a suspicious behavior on a server (e.g. too many password attempts in 1 s), it will most likely determine that a malicious insider is trying to gain access by guessing passwords. When investigated further by an organization with the help of their MSSP, they may determine that an automated process is running (e.g. a backup process, or a scheduled process which is invoked at a particular time and day is attempting to sign-on as a user whose password was recently changed) and it may not necessarily a malicious insider. In this case, an organization would correct that process. If it is determined that the process should not be running on the server, then it truly could be a malicious insider and a potential serious breach would be avoided.

Case 2: Yes SIEM, No MSSP

In this case, an organization already understands the benefits of SIEM, but uses it in one of two situations:

1. Monitoring the SIEM dashboard between regular business hours, in which case a determination should be made if they are prepared for a potential breach or cyber incident during off-hours and if the risks are acceptable. Most likely, a case can be made that they need 24x7x365 cyber monitoring.
2. Monitoring the SIEM dashboard 24x7x365 using their in-house SOC (Security Operations Center). In this situation, a key question to be investigated is the cost of the resources/budget allocated to monitoring, and whether they will be in a better position if they outsourced the monitoring to a MSSP and use their existing resources for incident response and vulnerability management tasks spawned from the MSSP/SIEM monitoring.

Case 3: Yes SIEM, Yes MSSP

In this case, an organization is already there. They must be seeing the benefits of both SIEM and MSSP. It is important that an organization continues to verify the benefits they are receiving from their MSSP and that they are actually monitoring the alarms. A periodic-simulated attack could verify that the MSSP is "on its toes" and truly monitoring for 24x7x365 cyber activities.

An organization could also periodically review the contracts and get external bids to ensure that they are getting equal or better services compared to other MSSPs. The reason this could be important is that the MSSP market is evolving and MSSPs are becoming creative by providing additional innovative services for same cost as an organization maybe paying their existing MSSP. Some examples of these additional innovative services include but are not limited to:

- Asset Inventory and Management – some SIEM software provide this feature. An organization may already have a software which performs this task, but if they don't, it could be an added benefit to use a specific MSSP/SIEM
- Vulnerability scanning – some SIEM software provide this additional service. Again, an organization may have a software which performs this task, but to see all your vulnerabilities on one dashboard with all the other alarms may be beneficial for some organizations
- File Integrity Monitoring, where you can monitor sensitive files for activities
- Endpoint Detection and Response or EDR - this feature allows an organization to perform forensic analysis on an endpoint and even take the endpoint off the network
- Cloud monitoring - some SIEM software do a better job of providing this feature by integrating it with their SIEM, whereas other SIEM could have a complex interface
- Dark Web Monitoring – this feature provides the ability to see which email and passwords within an organization's domain have activity in the dark web (e.g. passwords are being sold). This feature allows an organization to be proactive in resetting passwords and potentially prevent hacker penetration

Many organizations may find that having all these services and features viewable through one dashboard of the SIEM (and provided by MSSP) would enable better understanding of their environment.

REGULATORY COMPLIANCE REQUIREMENTS

Currently, there are no regulatory or compliance requirements which mandate the implementation of 24x7x365 cyber monitoring. The closest law is the 2017 New York Cyber Law (for financial services companies) where it indicates "The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments". It is possible that in the next couple of years, the continuous monitoring could become mandatory for regulatory compliance.

SUMMARY

If an organization has never tried SIEM or MSSP, they stand to gain a wealth of information and knowledge about their network. It is exactly the same way, a person who sees the doctor for the first time, gets a wealth of information and knowledge about its own body. An organization may find out that there are activities within their network which is not compliant with their security policies (e.g. certain servers may still have default user ids like Administrator, in some systems an anti-malware software is not installed). In some situations, they may find out that a malicious insider has been in their network for some time. In either case, they should feel more secure and better prepared to handle a cyber incident or a data breach.

SajayRai *CPA, CISSP, CISM is President & CEO of Securely Yours LLC, Bloomfield Hills, MI.*

Philip Chukwuma, *CISSP is Chief Technology Officer of Securely Yours LLC. He is located in Dallas, TX.*