An Effective Defensive Strategy

The most important aspect of heightening the defenses for manufacturers is to first acknowledge and address the statistics that are plaguing the industry. Once your organization has determined that the data held within your environment is in the crosshairs of attackers, the defensive strategy can ensue. It is not merely distant attackers that are seeking to compromise your security, but even internal employees that may be taking your sacred secrets to the competition.

1. Creating Continuity and Recoverability

In the event that insider threats or external attackers were to compromise your manufacturing operations, could you operate in a crippled state? If the answer to this question is no, it is time to consider some options.

1. Have a plan for a disaster (such as ransomware).
2. Create reliable backups.
3. Ensure that backup redundancy is implemented.
4. Test recoverability of such backups.
5. Ensure that speedy recovery operations can be implemented. The overall goal in this exercise is to ensure that when a disaster strikes, the organization can still operate. This should include items such as cyber-attacks, full network compromises, ransomware or malware propagation, or even system/data corruption.

2. Protect the Data

Your trade secrets, formulas, and other proprietary information are the lifeblood of your operations. You must protect this data at all costs from unauthorized disclosure and theft. A sudden competitor that is offering a comparable product at a lower cost will surely raise concerns on the board.

1. Conduct an inventory of all data types. Collect the type of information, location, owner, access granted, and what the level of criticality is for the organization. Rating such data on a criticality scale will enable your organization to implement focused security protocols, saving time, money, and resources.
2. Know who is accessing, modifying, or exfiltrating your data. A Security Information and Event Management platform will enable you to do just that.
3. Encrypt data-at-rest and data-in-transit. Furthermore, protect the keys for decryption.
4. Ensure that sensitive data does not migrate to less-protected systems.

Insider Threats

A study by IBM showed that 60% of attacks are perpetrated by insiders (IBM).

The most important aspect of heightening the defenses for manufacturers is to address the statistics that are plaguing the industry. Once your organization has determined that the data held within your environment is in the crosshairs of attackers, the defensive strategy can ensue. It is not merely distant attackers that are seeking to compromise your security, but even internal employees that may be taking your sacred secrets to the competition. Insider threats do not need to have malicious intent. These are often employees that make simple, yet consequential mistakes that lead to data breaches and network compromises. Insiders already have access to your networks, systems, data, and trust. This is a risky combination that leads to cybersecurity incidents that remain under-the-radar for extended periods of time. Detection of insider threats can be a daunting task. Organizations must first determine what is normal user activity to decipher what are the deviations from the standard behavior. A Security Information and Event Management System (SIEM) can assist with this critical component.