IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

DEFEND TODAY,
SECURE TOMORROW

ChemLock: Detection Security Goal

Developing a Security Plan

CHEM LOCK
Know your chemicals.
Lock in your security posture.

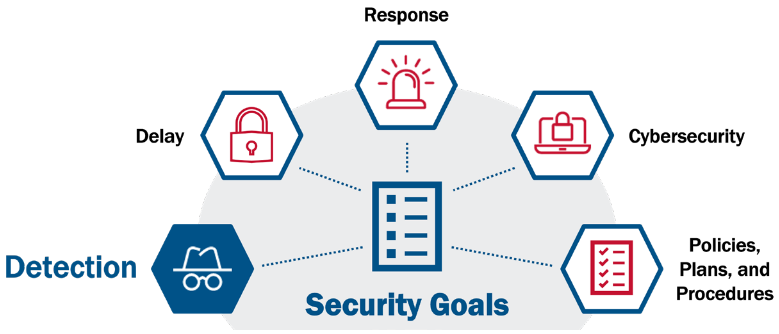
The Cybersecurity and Infrastructure Security Agency (CISA) encourages facilities with dangerous chemicals to develop a holistic, customized, site-specific security plan that mitigates risk and enhances chemical security at the facility. To assist your facility in developing a security plan, the ChemLock program presents five security goals to consider as you evaluate and implement security measures tailored to your facility's unique circumstances and business model. This fact sheet provides an overview of the Detection security goal.

Detection Security Goal

Detection is the ability to identify potential attacks or precursors to an attack and to communicate that information as appropriate. This means that a nefarious act must be detected or observed early enough so that appropriate first responders can arrive to deter or delay the attack from taking place. Thus, layers of detection, deterrence, and delay measures are inherently linked and complement one another.

Examples of Detection Security Measures

Detection measures include intrusion detection systems (IDS), camera systems, employees or on-site security personnel, security lighting, and inventory controls. Activity at your facility can be monitored through a combination of human oversight and a variety of technical sensors interfaced with electronic entry-control devices, remote surveillance imaging, and alarm-reporting displays. Multiple detection measures can be used to create layers of security at your facility.



1. **Intrusion detection system (IDS).** IDSs typically consist of various hardware and software elements and are used to detect an intrusion at an early stage. IDSs should be connected to a monitoring station to ensure prompt response by trained personnel or activation of cameras. Examples of IDS systems include infrared (IR) sensors, microwave sensors, fiber optic sensors, magnetic switches, and other motion sensors.
2. **Camera system.** Cameras can provide multiple angles of observation so that your facility can monitor critical assets and detect an intruder.
3. **Employees or on-site security personnel.** Employees and dedicated security personnel can be used to enhance facility security and provide a means of deterrence, detection, delay, and response. Employees should be trained to be vigilant and to know what to look for regarding suspicious activity. Security forces can be proprietary or contracted and can be armed or unarmed.
4. **Security lighting.** Well-lit areas not only aid in detecting potential intrusions, but also deter would-be intruders from attempting to breach your facility.
5. **Inventory controls.** A process for tracking, checking, and auditing chemical inventories, sales, transfers, and deliveries can provide early detection of nefarious actions.

Considerations for Detection

When evaluating detection security measures, your facility should consider the chemicals on site and their associated security concerns. These factors will drive the type of detection measures your facility will need to implement. For example, a facility might consider different detection measures for a toxic chemical that would cause harm if deliberately released into the air than would be considered for an explosive precursor chemical that is being protected against theft or diversion.

When considering detection measures, be sure to account for different threats as well. Some detection measures may be highly effective against some attacks, but not against others. For example, inventory control measures can be effective at mitigating the risk of theft, but they may not be effective in detecting that a chemical has been deliberately released.

You will also want to consider how your facility's operational processes may contribute to the type of detection measures implemented. For example, a smaller facility may find it feasible to use personnel that have been trained in security awareness to detect a nefarious actor, whereas a larger facility may need to rely on an alarm system or on-site security personnel. You should also consider whether the goal of the security plan is to protect a particular asset, the entire facility, or a combination of both.

Security-in-Depth

An optimal security plan typically involves the use of multiple security measures that provide layers of security (also known as security-in-depth). Complementary layers of security measures not only ensure that your critical assets are secured against different kinds of security threats, but also provide redundancy in case one security measure fails or is compromised by a nefarious actor. For example, cameras may be more effective when paired with proper lighting or IDS systems. Elements of detection are part of security-in-depth and are critical to any security plan.

CISA Security Resources

- ChemLock: cisa.gov/chemlock
- ChemLock: Secure Your Chemicals Security Plan: cisa.gov/chemlock-security-plan
- Chemical Sector Resources: cisa.gov/chemical-sector
- Counter-Improvised Explosive Device (IED) Training Courses: cisa.gov/bombing-prevention-training-courses
- Insider Threat Mitigation: cisa.gov/insider-threat-mitigation
- Power of Hello: cisa.gov/power-hello

Next Steps

Here are some questions you can use to evaluate your facility's detection security measures:

- What are the threats that your facility should be most concerned about?
- Do all access points at your facility have some kind of detection security measure?
- Will detection security measures still function if your facility lost power?
- Does your facility need dedicated on-site security personnel?
- What training has been provided for all your personnel responsible for detection security measures?
- Is the lighting at your facility sufficient to ensure that detection security measures can be effective?
- Does your facility have sufficient inventory control processes in place to detect anomalies?
- If suspicious activity or nefarious actions are detected, what is your facility's reporting process?
- What delay security measures are in place to allow appropriate response to a detected incident?
- Has your facility conducted an exercise to test the effectiveness of existing detection security measures?