How AlienVault ICS SIEM Supports Compliance with CFATS (Chemical Facility Anti-Terrorism Standards)

The U.S. Department of Homeland Security has released an interim rule that imposes comprehensive federal security regulations for high-risk chemical facilities. The CFATS regulations require specific cyber security steps be taken by facility owners and operators and lays the framework for future regulation of cyber assets. AlienVault has produced this document to assist facility owners in their efforts to create and execute on actions plans to mitigate risks and ensure compliance.

AlienVault ICS SIEM provides a uniquely integrated platform which provides support for all cyber requirements in CFATS. Reporting, identification, management, training, enforcement, response and recovery capabilities form a framework for a continuous planning and operations environment. Integration with existing equipment including physical security systems allows AlienVault operators to consolidate and improve security across entire facilities.

AlienVault ICS SIEM combines Detection, Prevention and Situational Awareness with Forensic Auditing and Reporting. A fully integrated security system, SIEM intelligence is supported by automated intrusion detection, vulnerability assessment, network discovery and asset management to provide full functionality in every installation. The AlienVault console is the single interface into a security deployment leveraging and protecting every cyber asset. Forensically secure audit trails are created and stored in an encrypted and digitally-signed environment for automated and accurate compliance reporting.

The following pages illustrate specific points of value AlienVault ICS SIEM provides to CFATS compliance efforts. Additional portions of CFATS may be supported in your environment.
§ 27.215 Security Vulnerability Assessments

(a) Initial Assessment. If the Assistant Secretary determines that a chemical facility is high-risk, the facility must complete a Security Vulnerability Assessment. A Security Vulnerability Assessment shall include:

(1) **Asset Characterization**, which includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection;

AlienVault’s capability to automatically discover and classify cyber assets assists licensees’ efforts by providing empirical data on installed and active cyber assets and control pathways. The Asset Inventory created by AlienVault ICS SIEM is continuously updated. Cyber pathways to Critical Assets can be identified and confirmed and existing security implementations detected and integrated.

(2) **Threat Assessment**, which includes a description of possible internal threats, external threats, and internally-assisted threats;

AlienVault ICS SIEM includes an embedded Vulnerability Scanner and other tools which automatically perform cyber vulnerability assessments of all other cyber assets and maintains a forensically security archive of all vulnerability and topology information. This functionality allows facility owners to identify and categorize internal and external risks that could be exploited to realize a potential threat.

(3) **Security Vulnerability Analysis**, which includes the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards;

AlienVault ICS SIEM includes an embedded Vulnerability Scanner and other tools which automatically perform cyber vulnerability assessments of all other cyber assets and maintains a forensically security archive of all vulnerability and topology information. Accurate identification of existing vulnerabilities allows for appropriate countermeasures to be designed to address such vulnerabilities.

(4) **Risk Assessment**, including a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a success of an attack; and

The system-wide vulnerability awareness provided by AlienVault ICS SIEM allows facility owners to identify key cyber assets that can affect critical assets and the likelihood of success of an attack in impacting the subject industrial process.

(5) **Countermeasures Analysis**, including strategies that reduce the probability of a successful attack or reduce the probable degree of success, strategies that enhance the degree of risk reduction, the reliability and maintainability of the options, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

The AlienVault platform is specifically designed to support the development and maintenance
of response plans and countermeasures. In response to Cyber Security Incidents, the specific executable actions according to the plan will be carried out automatically, including alerting appropriate staff and executing predefined actions (including such actions as removing a device or user from the network, blocking external traffic, activating recovery plans, etc.). This capability allows facility owners to develop strategies that reduce the probability of a successful attack or reduce the probable degree of success, enhance the degree of risk reduction, the reliability and maintainability, effectiveness, maintainability, capability and effectiveness of mitigation options. This implementation of countermeasures and visibility into past and present control system behavior allows for on-going empirical analysis of countermeasures.

(1) A covered facility must update and revise its Security Vulnerability Assessment in accordance with the schedule provided in § 27.210.

AlienVault ICS SIEM provides the ongoing visibility into security vulnerability for comprehensive and efficient SVA updating and revision.

(2) Notwithstanding paragraph (d)(1) of this section, a covered facility must update, revise or otherwise alter its Security Vulnerability Assessment to account for new or differing modes of potential terrorist attack or for other security-related reasons, if requested by the Assistant Secretary.

AlienVault ICS SIEM provides a baseline of empirical state and behavior that can be used as a foundation against which to revise SVAs to account for differing modes of potential terrorist attack or for other security related reasons.

§ 27.225 Site security plans.
The Site Security Plan must meet the following standards:

1. Address each vulnerability identified in the facility’s Security Vulnerability Assessment, and identify and describe the security measures to address each such vulnerability;

AlienVault ICS SIEM’s automated Vulnerability Assessment capabilities allow facility owners to specifically identify existing vulnerabilities. This awareness provides the basis for designing security measures to address each such vulnerability.

2. Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water-borne explosive devices, ground assault, or other modes or potential modes identified by the Department;

AlienVault ICS SIEM allows facility owners to model security measures against their deployed framework of cyber assets and refine security measures to prioritize those which address specific risks to the industrial process.

3. Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard for the appropriate risk-based tier for the facility; and

AlienVault ICS SIEM provides a platform for securely documenting the effectiveness of security measures. This forensically secure history of control system activity prior to and following the deployment of such security measures can be used to demonstrate how such measures meet or exceed performance standards for relevant risk-based tiers.

4. Specify other information the Assistant Secretary deems necessary regarding chemical facility security.

AlienVault ICS SIEM maintains a continuous awareness of system activity, allowing facility operators to provide accurate response to any information request.

When a covered facility updates, revises or otherwise alters its Security Vulnerability Assessment pursuant to § 27.215(d), the covered facility shall make corresponding changes to its Site Security Plan.

AlienVault ICS SIEM provides a baseline of empirical state and behavior to measure change against, as well as a platform for monitoring and validating authorized changes and detecting unauthorized changes or unforeseen impacts due to authorized changes.

A covered facility must also update and revise its Site Security Plan in accordance with the schedule in § 27.210.

A covered facility must conduct an annual audit of its compliance with its Site Security Plan.

AlienVault ICS SIEM provides forensically secure records of compliance with Site Security Plans that can be produced as reports.

§ 27.230 Risk-based performance standards.
(a) Covered facilities must satisfy the performance standards identified in this section. The Assistant Secretary will issue guidance on the application of these standards to risk-based tiers of covered facilities, and the acceptable layering of measures used to meet these standards will vary by risk-based tier. Each covered facility must select, develop in their Site Security Plan, and implement appropriately risk-based measures designed to satisfy the following performance standards:

(1) Restrict Area Perimeter. Secure and monitor the perimeter of the facility;

AlienVault ICS SIEM integrates with physical security technology such as video surveillance and access systems and correlates this information with cyber activity records. Out of compliance cyber activity by an internal user is associated with physical entry to the facility.

(2) Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility;

AlienVault ICS SIEM integrates with physical security technology such as video surveillance and access systems and correlates this information with cyber activity records. Out of compliance cyber activity by an internal user is associated with physical entry to the facility.

(3) Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,

(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and

(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;

AlienVault ICS SIEM integrates with physical security access technologies to monitor and enforce physical access authorization.

(4) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

AlienVault ICS SIEM allows facility owners to develop and maintain comprehensive deterrence packages covering all cyber and electronic physical security assets. The comprehensive visibility provided by the AlienVault platform allows detection of cyber attack at the moment of first contact with the facility. AlienVault ICS SIEM includes honeypot capabilities, allowing facility owners to create false assets to delay attackers and provide security staff captive observation of attackers.

(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;

(iii) Detect attacks at early stages, through counter surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
AlienVault ICS SIEM provides detailed visibility into all attempted contacts from external entities. ICS SIEM’s honeypot features allow facility owners to create false cyber assets and attract attackers into controlled environments where their methods and behavior can be studied. Supporting an integral electronic security perimeter and providing honeypot assets frustrates attempts to observe potential cyber targets.

(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning;

AlienVault ICS SIEM provides the earliest possible warning of cyber attack, from the first sign of out-of-policy behavior. ICS SIEM’s honeypot features provides facility operators the ability to create false cyber assets, luring attackers into attempting to compromise attractive false targets while operators gather information about them and enact mitigations.

(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;

AlienVault ICS SIEM.

(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;

AlienVault ICS SIEM.

(7) Sabotage. Deter insider sabotage;

In an industrial environment where AlienVault ICS SIEM has been fully deployed, all control system activity is monitored. Insider saboteurs would be deterred from attempting to use cyber control systems to compromise industrial processes due to the presence of a comprehensive monitoring system. Attempts at insider sabotage using cyber assets would have a high probability of being detected and prevented when the subject facility has implemented accepted best practices in policy management and implementation.

(8) Cyber. Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems;

Attempts at sabotage using cyber assets would have a high probability of being detected and prevented where the subject facility has implemented accepted best practices in policy management and implementation of AlienVault ICS SIEM. Unauthorized onsite or remote access attempts can be detected and trigger alarms and/or termination of access.

(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;

AlienVault ICS SIEM provides facility operators a complete cyber-incident response platform. As part of a comprehensive emergency response plan, ICS SIEM allows for the implementation and exercise of cyber response plans. Alerting of appropriate staff, law enforcement and first responders, automated cyber responses (such as shutting down remote access, removing non-essential devices from the subject industrial network…) can be triggered by defined emergency conditions. Staff can use the actual data produced by the subject industrial networks which has been archived by AlienVault ICS SIEM to plan and enact exercises specific to their environments.

(10) Monitoring. Maintain effective monitoring, communications and warning systems, including,

AlienVault ICS SIEM is specifically designed to provide uninterrupted and effective monitoring of all
Aspects of cyber activity and includes automated testing, communicating and warning systems.

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

AlienVault ICS SIEM automatically and continually tests the security and availability of all cyber assets.

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

The AlienVault ICS SIEM platform continually tests all aspects of security automatically, and contains tools to perform customized security testing to fit any requirement facility operators present. Deficiencies in cyber security are automatically noted, guiding the correction of them and recording results for later inspection.

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

AlienVault ICS SIEM includes Service and Network Availability functionality that will detect loss of function of any connected device or service.

(11) **Training.** Ensure proper security training, exercises, and drills of facility personnel;

AlienVault ICS SIEM provides a platform for implementing cyber security awareness communication. Personnel access to cyber assets can be made contingent on completion of scheduled reinforcement training. The system can produce documentation validating that the awareness regime is being enforced. Establishing and maintaining cyber security awareness regimes is facilitated by the system’s situational awareness and forensically accurate historical visibility.

The system can be configured to alert personnel via email when training is required or when critical information must be communicated in a timely fashion.

(12) **Personnel Surety.** Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

(i) Measures designed to verify and validate identity;

AlienVault ICS SIEM maintains a hierarchy of personnel with authorized cyber access to Critical Cyber Assets, including their specific electronic and, where integrated with physical-access identification systems, physical access rights to Critical Cyber Assets. AlienVault system can remove all cyber access rights and maintain a forensic record of user account usage and time of termination.

(13) **Elevated Threats.** Escalate the level of protective measures for periods of elevated threat;

Policies to be enforced during periods of elevated threat are implemented in AlienVault ICS SIEM. These policies would be designed to escalate the level of protective measures. During a period of elevated threat facility operations are measured and enforced according to these policies.

(14) **Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;**
AlienVault ICS SIEM allows facility owners to immediately respond to specific threats of cyber attack. Indications of the threat being realized can be immediately ascertained and mitigation applied as necessary. Using the visibility provided by the AlienVault platform, countermeasures specific to the facility can be developed to the specific threat.

(15) **Reporting of Significant Security Incidents.** Report significant security incidents to the Department and to local law enforcement officials;

The AlienVault system can provide automated reporting of Cyber Security Incidents to law enforcement if desired, and/or act as a platform for producing such reporting following a significant security incident.

(16) **Significant Security Incidents and Suspicious Activities.** Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

The AlienVault dashboard provides a single console for incident response team. Roles and responsibilities of Cyber Security Incident response teams are defined, Cyber Security Incident handling procedures, and communication plan documentation can be embedded. Automated communications can be created including pertinent data and sent to predefined individuals and groups.

(17) **Officials and Organization.** Establish official(s) and an organization responsible for security and for compliance with these standards;

The granular access controls inside the AlienVault platform allow for authority for specific actions to be delegated to specific individuals. All use of this authority is forensically archived for auditing purposes. The AlienVault platform allows for higher-authority users to create exceptions to policies for lower-authority users. All actions are forensically archived and can be used to produce report documentation.

(18) **Records.** Maintain appropriate records; and

AlienVault ICS SIEM can produce forensically accurate reports on all cyber activity on the subject industrial control system.

(19) **Address any additional performance standards the Assistant Secretary may specify**

AlienVault ICS SIEM provides facility owners consistent visibility into current and past cyber security policies and implementation effectiveness. This platform of awareness allows facility owners to respond to performance standards as they evolve.