CYFLARE
The threat stops here.

# 7 Things You're Probably Not Doing with Your AlienVault Deployment

Every week, we encounter existing AlienVault deployments marginally, and key features are not being leveraged. This infographic highlights key features within AlienVault that can quickly and easily be enabled. These features are a core part of our deployment checklist for AlienVault and are must-haves for every deployment to extract maximum value out of the solution.

## Vulnerability Scanning

Despite being a cornerstone for the AlienVault platform, most clients don't enable credential-based (more extensive) scans. This can be configured easily and major value realized within hours. An essential part of a security program is understanding your network vulnerabilities and operationalizing and updating those systems. Patched and updated systems are far less likely to be exploited; the first step is identifying the systems requiring the updates.

## Dark Web Enablement

Dark Web Scanning alerts you when there is a direct hit for your credentials using @yourdomain accounts, includes information on whether the password was posted, and allows up to 10 personal email IDs for monitoring. This provides immediate value on day 1 to identify possibly compromised user accounts that need to be investigated. We use this tool in the SOC consistently to correlate against login events, locations of those events, failed logins, and brute force attackers. Turn this feature on straight away!

## Asset Discovery & Classification

A quick and easy value-added feature is to sweep your network segments to identify devices on your network(s). Performing asset discovery allows you to take inventory of assets on the network and discover rogue devices — and it helps your security team *classify* those assets. Classifying the assets becomes critical when investigating potentially anomalous events. Understanding what the device is and its functional role and having context around what is normal usage goes a long way when determining if it is expected behavior or not.

## Filtering Rules

Enabling filtering rules is an essential component of setting up the system. Filtering log data that is not essential, required for compliance, or essential for investigation allows you to store fewer data sets. This can potentially reduce your AlienVault costs and reduce additional noise from potential alarms that would be generated that are false positives and not essential. Filtering specific events and behaviors that are known should be done within the first 30 days of deployment.

## Help Desk Integration

Integrating alarm notifications once the solution is properly tuned is essential for staying aware of the events as they happen. We highly recommend integrating with the Slack app to stay up to the minute on what Is happening with your deployment. Once the system is tuned and only meaningful alarms are generated, it is recommended warnings are sent to the ticketing system for event tracking and proper diligence.

## Compliance Reporting Enablement

Without classifying your assets as HIPAA, PCI, NIST assets, etc., the compliance template reports will not populate any data, will not give your auditor what they need to see, and will not help you achieve compliance. In-scope assets must be properly classified, or the compliance correlation and reporting will not work. Simple fix, high value on this configuration step!

## AlienApp Enablement

This is our favorite part of the deployment. Did you know you could be automating remediation actions right now? AlienVault continues to publish direct integrations with major vendors to easily ingest event data and take action by creating tickets, quarantining endpoints, shutting machines down, blocking IPs at the firewall, and much more. As of this writing, there are 17 AlienApps available for integration.

**CONTACT US!**

**sales@cyflare.com**
**877-729-3527**