ADLUMIN SIEM PLATFORM CHECKLIST

Daily Checklist

- ☐ **Review each new Critical and High detection** in the dashboard**.**
- ☐ **Always Investigate Critical and High detections.**Use Investigate (+/-) 5 minutes, 1 hour, 1 day to scope the timing of suspicious account and system activity anomalies.
- ☐ **Acknowledge all detections** that have appeared since the prior day. Click on the Show Activity Histogram toggle switch to review high level details about new unacknowledged detections. Refer to the detection details table for more granular information. After reviewing a detection, use one of the many methods discussed in Training Session II to acknowledge and clear the detection from the dashboard.
- ☐ **Implement tracking of any suspicious accounts or systems** using the **Enhanced Monitoring features** in the tools menu**.**
- ☐ **Clear out unnecessary accounts and systems** that have enhanced monitoring trackers.
- ☐ **Launch an investigation** to track a series of suspicious events over time.

Weekly Checklist

- ☐ **Review all Critical and High detections** analyzing them for anomalous activity.
- ☐ **Review current investigations in progress** to track a series of suspicious events or activity over time.
- ☐ **Run a "Privileged Account Activity Report"** and analyze the results. Investigate the activity of all suspicious privileged accounts.
- ☐ **Run an "Account Manipulation Report"** to review newly created or modified accounts within the environment. Investigate suspicious account manipulation activity.

Monthly Checklist

- ☐ **Review network health statistics for changes in compliance violations.** Remove newly identified compliance violations using Adlumin, Active Directory, or some other means.
- ☐ **Run an "Account Group User Audit Report"** for your domain's privileged groups. Review and analyze the results removing all unnecessary privileged accounts.
- ☐ **Run "Group Activity Report" for highly privileged groups** like "Enterprise Admins," "Domain Admins," and "Administrators."
- ☐ **Review At-Risk shares, systems, and groups** making the necessary network configurations, active directory modifications, system configurations, or exemptions to reduce your At-Risk level and increase your network health index.

Quarterly Checklist

- ☐ **Run a "Server Privilege Analysis" Report in Privilege Analysis under the Tools Menu** removing unnecessary access to servers that hold sensitive data.
- ☐ **Run a "Share Drive Access Audit" Report in Privilege Analysis under the Tools Menu** and remove unnecessary access to network shares holding sensitive data.
- ☐ **Run a "Server Activity Report" in the Reports section** along the top of Dashboard reviewing activity and access to sensitive servers.
- ☐ **Investigate all suspicious activity and access by reviewing events and launching an investigation.**