Automating NERC CIP Compliance

How Swimlane's SOAR solution can ease NERC CIP compliance

About Swimlane

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market. By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across the security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.

The unified defense platform offers a broad array of features aimed at helping security operations centers (SOCs) to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire organization.

Swimlane's support of NERC CIP

Swimlane's security orchestration, automation and response (SOAR) solution not only provides coverage of many security-based NERC CIP controls, but by leveraging Swimlane's workflow automations and integrations with your cyber assets, you can achieve additional support of overall audit objectives.

Swimlane helps support various CIP controls, most notably CIP 008-5/-6, involving incident reporting and response efforts. Existing content and use cases of common attack methods provide immediate resources for SOC teams looking to automate supported controls. Workflows and integrations can help your team manage alerts coming from various boundary protection devices, aiding in finding the needle in the haystack to reduce mean-time-to-detect (MTTD), mean-time-to-remediate (MTTR), and noncompliance.

The reporting requirements for NERC CIP can be challenging: Organizations must produce a great number of Reliability Standard Audit Worksheets (RSAW), which are audit reports that need to be populated, centrally collected, reviewed, and sent to archive for future audit validations. Swimlane can facilitate portions of the RSAW process, audit package preparation, and CIP-003-7/-8 Security Management Controls.

Additionally, Swimlane can automatically capture a full audit trail of incident investigation steps and results for compliance and governance and track user interactions and changes within the platform to ensure completeness and accuracy in support of control objectives and remediation efforts.

Benefits of automating NERC CIP compliance

- Save time collecting audit evidence and building the audit package, which are very time consuming and resource intensive for any audit program.
- Realize cost and time savings through freeing up security teams from manually supporting audit requests or ownership of controls, which take away from daily job duties.
- Efficiently manage the wide range of periodic compliance reviews with workflows and automated communications.
- Quantify the cost savings of automating aspects of compliance programs with ROI-focused dashboards.