A JANUS Case Study | June 2026

AUTOMATED STAKEHOLDER NOTIFICATION & USER REPORTING: How JANUS Reduced Incident Blind Spots Across Regulated Environments

TEL: +1 203.251.0200

INFO@JANUSASSOCIATES.COM

1200 HIGH RIDGE ROAD STAMFORD, CT 06905

JANUSASSOCIATES.COM

Client Context

JANUS Associates works with security and risk leaders across federal agencies, mid-market commercial organizations, healthcare providers, and financial institutions that operate under strict regulatory and contractual obligations. These organizations typically run complex environments with SIEM, EDR, identity platforms, and ticketing tools already in place, but still struggle to turn alerts into coordinated action.

In each of these sectors, regulators and oversight bodies expect timely incident notification, complete audit trails, and demonstrable security awareness training programs. Frameworks such as NIST CSF 2.0, NIST SP 800-53, HIPAA, GLBA, SOC 2, PCI DSS, and FedRAMP require not just detection, but effective communication, documentation, and user participation in incident response.

Challenge

Across JANUS client environments, one pattern shows up repeatedly in post-incident reviews: the right people are informed too late (or not at all) when a significant cyber event occurs. The core challenges fall into two related gaps:

1. Stakeholder notification gap

In many incidents, the SIEM and EDR tools work as intended: alerts are generated and analysts investigate. However, the handoff from technical detection to business and regulatory stakeholders is inconsistent and highly manual. Analysts often spend 20–40 minutes deciding who to notify, executives learn of incidents informally, and regulatory notification clocks start running before anyone realizes it.

2. User reporting gap

At the same time, end users regularly see suspicious behavior—strange emails, unexpected login prompts, unusual data access, but fail to report it because they are unsure what to report, when to report, or where to report. Reported tips may sit in inboxes, and users often receive no feedback, eroding trust in the reporting process.

The net effect is increased dwell time, higher regulatory exposure (e.g. HIPAA and FISMA notification timelines), incomplete audit trails, and a missed opportunity to turn the workforce into an active detection layer.

JANUS Approach

JANUS Associates engaged with clients to design and implement a combined solution that addresses both the outbound and inbound sides of incident communication: automated stakeholder notification and structured user incident reporting training.

The engagement followed a structured cybersecurity consulting and IT risk assessment approach:

Current-state assessment

- Review existing incident response practices, notification processes, and escalation paths.
- Map applicable regulatory and contractual notification obligations by vertical (e.g., HIPAA 72-hour reporting, FISMA and FedRAMP requirements, GLBA and SEC guidance).

Design of notification logic

- Define severity tiers and event triggers across ransomware, credential compromise, insider threat, and phishing scenarios.
- Build a notification matrix that specifies who must be notified, how quickly, and by what channel for each type of incident and vertical.

Training and reporting channel strategy

- Develop a user incident reporting training curriculum that answers three questions for every user: what to report, when to report, and where to report.
- Design low-friction reporting channels (email buttons, aliases, ITSM categories, hotlines, and anonymous channels) and integrate them into the incident management process.

I**mplementation of roadmap and governance**

- Establish a phased roadmap covering foundation, training rollout, SOAR integration, and continuous improvement.
- Clarify roles and responsibilities across SOC, IT, GRC, Legal, HR, end users, and JANUS advisors through a RACI model.

Solution and Implementation

JANUS and the client teams implemented a joint solution built on two pillars: SOAR-driven automated stakeholder notification and a targeted user incident reporting training program.

Automated Stakeholder Notification

Using the client's SOAR and SIEM platforms, JANUS helped define and implement playbooks that automatically notify the right stakeholders within defined SLAs when specific incident conditions are met.

Key elements included:

- **Scenario-based triggers.**
  - Ransomware detonation and lateral movement.
  - Credential compromise and account takeover.
  - Insider data exfiltration events.
  - Phishing campaigns leading to malware execution or credential harvesting.
- **Notification matrix.** For each severity level and trigger, the SOAR playbooks:
  - Identify required recipients (e.g., CISO, CIO, Legal, HR, IT Ops, Privacy Officer, Compliance Officer, business unit heads, JANUS on-call advisor).
  - Enforce SLAs (e.g., under 5 minutes for CRITICAL events and key regulatory triggers).
  - Execute automated actions such as account disablement, legal hold triggers, and bridge call initiation where appropriate.
- **Regulatory alignment.** The playbooks incorporate vertical-specific obligations:
  - Federal environments: FISMA and NIST SP 800-53 requirements, including rapid reporting to ISSO, Authorizing Official, and agency CISO.
  - Healthcare: HIPAA/HITECH breach notification timelines and training mandates.
  - Financial services: GLBA, SOX, PCI DSS, and SEC material incident expectations.
  - Commercial: SOC 2, NIST CSF, and contractual SLAs with customers.

All notifications are logged with timestamps, recipients, and delivery status, creating a defensible audit trail that supports compliance audits and post-incident reviews.

User Incident Reporting Training Program

To ensure the inbound side of incident communication is equally strong, JANUS designed an incident reporting training program tailored to each client's environment.

The program is built around these principles:

- Training must clearly explain what to report, when to report, and where to report.
- Reporting channels must be easier to use than ignoring the issue.
- Content is tailored to the client's threat landscape; generic awareness material is de-emphasized.

The curriculum includes modules such as:

- Recognizing a security incident (phishing, ransomware indicators, unusual account behavior).
- How to report an incident (channels, expectations, and what happens next).
- Phishing identification and reporting, with integrated simulations and one-click “Report Phishing” buttons.
- Data handling and classification, insider threat awareness, and role-specific obligations for IT, SOC, GRC, and Legal.

Training is delivered through LMS-based modules, phishing simulation campaigns, tabletop exercises, and role-based live sessions. Completion is tracked by department and role, and gaps are escalated through governance dashboards.

Reporting Channel Design and Integration

JANUS worked with the clients to implement a small set of high-impact reporting channels, including:

- Dedicated security email aliases and ITSM categories.
- Integrated “Report Phishing” buttons for email clients.
- Help desk hotlines and anonymous reporting options for insider threat concerns.

All channels feed into the SOAR triage queue, where user-submitted reports automatically create low-severity incidents, trigger acknowledgment responses, and are tracked end to end.

Results and Impact

After deploying automated stakeholder notification and the user incident reporting training program, clients saw material improvements in both notification and reporting performance.

On the **notification side**, organizations achieved:

Faster stakeholder awareness

- Mean Time to Notify (MTTN) for CRITICAL incidents dropped from highly variable, manual processes to a consistent target of under five minutes from SOAR classification.

Consistent delivery against SLAs

- Required recipients received notifications reliably within defined SLAs across scenarios such as ransomware, insider threat, and credential compromise, rather than relying on ad-hoc analyst judgment.

Stronger regulatory posture

- Regulatory notification compliance rates improved as GRC and Legal teams received automated alerts when regulatory thresholds were met, reducing the risk of missed HIPAA, FISMA, or GLBA timelines.

Complete audit trails

- Notifications are now logged with full timestamp, recipient, and acknowledgment data, improving audit defensibility and simplifying post-incident investigations.

On the **training and reporting side**, clients realized:

Higher training participation and accountability

- Completion rates for targeted security awareness and reporting modules increased, with executive dashboards tracking progress by role and department.

More active user reporting

- User-submitted reports increased in volume, giving SOC teams earlier visibility into phishing campaigns, account takeover attempts, and insider threat indicators.

Improved phishing resilience

- Phishing simulation reporting rates trended upward over time, with users more likely to report suspicious emails rather than click or ignore, supported by immediate feedback loops.

Closed feedback loops with end users

- Automated acknowledgments and follow-up messages helped eliminate the “black hole” perception around reporting, encouraging users to continue contributing to detection.

Together, these changes reduced dwell time, improved regulatory confidence, and gave leadership more reliable, timely insight into cyber incidents.

> ***“Before this program, we relied on individuals to make judgment calls under pressure. Now, our stakeholders are notified consistently within minutes, and our users know exactly how to raise a hand when something looks wrong.” – CISO, U.S. Regulated Organization***

Why JANUS Associates

JANUS Associates brings a combination of cybersecurity consulting, IT risk assessment, incident response, and training expertise tailored to regulated environments.

Key differentiators for this engagement included:

Framework-driven approach

- Alignment with NIST CSF 2.0 GOVERN, DETECT, RESPOND, and RECOVER functions and with sector-specific regulations from the outset.

Integration of technology, process, and people

- Rather than focusing solely on tools, JANUS combined SOAR and SIEM playbooks with stakeholder processes, user training, and reporting channel design.

Cross-vertical experience

- Experience with federal, healthcare, financial services, and commercial organizations enabled JANUS to configure notification and training to meet multiple regulatory regimes simultaneously.

Ongoing advisory and maturity assessment

- JANUS continues to support clients through maturity assessments, tabletop exercises, curriculum updates, and SOAR tuning, keeping incident response programs aligned with evolving threats and regulations.

Organizations that want to reduce incident notification delays, strengthen regulatory compliance, and build a genuine reporting culture can engage JANUS Associates to:

- Conduct an incident notification and reporting maturity assessment aligned with NIST CSF 2.0.
- Design and implement SOAR-backed notification workflows tailored to their vertical, environment, and regulatory obligations.
- Develop and roll out a targeted user incident reporting training program with integrated phishing simulations and reporting channels.

To explore how this automated stakeholder notification and user reporting model can work in your environment, **contact JANUS Associates to schedule an incident response readiness consultation.**