# GUIDED INVESTIGATIONS
## ENSURING CONSISTENCY, EFFICIENCY & DEFENSIBILITY

**FORCE MULTIPLIER**
Amplify the impact of SMEs and senior investigators

**BUILT-IN INSTRUCTIONS**
Guide junior investigators each step of the way

**ON-DEMAND OVERSIGHT**
Provide transparency without slowing down

D3 is known for its full-lifecycle solutions. One of our key differentiators in the market is that we can cover the entire incident process from SIEM detection, to automated data gathering, orchestrated incident response, and case management that supports forensics, legal, and compliance functions. Our case management module has always been a strength, but we've recently revamped it to offer even more value through **guided investigations**.

We call it "investigations on rails", because of how it streamlines the case management process, keeping everyone on track, and minimizing the possibilities for human error and inefficiency. D3's guided investigations solution also supports compliance efforts, with an embedded policy library and the ability to dynamically generate workflows based on region, incident type, and more.



## BRIDGE THE SKILLS GAP

Transform policies and SME knowledge into on-demand instructional elements that guide investigators through every step, including:

- **Interviews**
  gather information in a legally defensible manner

- **Correlations**
  provide examples and tips to ensure accuracy

- **Reporting**
  save report templates with SME commentary

**Insider Threat**

Legal Hold

**Before sending, check:**
- **Custodian History**
- **Recipient List**
- **Acceptance Notice**

# GUIDED INVESTIGATIONS

Guided investigations are at the heart of D3's case management offering. This methodology keeps users of all experience levels in line with the established processes and best practices for complex investigations. Even with the best conventional tools, training, and documentation, users might not recall the next step in the workflow, take the next step quickly enough, or locate the information they need to inform their decision.

## STANDARDIZED PROCEDURES

Using D3's "investigation on rails" capabilities helps keep your entire team working from the latest procedures and policies. This allows companies to regularly implement improvements, without the cost of additional training or the risk of confusing their investigators, because the changes will be integrated directly into the guidance provided by D3.

## CONFIGURATION CRITERIA

D3's guided investigations are configured based on five criteria: business unit, country, case category, priority, and "other" category. The configuration of these variables during intake will trigger completely different processes to follow. For example, the country selection will determine what terminology is used in the interface, as this varies greatly around the world.

## TOOLTIPS

Throughout the entire case intake and investigation process, the user will have access to on-demand tooltips and contextual instructions for each form, section, and field. Tooltips—which appear when the user hovers the mouse over an element—can be fully customized by user administrators, and are dependent on configuration criteria. Don't know your configuration criteria? That's no problem—our software comes loaded with best practices-based, industry-tailored instructional elements.

## TASKS

Required tasks, along with alerts for potential SLA violations, are always prominently displayed in the interface. Tasks are ranked by urgency, with color-coding and dynamic filtering designed to keep users focused on high priority or overdue tasks. The task management view can also be filtered to show only the tasks relevant to the current stage of the investigation. Custom tasks can be added by the user, tracked, and reported on.

# COMPLIANCE

Because case management can involve the investigation of numerous incidents, a case management solution needs to account for the complex compliance requirements that may result from bringing together incidents of disparate origins and types. D3's granular configurability accommodates the compliance needs of groups and business units in different regions. This facilitates compliant investigations in complex scenarios, such as when the applicable regulations and policies where a case originates are different from the requirements of the region in which it is being investigated.

## CONFIGURATION BY COUNTRY OR BUSINESS UNIT

D3's case configuration criteria include country and business unit. This locks the investigation into compliant processes that meet the latest regulatory or legal requirements, thus eliminating the risk of human error related to new or evolving regulations.

## POLICY LIBRARY

Internal policies and external regulations can be saved to D3's policies library to be linked to cases, or made available for convenient referencing. Default policy options can be modified based on a case's configuration criteria, to ensure that analysts are able to follow the complex requirements of large organizations.

# COLLABORATION

Collaboration is absolutely necessary when investigating major incidents, but effective collaboration requires strong communication. Everyone needs to know their responsibilities, deadlines, and the boundaries they need to operate within to stay compliant with confidentiality requirements. D3's collaboration tools keep everyone working effectively toward their common goals.

## COMMUNICATION

D3 provides a centralized communications platform. This supports collaboration by ensuring that everyone is aware of all relevant messages, and that messages are sent to only the appropriate people with minimal redundancy. All communications are tagged with case number IDs and fully logged for audit purposes. There are even communication templates included based on configurability criteria.

## STAGE-BASED WORKFLOWS

D3's stage-based interface literally keeps everyone on the same page, by only showing the relevant tasks, information, and features for the current stage of the investigation. This supports collaboration by preventing users from getting too far ahead or behind of the overall investigation. Access controls are also stage-dependent, for more granular information security.

## REMINDERS AND ALERTS

Reminders and alerts can be sent for required tasks, such as assigning a team member to send an incident acknowledgment letter, or scheduling an interview. Customizable reminders can be used alongside SLA-driven alerts. Particularly important SLA violations are sent to managers as alerts so they can follow up.

## REPORTING

Collaboration requires support from leadership, which requires leadership to understand what's going on in the investigation. D3 provides appropriate access to managers in the investigator's reporting chain, enabling the sharing of summary reports, metrics/KPIs, historical case data, and investigation timelines.