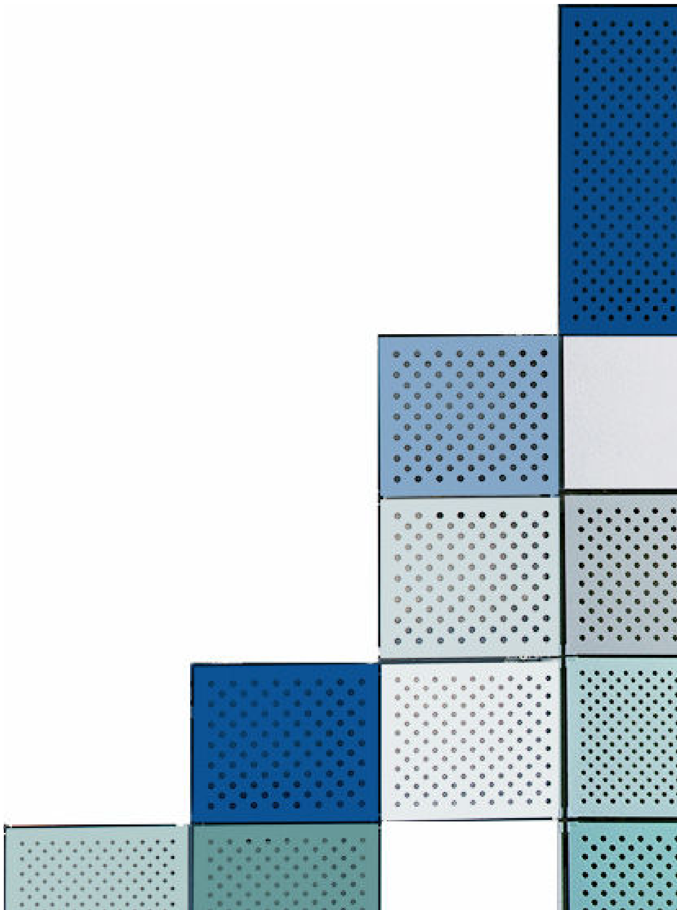
ONTIC

WHITEPAPER

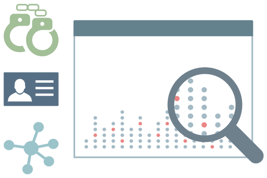
Centralized Intelligence: The Future of Incidents, Investigations and Case Management

THE CRITICAL NEED FOR ALWAYS-ON, COMPREHENSIVE INCIDENT AND INVESTIGATION PROCESSES



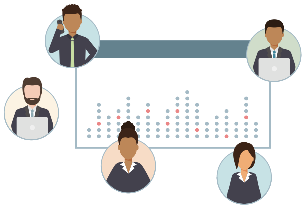
Executive summary

Disruption of any kind can impact business performance. These crises come in many forms, from issues with the supply chain or adverse weather events to physical or digital security incidents and business crimes. For example, organizations ranging from agriculture to healthcare incurred financial losses between 6-10% of annual revenues as a result of the supply chain disruptions of 2020, not counting the impact to brand reputation. Further, increasing crime rates and newly organized crime rings are leading to high costs, to the tune of $68.9 billion in product losses in retail. To make matters worse, the insurance industry has responded to increased risk by making it harder to obtain commercial and cyber insurance coverage — or, in some cases, denying coverage altogether.



INCIDENT MANAGEMENT

The process of capturing and documenting incidents (physical or digital) to activate appropriate response and to mitigate business disruption or damage to assets.



INVESTIGATIONS

The process of conducting research, collecting and documenting data, records and findings to support analysis, tracking and reporting for critical insights and actionability.

CASE MANAGEMENT

A customizable, central system of all information related to incidents and investigations organized for confidential collaboration, in-depth analysis and ongoing monitoring.

$9.44M

Average cost of data breach in the US[1]

$120B

Cost of workplace violence in the US[2]

$50B

Cost of crime in the workplace to US organizations[3]

[1] IBM, Cost of a data breach 2022, (Accessed October 3, 2022), *https://www.ibm.com/reports/data-breach*

[2] InterWest Insurance, As Workplace Violence Increases, a New Policy Covers Associated Costs, (Accessed October 3, 2022), *https://www.iwins.com/as-workplace-violence-increases-a-new-policy-covers-associated-costs/*

[3] Elaine Pofeldt, This crime in the workplace is costing US businesses $50 billion a year, (September 12, 2017), *https://www.cnbc.com/2017/09/12/workplace-crime-costs-us-businesses-50-billion-a-year.html*

EXECUTIVE SUMMARY

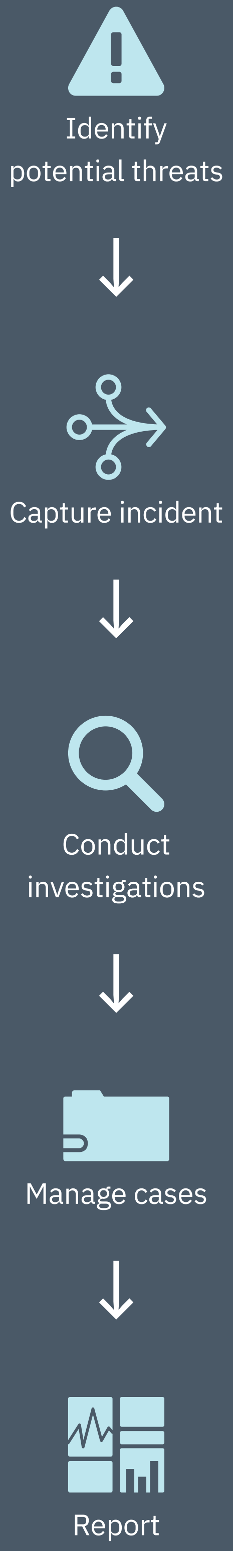
While physical security, cybersecurity and IT, human resources, and legal and compliance leaders all deal with threats and business risks, each have their own processes and tools to document and manage incidents. These department silos create walls around threat intelligence that have real-life impacts on business continuity. In a recent survey of C-level employees, half noted that 51% or more of threats that disrupted business continuity resulting in harm or death could have been avoided if teams shared and viewed the same intelligence in a single platform.

Real-world events, internal demands and the frustrations of internal teams have created the demand for real-time, integrated intelligence solutions to centralize all information related to incidents – digital and physical – and the resources necessary to conduct investigations. By creating 'one pane of glass' for incidents, investigations and case management, organizations ensure that they have actionable data to identify and manage risks and eliminate vulnerability gaps. Further, applying intelligence to cases can provide critical insights that improve proactive risk mitigation to prevent incidents, including theft, violent attacks and organized crime.

Incidents, investigations and cases could be managed in spreadsheets, paper folders, across email or in specialized tools. Some of the specialized tools designed to detect threats, log incidents, investigate, report and track cases include:

- Connected systems data
  (vehicle, visitor management systems (VMS), access control, CRM)
- Public record search
  (OSINT, Public, Criminal, Civil Records)
- Social media and dark web monitoring
- Cyber threat intelligence tools
  (insider threat monitoring, intrusion detection, endpoint protection)
- Fraud detection software
- HR records
- Case management software

THE STAGES OF INCIDENT MANAGEMENT, INVESTIGATIONS AND CASE MANAGEMENT



Identify potential threats

↓

Capture incident

↓

Conduct investigations

↓

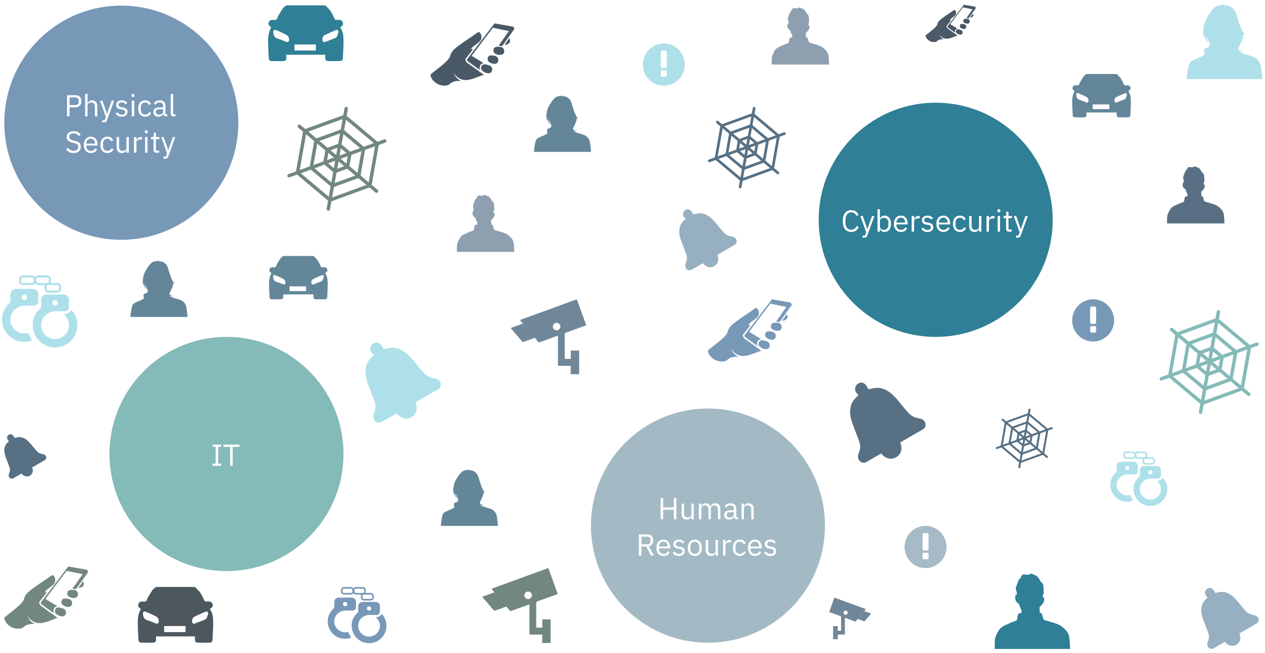
Manage cases

↓

Report

Outside of digital incidents, which can include automated intelligence tools and push notifications that an incident has been detected, security and investigation tools mostly rely on manual spreadsheets, documents or pull-based solutions. Security teams must manually watch for or search for threat detection signals from multiple sources, relying heavily on instinct – and some luck – to identify threats. Once a threat has been identified, investigative teams must research and collect data from all the various internal tools and public record databases to create a complete dataset about an incident or person of interest (POI), dispatch personnel to manage a task, and manage cases.

Many security teams use a case management software solution to help them document, track and report on incidents, investigations and cases. Most case management solutions are built as empty vessels – security teams are responsible for putting in the history, loading the cases, manually entering data from all of these external tools and sources, and coordinating the dispatch of security personnel. Any coordination between individuals, across functions or with external third parties (e.g. law enforcement) is also external to the tool, primarily by email or phone, supported by manually compiled reports.



While physical security, cybersecurity and IT, human resources, and legal and compliance leaders are trained in threat assessment and threat management, departmental silos and disparate point solutions are hampering effective company-wide threat and risk management. According to a 2022 survey of physical security, legal and compliance executives, 84% agreed that the lack of unified intelligence and poor communication between teams at their organization resulted in missed threats – sometimes up to half of all threats. Additionally, these four departments often assess and investigate the same threats – a source of significant redundancy and inefficiency.

The critical need for a consolidated, real-time platform

The security industry has traditionally been presented with rigid solutions akin to empty containers and workflows. These solutions have their purpose, but when a new use case or business need emerges, it can be difficult for a solution like this to serve these changing needs. As a result, more and more layers of point solutions are added and teams are left with the complex task of trying to piece together a holistic picture of threats, investigations, and risk intelligence.

Today's security teams are at an inflection point, considering if their point solution(s) are keeping pace with their needs.

Are point solutions keeping pace with your needs?

COST

Point solutions often have a lower up-front or one-time cost, but these costs can quickly add up as more solutions are added and more time is invested in managing the systems or pulling in outside data. Multiply this cost by each department or team.

TIME & PERSONNEL

Research is being conducted using disparate tools and manually recorded, consuming significant time. Pulling a report, for example, could take much longer when different information is pieced together from various systems. Department silos are likely to lead to duplicate, redundant threat assessments and investigations, and inefficient cross-functional communication.

INFLEXIBLE & SILOED TOOLS

Many point solutions are either locked into specific functions of the enterprise or are inflexible to emerging needs, increasing the need for new point solutions and resulting in a more complicated tech stack.

INCONSISTENT DATA & REPORTS

Documentation and findings are inconsistent and unstructured, often requiring manual manipulation and documentation of insights to create an actionable report.

ACCOUNTABILITY

Lack of visibility and accountability over the progress of investigations, how much time is spent, or ongoing monitoring of completed investigations or closed cases.

MISSED THREATS

With data in multiple systems, the biggest danger of a tech stack of point solutions for security teams is missed threats. A lack of unified intelligence can inhibit situational awareness and an ability to see and act upon the complete picture or to identify common issues or patterns. Further, duplicate and uncoordinated efforts can create delays in response times. Missed threats and delayed response times increase the threat impact.

OUTDATED INTELLIGENCE

Investigators need to manually collect information from disparate systems to support active or open cases and investigations. Data on activity or actions related to a POI risk becoming out of date as soon as it is pulled.

THREAT IMPACT CAN TAKE MANY FORMS:

Financial • Reputational • Operational
Human Capital • Legal & Regulatory

Most organizations today are digitally transforming operations and outdated manual processes. Still, to date, many efforts have focused on value-creating areas of the organization. However, as organizations continue to face the increased volume and complexity of threat data and the pressure to protect operations and reduce liability, there is a growing recognition of the need for an always-on, centralized threat intelligence, incident and investigative solution.

As organizations lean more heavily on frameworks such as those developed by the National Institute of Standards and Technology (NIST), there is the recognition that enterprise-wide incident management could benefit from the same structured processes. For example, the NIST SP 800-61 incident response life cycle provides an important clue as to the circular nature of incident handling – that the way we detect, contain, and learn from past incidents helps inform, prepare for or prevent future incidents from occurring.

Since today's incidents rarely fit neatly inside any one box (department/team/incident type), it makes sense to apply the incident response lifecycle at scale across the organization:

1. PREPARATION

Implement controls to limit the number of incidents that occur. Continually gather real-time and historical signals for insights to better inform preparation.

2. DETECTION & ANALYSIS

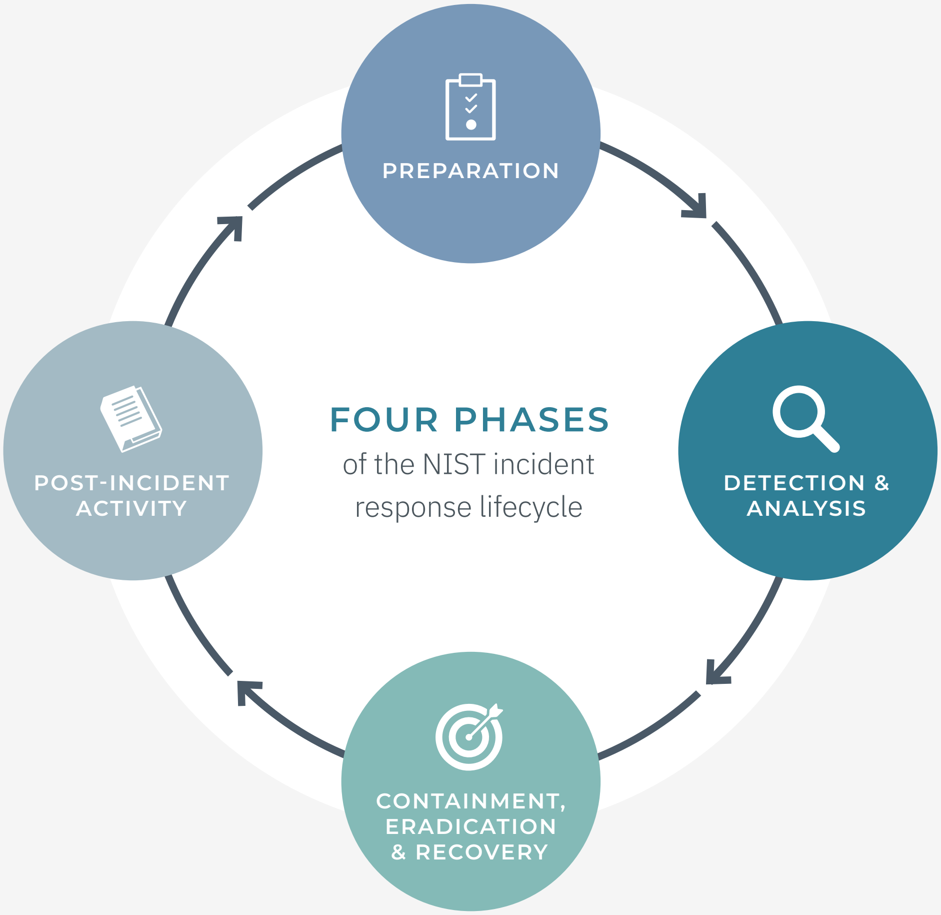
Rapid detection of potential threats from various sources: people, incidents, social media, IoT devices and more. Rule-triggered alerts, early investigations to inform threat severities & risk assessments.

3. CONTAINMENT, ERADICATION & RECOVERY

Continue investigation and threat response activities to contain or mitigate the impact of the incident. Continuously monitor cases.

4. POST-INCIDENT ACTIVITY

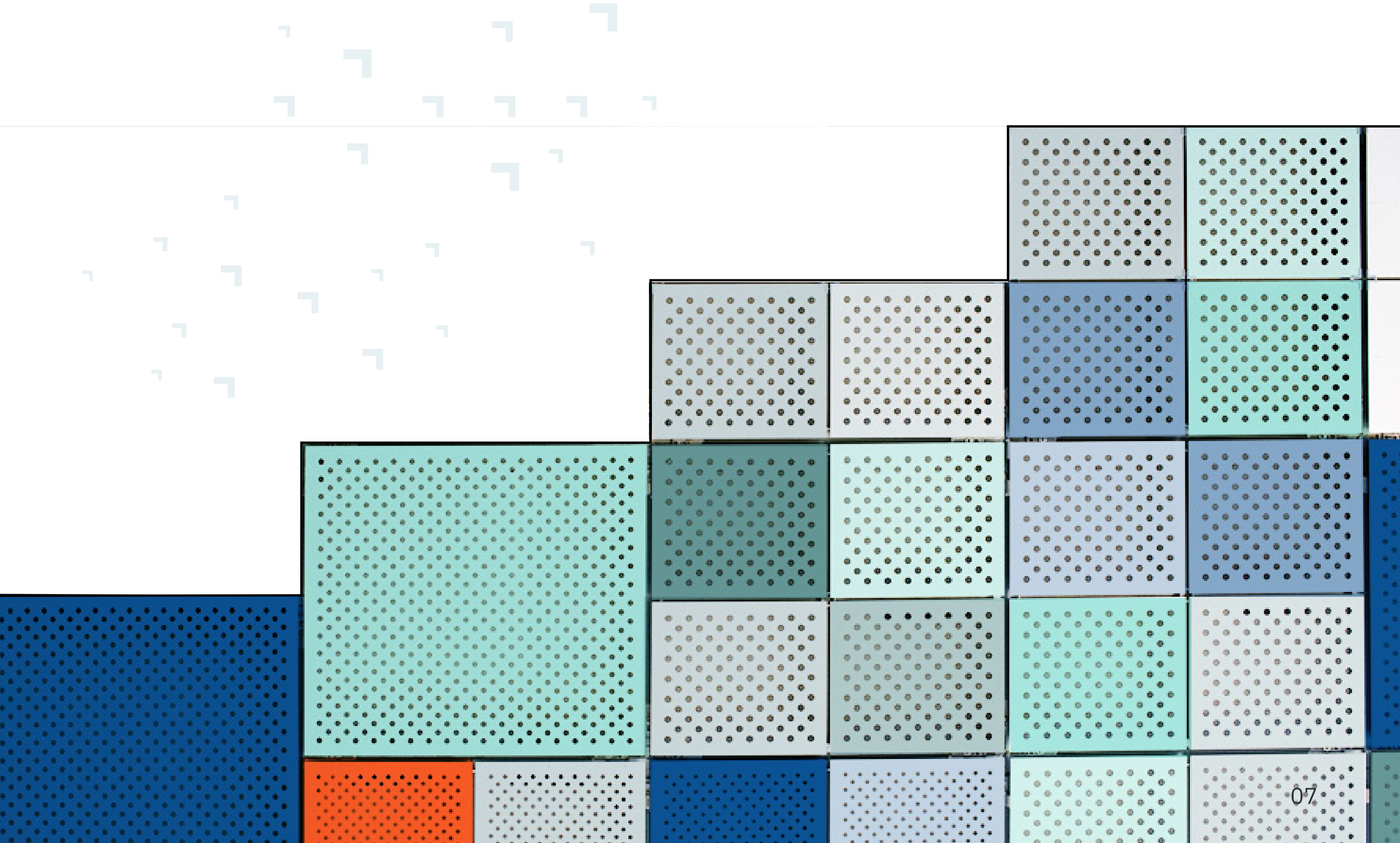
Report and post-incident learning to inform improved preparation or response activities, preserve critical knowledge and best practices.


PREPARATION
DETECTION & ANALYSIS
CONTAINMENT, ERADICATION & RECOVERY
POST-INCIDENT ACTIVITY
FOUR PHASES
of the NIST incident response lifecycle

THE CRITICAL NEED FOR A CONSOLIDATED, REAL-TIME PLATFORM

Consolidating multiple threat intelligence, monitoring and alerting solutions, investigation and case management solutions into a single platform helps accelerate threat detection and response efforts, improve communication across functions and enhance accountability. Further, having a centralized repository for all intelligence, incidents, investigation and associated activities allows the organization to detect and measure not only security outcomes but business outcomes as well.

At the business level, this translates into costly threats that are avoided or remediated quickly, recovered losses from theft or fraud, reduced insurance claims, and reduced operational downtime Lastly, this same self-informing incident response process is designed to improve organizational effectiveness over time, putting the organization in a better position to meet the demands of today’s evolving threat landscape.



What to look for in an incidents, investigations and case management solution

Organizations looking to consolidate incident and investigation processes across the organization need a solution that replaces all the "empty container" solutions, worksheets and file folders with a dynamic, fully-integrated centralized solution – a platform that pulls in data, eliminates manual workflows, and bubbles up intelligence to support enterprise-wide dynamic collaboration.

To ensure your enterprise case management solution is built to meet the emerging needs of your organization, look for a comprehensive, collaborative and converged solution that includes:

END-TO-END INVESTIGATIVE CASE MANAGEMENT

Centralized solution to log incidents, research, collaborate, report and track cases from anywhere in the organization.

CENTRALIZED, PROACTIVE THREAT PLATFORM

Connection to a powerful, cloud-based solution to proactively manage and mitigate threats.

ALWAYS-ON INTELLIGENCE

Continuous access to data sources and integrated tools for automated updates of new information or activities.

INTEGRATED RESEARCH

Always-on, fully-integrated research tools eliminate the need to log into or copy data from other sources.

STREAMLINED COLLABORATION

Anytime, anywhere access to view or update investigation progress with easy cross-functional collaboration tools including embedded chat, task management, notes and reporting.

INCIDENT & INDUSTRY AGNOSTIC

Flexible to any team and any definition of an incident to support the changing needs of any business.

DYNAMIC WORKFLOWS

Support productivity by connecting research data with automated entity, attribute and signal detection to see associations and link analysis. One-click incident to investigative support.

REPORTING

Track resource metrics, timelines and cost details for consistent reporting to leadership. Configurable reports for key investigation results, case status and risk mitigation that can be shared inside and outside the platform (e.g. law enforcement).

CUSTOMIZABLE

Customizable investigation workflow, dashboards and reports make it easy for individuals or teams to track what matters most. Customizable roles, access permissions and layouts help maintain consistent documentation of data collection.

FIELD SUPPORT

Integrate with dispatch providers, assign tasks, log incidents, upload files and leverage a mobile app for field input.

ROBUST METRICS & INSIGHTS

Robust metrics and dashboards to support investigation trends analysis and case visibility. Key metrics include: time to resolution, case load distribution, trends, and cost details. Ability to view data at macro or micro levels.

AUDIT TRAIL

Automated activity tracking to meet compliance requirements.

FLEXIBLE INGESTION

Integrate with any ingestion system - email, HR, tipline, alerting system, CRM, case management

REPORTING

Track resource metrics, timelines and cost details for consistent reporting to leadership. Configurable reports for key investigation results, case status and risk mitigation that can be shared inside and outside the platform (e.g. law enforcement).

ROBUST METRICS & INSIGHTS

Robust metrics and dashboards to support investigation trends analysis and case visibility. Key metrics include: time to resolution, case load distribution, trends, and cost details. Ability to view data at macro or micro levels.

The importance of robust metrics, insights and reporting

Security teams are frequently dealing with budget constraints and demands to “do more with less.” It’s important to clearly articulate the return on investment for tools and personnel, demonstrating outcomes tied to business goals. A platform with a robust metrics and dashboarding engine allows teams to capture, store, and review the cost of each incident. Conversely, for every incident prevented by an intervention, the team can apply a monetary value to the cost savings generated for the organization.

Robust metrics and insights are essential to support incidents, investigations and case management processes. The ideal solution will have both easy-to-use dashboards and the ability to drill down into data to spot incidents and analyze trends, as well as ready-made and exportable reports, making it easy to meet compliance requirements, coordinate with law enforcement, or report on business outcomes.

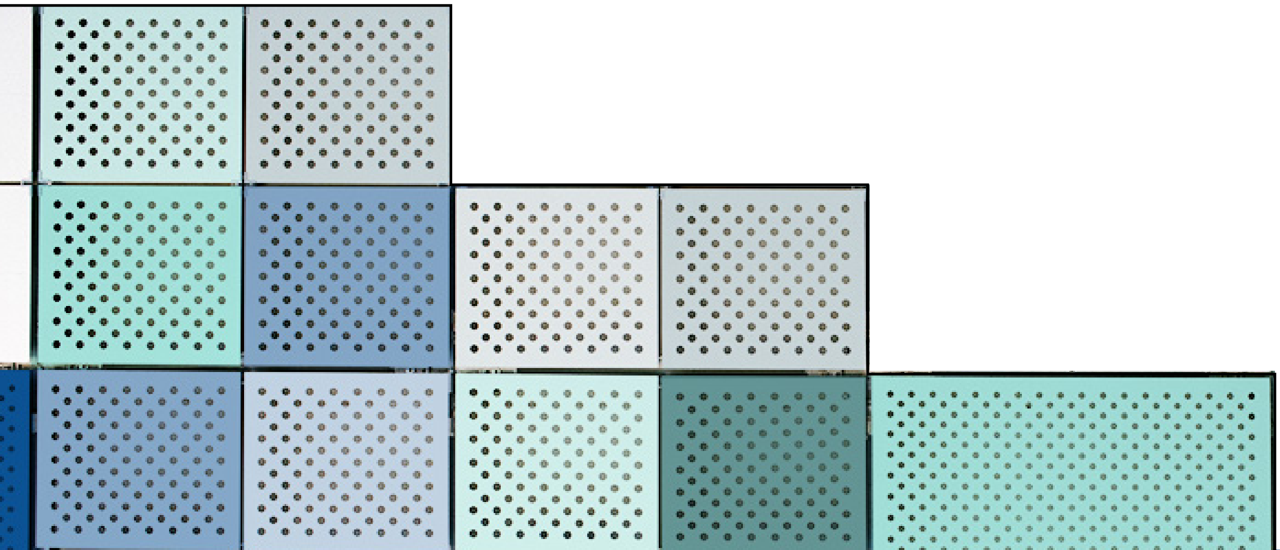
With a central pane of glass and easy report sharing, the solution allows for smarter collaboration throughout the enterprise, enabling teams to share real-time and historical intelligence to better identify pre-incident indicators, assess risk, and mitigate potential threats.

Key takeaways

In the face of growing threats and greater threat complexity, organizations that manage incidents, investigations and cases manually in spreadsheets, on paper or with various point solutions have found it impossible to identify and manage risk effectively.

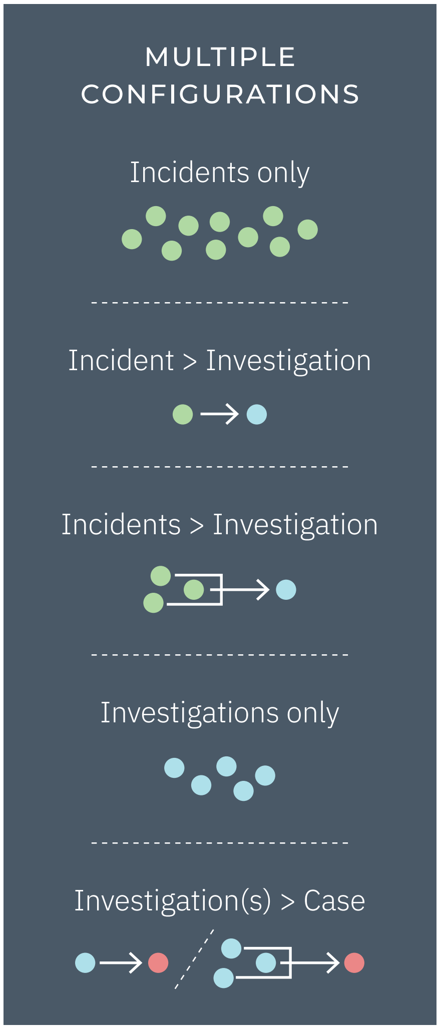
Today’s threats permeate a wider range of areas. That physical harm can be facilitated through cyber means is no longer a question, for example. While physical security, cybersecurity and IT, human resources and legal and compliance leaders will always need and be relied on for their deeper specialized expertise, the heightened threat landscape, technology adoption, and consolidation mean walls are falling with the recognition that data-sharing raises the effectiveness of all.

A platform that provides centralized intelligence has emerged as a strategic priority for organizations in order to better respond to incidents, conduct investigations, assess and prepare for threats.



Ontic's Incidents, Investigations and Case Management solution is the only software solution integrated with an end-to-end threat management platform to support a true comprehensive incident response lifecycle across the organization, providing always-on intelligence designed to support both digital and physical incidents of any kind. With flexible workflows, dynamic research and automated connections and link analysis, organizations can maximize efficiency and respond more effectively. Ontic's always-on platform includes:

- One database to store all research and documentation
- Easy integrations to other systems (CRM, HR tools, VMS, IoT systems)
- Customized access roles to maintain privacy and support compliance requirements
- Automated recording of all actions
- Flexible report dashboards powered by extensive metrics tracking
- Alerts for new information or activity
- Connected threat assessment workflows
- Easily accessible historical case data for always-on tracking and analysis



MULTIPLE CONFIGURATIONS

Incidents only

Incident > Investigation

Incidents > Investigation

Investigations only

Investigation(s) > Case

INCIDENT MANAGEMENT

Flexible intake

Smart matching

Tracking

Metrics & reporting

INVESTIGATIONS & CASE MANAGEMENT

Flexible intake • Tasks

Research • Link analysis

Timeline • Collaboration

Metrics & reporting

> *At this point the Ontic platform acts as a massive force multiplier, allowing me to track and research far more things in a shorter period of time, automating many manual processes while providing a convenient 'one-stop shop' for investigations and research.*
>
> INTELLIGENCE ADVISOR, GLOBAL BIOTECHNOLOGY COMPANY

CLICK HERE FOR MORE INFORMATION ABOUT ONTIC'S INCIDENTS, INVESTIGATIONS AND CASE MANAGEMENT SOLUTION

ONTIC