ONTIC

Whitepaper

Real-Time Threat Detection

Gaining Situational Awareness to Inform Action

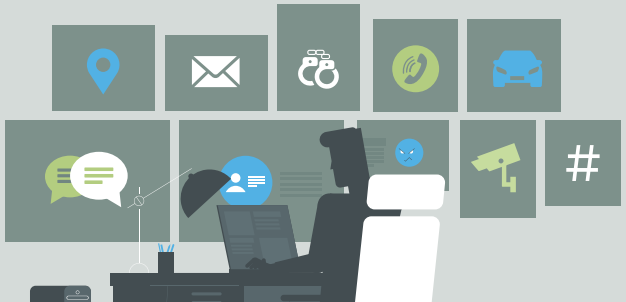
Whether it's the corporate office, business logistics or events, security professionals and leaders are tasked with collecting the right data, and surfacing important signals to understand the conditions of their environment. Success hinges on keeping executives, employees and assets safe.

With new information pouring in each day from sources like Open Source Intelligence (OSINT), Dark Web, weather, real-time news and public events, businesses are seeking situational awareness in their security and operational strategies. There is an increasing need for one view that combines this information with interactive maps, additional research, investigation and assessment tools to surface the signals that matter and keep track of changing situations. It's the difference between **knowing a threat is there** and **knowing how to act.**

Within this whitepaper, we share why a central source is needed to gain situational awareness and take action, specifically:

1. The impact of today's threat landscape
2. The key components to making real-time threat detection a reality
3. How managing threats in real time helps to inform action

You may be using an array of data and technology to observe the landscape and recognize potential risks or threats to people, assets and business operations, but do you have a central source of truth that brings all the information into one view?



Making sense of the threat landscape

Time is everything when it comes to identifying risks. But recognizing signals early is tough when you're sorting through disconnected tools and manually reviewing data. Receiving alerts is not enough — teams have to know what's next and how to best communicate the information to others within the organization who need to know.

It's increasingly rare for teams to be in one place at any given time. The impact of remote work, multiple office locations and travel makes knowing the full context of a threat increasingly difficult. Staying informed in a granular and geo-targeted way across multiple locations helps teams contextualize threats by location and principals/facilities. This geo-specific information includes anything from news to weather alerts to arrest records.

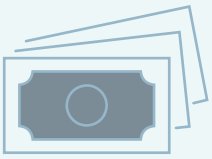
What security teams often realize, albeit too late, is that their work extends far beyond keeping employees safe, and into business continuity, financial liability and reputational impact. A missed signal can lead to acts of workplace violence, supply chain disruption, and a general feeling of uneasiness.

The impact of a missed threat is clear

The financial impact of cyber-physical security attacks resulting in fatal casualties will reach over **$50 billion** by 2023, and **75%** of CEOs will be personally liable for cyber-physical incidents by 2024.[1]

24%

of security leaders report that CEOs and/or their family members working at home and/or traveling received threats or were harmed[2]



The annual cost of workplace violence for employers is

$121B[3]

The average cost of an insider threat incident is over

$11M[4]

1. Gartner
2. 2021 Mid-Year Outlook State of Protective Intelligence Report
3. National Institute for Occupational Safety and Health
4. Ponemon Institute

Making real-time threat detection a reality in your organization

A central destination for your entire security program makes the ability to detect threats in real time a reality. A solution that stores data, collects research and investigates threats gives teams a full picture of the threat landscape and informs action.

Examples of data that are critical to advising decisions include:

REAL-TIME NEWS

Knowing what events are on the horizon and visualizing their proximity to your employees, assets and virtual assets helps teams collaborate and take proactive steps to mitigate impact.

WEATHER AND INTERACTIVE MAPS

Weather conditions can influence consumer activity, supply chain operations and employee safety — especially when travel is on the horizon. Moving people or assets quickly out of harm's way can positively impact business continuity, revenue, and — of course — safety.

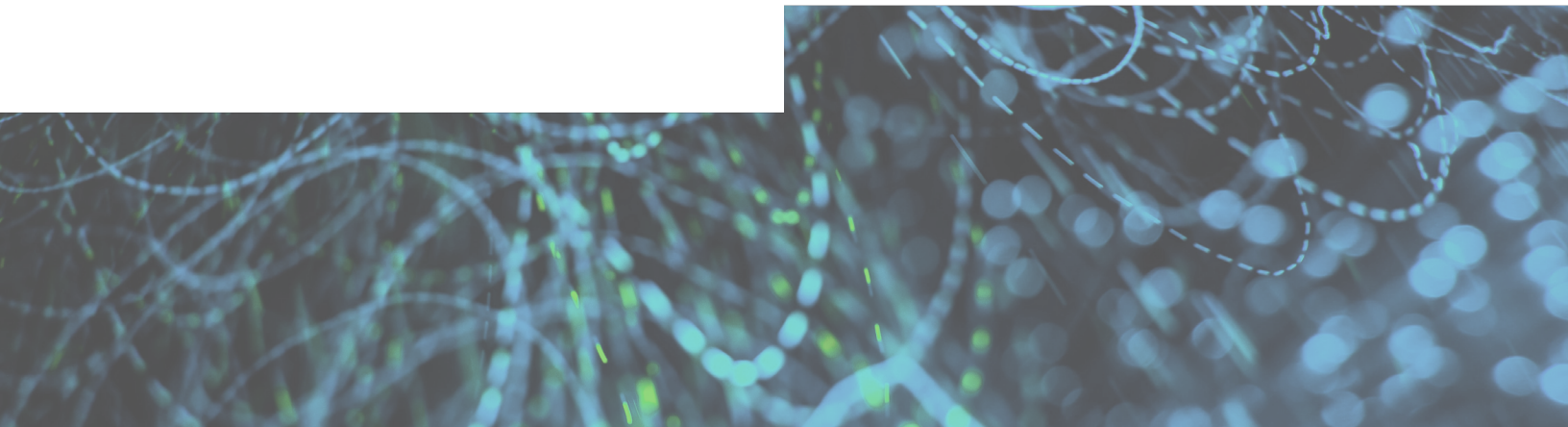
DARK WEB AND SOCIAL MEDIA

Monitoring the global web that is not open to search engines gives teams information that isn't readily available on the surface. Social media can enable quick identification of potential threats and surface anomalies that need to be investigated.

HUMAN INTELLIGENCE AND TECHNOLOGY SYSTEMS

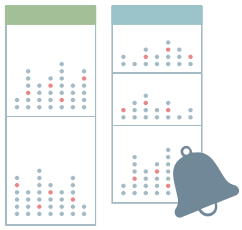
The value of human intelligence and leveraging experience and intuition to make data-driven decisions should not be underestimated. These decisions are based on viewing information from connected devices (cameras and access control systems) for proactive facility protection and internal systems (HR systems, authentication tools).

One or two way communication between systems and tools across the organization helps your team connect the dots using historical and real-time information. A threat is rarely just tied to security, and the more information known about a potential threat creates a more powerful position in today's demanding threat landscape.



Managing threats in real time informs action

Having a centralized view of all available data that impacts your organization, from news to weather to content on the Dark Web, provides teams with the information they need to act. They can effectively detect, understand and take appropriate action. Seeing a clear and complete picture allows them to pick up on patterns or anomalies within the data to investigate further and identify trends over time and by region.



DETECT

See the critical signals through the noise with real-time curation and alerts

UNDERSTAND

Bring together data, people, and processes to verify and develop advanced understanding and context

ACT

Ensure a coordinated response with connected workflows to activate operations and facilitate action

Below are two scenarios of teams using real-time threat intel to inform their actions:

SCENARIO 1: INSIDER THREAT

An insider threat team was able to identify a potential threat actor within the company based on violent media mentions of the organization's leadership by the employee. The team proactively interviewed the employee to understand his intentions and frustrations with leadership, and provided him with mental health assistance.

SCENARIO 2: EXECUTIVE TRAVEL

The executive protection (EP) team of a high-profile individual was able to detect that members of the media have begun tracking the arrival and departure of their Gulfstream Jet. When images and information about the jet (i.e., tail number and location) were posted in online forums, the EP team's intel analyst was able to identify them, notify the team on the ground, and then take measures to decrease the executive's exposure while traveling.

The benefits of an integrated approach

When searching for a way to better surface threats in real time, consider:

SMART DATA FEEDS

Filter to cut through the noise to focus on the critical signals, spending time on what's most important at that moment.

VISUALIZATION

Leverage visualization and maps to see what's happening and contextualize threat information in relation to important people and places.

PAST, PRESENT, FUTURE

Continuously gather real-time data and monitor resources to gain a holistic, connected picture.

One view, possible through the integration of systems that matter to your organization, allows teams to effectively detect threats, putting critical information in the hands of the right people at the right time so they can respond with confidence.

Ontic's Protective Intelligence Platform enables enterprise security teams to see around corners and keep their businesses safe.

Learn More

Let's make nothing happen together™

Named the top industry innovator in the Frost Radar™: Digital Intelligence Solutions, 2021, Ontic is the first protective intelligence software company to transform how Fortune 500 and emerging enterprises address physical threat management to protect employees, customers and assets. Ontic's SaaS-based platform collects and connects threat indicators to provide a comprehensive view of potential threats while surfacing critical knowledge so companies can assess and action more to maintain business continuity and reduce financial impact.

Ontic provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals through its Center for Protective Intelligence and Center of Excellence, the latter of which also offers program development and training services in behavioral threat assessment, threat management, and violence prevention for major corporations, educational institutions and government agencies.

For more information please visit ontic.co or follow us on Twitter @ontic_co

ONTIC®