Resolver.
A KROLL BUSINESS

The Four Pillars of Successful Threat Protection Programs

Presented by Resolver

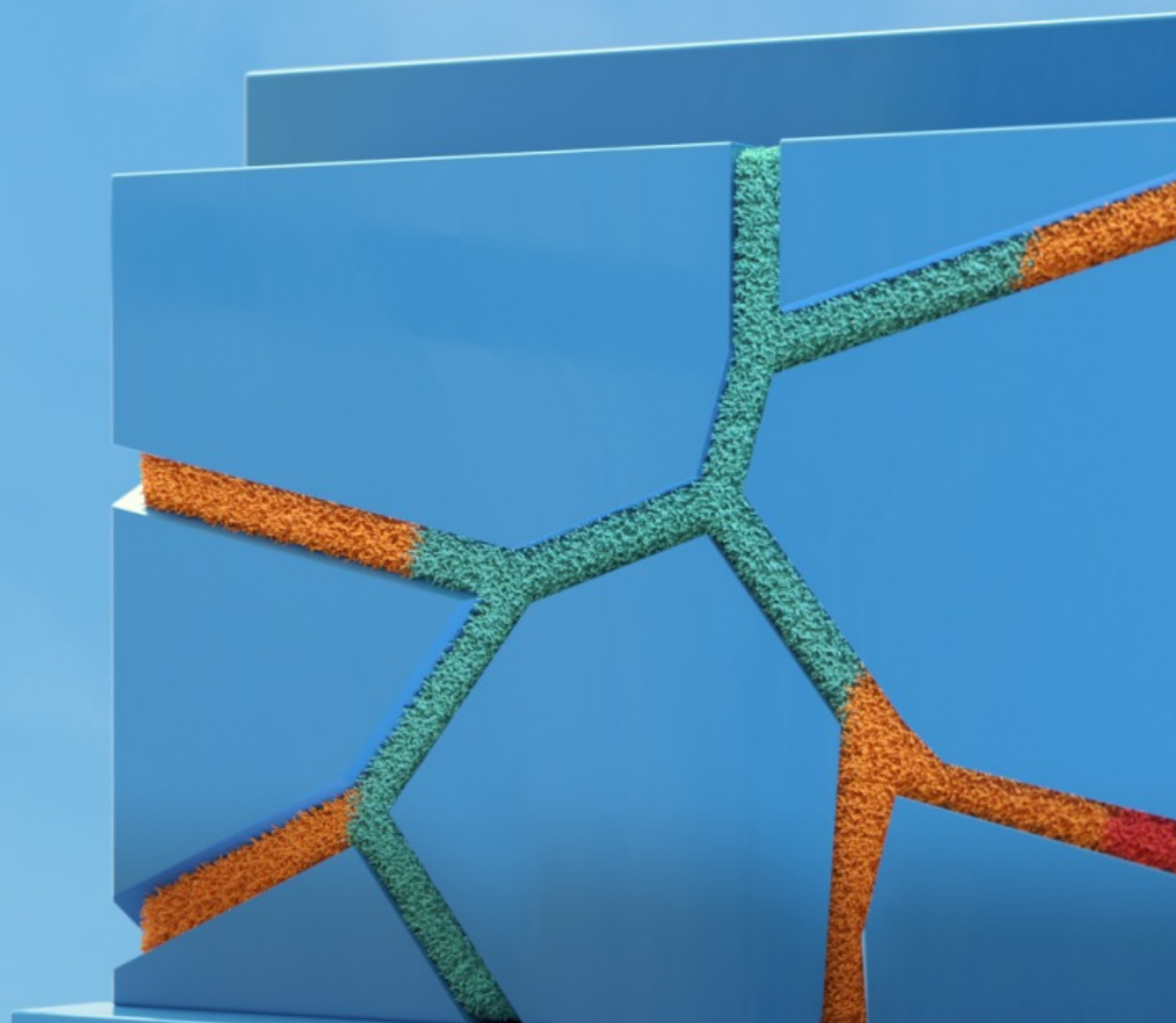
About Resolver

Resolver is an end-to-end security platform.

We enhance and integrate our client's threat, security risk, incident management, and security operations capabilities to help them ensure the protection of their organization.

Whether you're using one of our applications or the entire suite, with Resolver your team will have better information, operate more efficiently, and be able reduce the frequency and severity of incidents.

And with our platforms advanced analytics and reporting capabilities, you'll be able to prove that impact to the rest of the organization.



Agenda

- **Why Invest in Threat Protection?**
- **The Four Pillars of Successful Threat Protection Programs**
  - **Threat Detection**
    - Inventory your assets and threat landscape
    - Match and refine
    - Identify feeds and sources to use
  - **Triage**
    - Consolidate and enrich data
    - Develop a Tirage process
  - **Investigation & Assessment**
    - Investigations
    - Assessments
  - **Response & Mitigation**
    - Immediate response
    - Long-term mitigation
    - Reporting

Why Invest in Threat Protection?

Duty of Care

In 2021, 58% of CEOs received physical threats after taking a position on a racial or political issue. **– 2022 Protective Intel Report**

In 2021, workplace violence cost U.S. businesses up to 330 billion.

– U.S. Department of Labor

Fewer Incidents

“In 2021, 51% of incidents that interrupted business operations and/or harmed employees could have been prevented if an integrated threat program was in place.”

– 2022 Protective Intel Report

Today’s Climate

“In the coming months, we expect the threat environment to become more dynamic… threat actors have recently mobilized to violence due to factors such as personal grievances, reactions to current events, and adherence to violent extremist ideologies.”

– U.S. Department of Homeland Security, June 2022.

Less Harmful Incidents

In 2021, insider threats identified within 30-days cost an average of $11.2M. Those that went undiscovered for over 90-days cost an average of $17.2M

– 2022 Ponemon Cost of Insider Threats Global Report

The Four Pillars of Successful Threat Protection Programs

01

Threat Detection

02

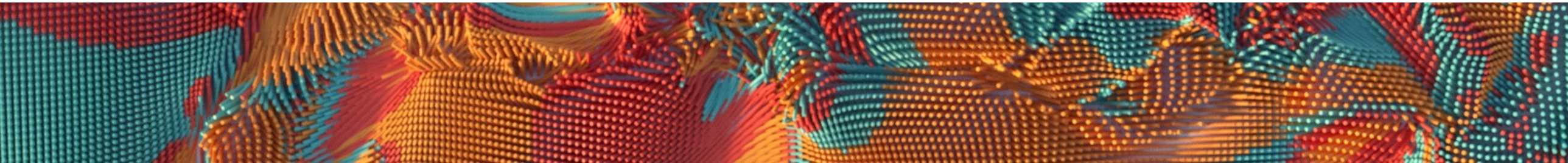
Triage

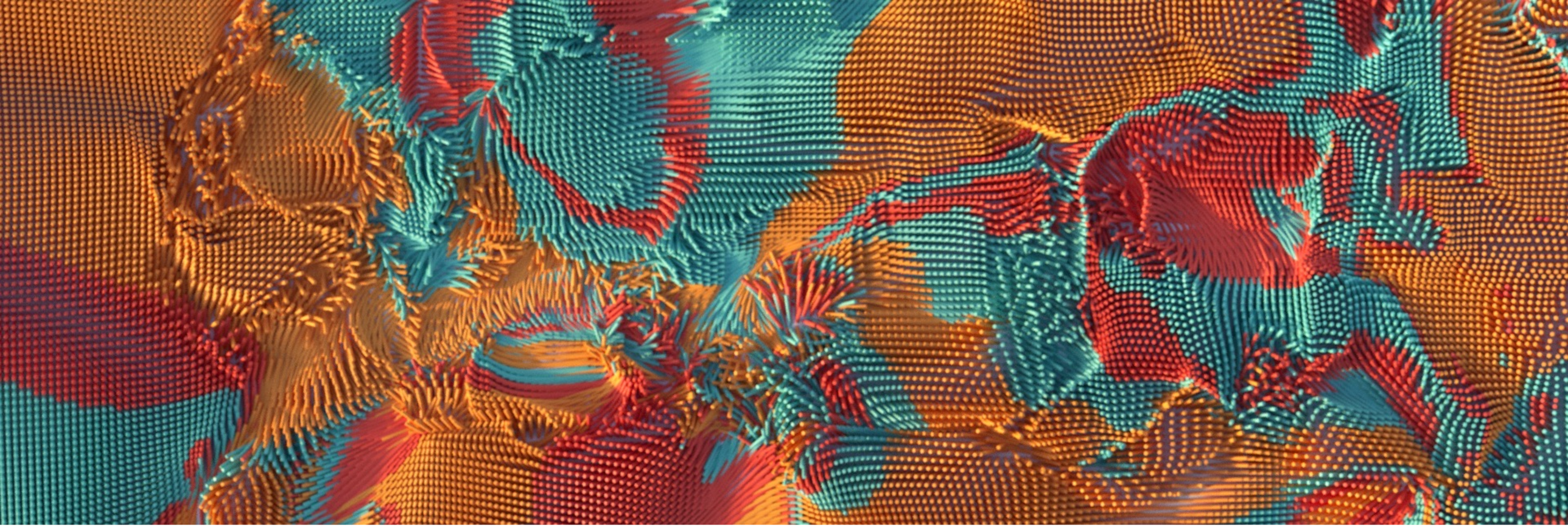
03

Investigation & Assessment

04

Response & Mitigation





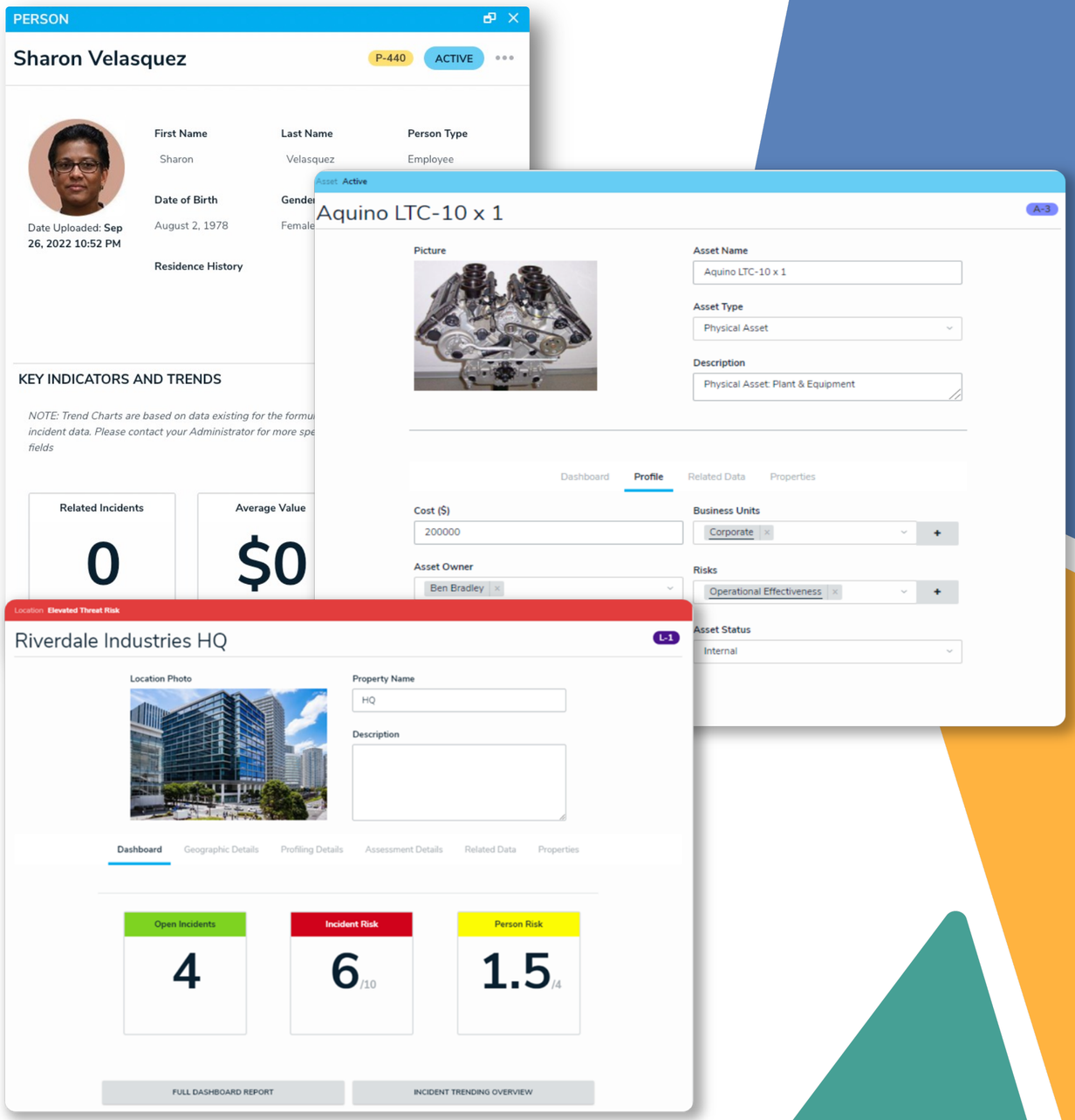
Pillar

01

Threat Detection

Inventory your assets

- **Critical people with exposure**
  - Typically executive team and ambassadors with public-facing responsibilities and presence
  - Closely tied partners
  - Others at high risk
- **Physical locations**
  - Offices
  - Distribution centers
  - IT infrastructure
  - Critical partner facilities
- **Intellectual property, brands, products**
- **Online presence**
- **Other**

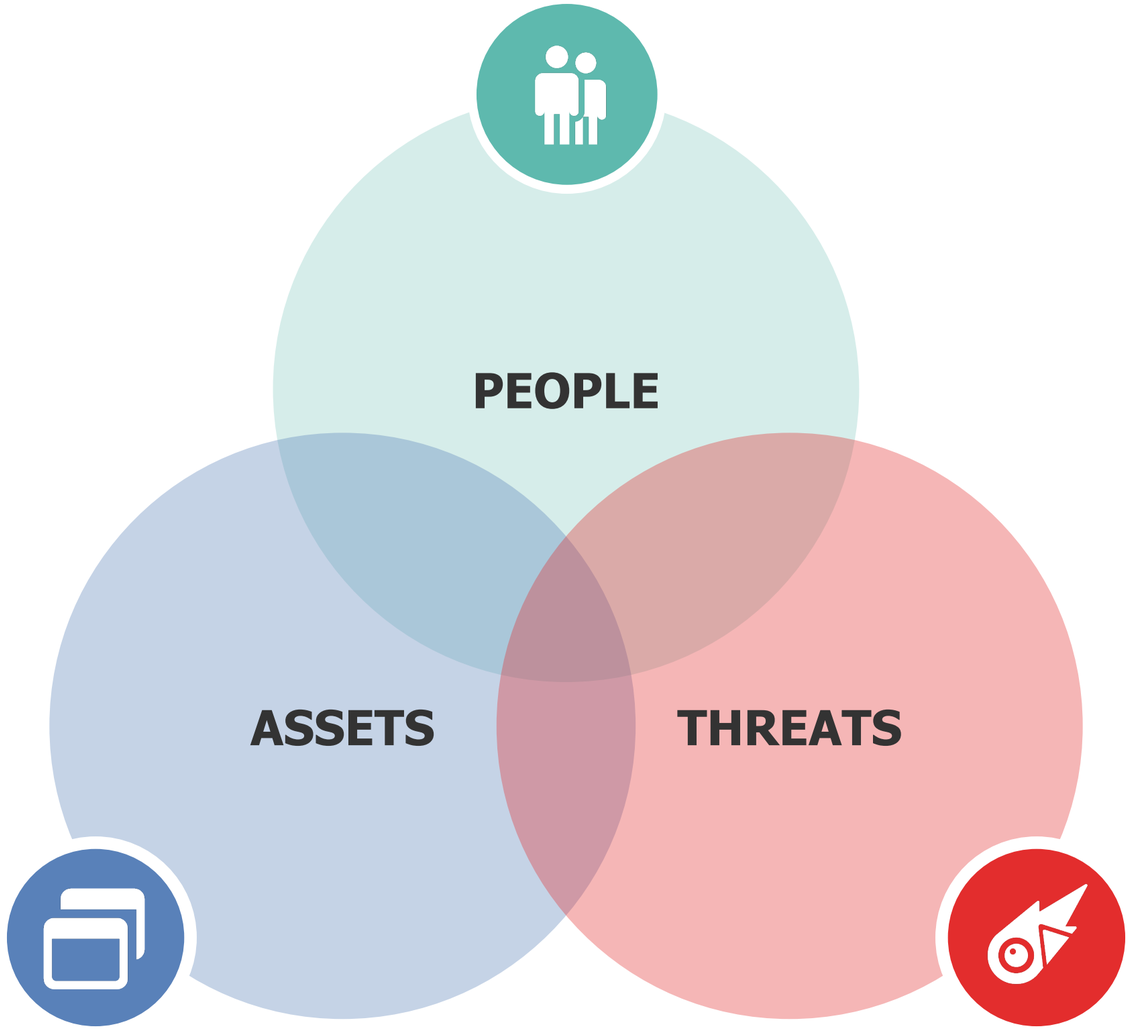


Inventory your threat landscape

- **Reflect on past events**
- **Benchmark to your segment and industry**
- **Actively research OSINT**
- **Curate your topics**
  - Physical / Violence
  - Protest
  - Business disruptions
  - Cyber
  - Doxxing
  - Impersonations
  - And more
- **Track your knowns up-front**
  - Special interest groups
  - Disgruntled employees
  - Prior threat actors

Match and refine

- Don't make the mistake of monitoring everyone and every asset for every threat
- Be precise in how you classify your assets and threat landscape (a brand is unlikely to get stabbed, but a person might be)
- Recognize that this rubric is a fluid concept that evolves with time, events, financial results, product launches, executive statements, etc.
- You don't need to do this by yourself – (hire consultants)



Online Sources

Online Monitoring

Tools and services that monitor the online space, social media, forums, deep web, and dark web for threats relevant to your people, buildings, brands, and products.

Facebook Groups

An event planned with 200 registrants to protest at your Headquarters on a specific date and time. Lots of incitement to cause some property damage and disrupt business operations.

Scenario

The business has time to react and plan, collaborate with local law enforcement, set up a safe environment to receive a protest, take action to prevent it from occurring on their property or deny effect by closing the office that day.

Internal Sources

Internal Systems

Access control, video analytics, data loss prevention, user, and endpoint monitoring systems that generate alerts for insider threats.

Access Control Alert

Exception alert of an employee frequently accessing the office after hours, which is out of pattern.

Scenario

Organization is able to review patterns and determine whether an investigation is necessary into the activity of the employee. This could be a warning sign for theft or espionage activity.

Human Sources

Human Reporting

Employees, contractors, vendors, customers, and members of the public report insider threat concerns through a portal or confidential hotline.

Web Portal Alert

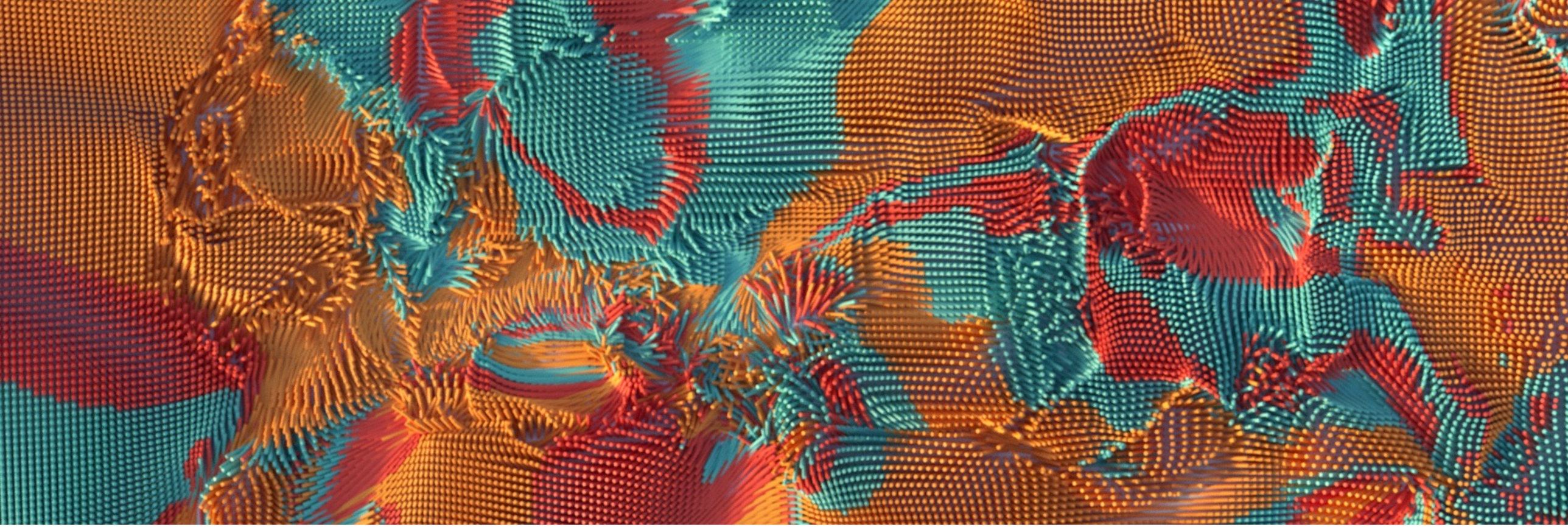
Employee submits a complaint through an anonymous portal that they've observed a manager threaten to harm their direct reports physically on several occasions.

Scenario

Business can assess and investigate the allegation, initiate a response in line with their policy, and act quickly to stop workplace harassment.

Poll: What systems do you **actively** collect threat intel from today? Select all that apply.

- Open source intelligence (social media, deep & dark web, forums)
- Internal systems (access control, video analytics, endpoint monitoring systems)
- Human reporting (employees, contractors, vendors, members of the public)



Pillar

02

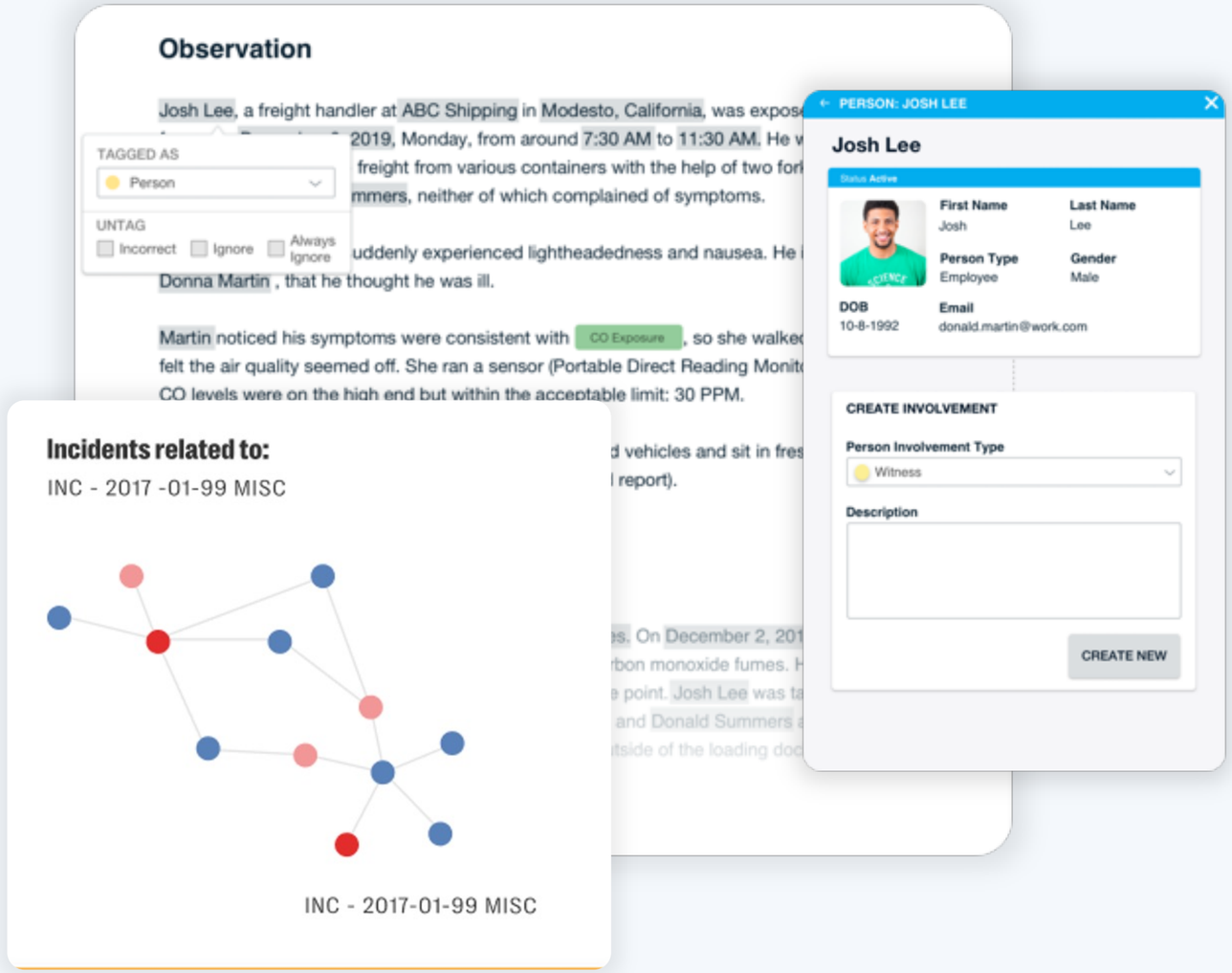
Triage

Consolidating and enriching your intel

One piece of intel rarely tells the whole story. Consolidate data from online monitoring, internal systems, and human reporting.

Data tagging and classification. Properly tagging and classifying your threat intel sets the stage for analysis.

Data linking and contextualization. Leveraging software to find links between previously siloed threat intel is critical for fast and accurate triage.



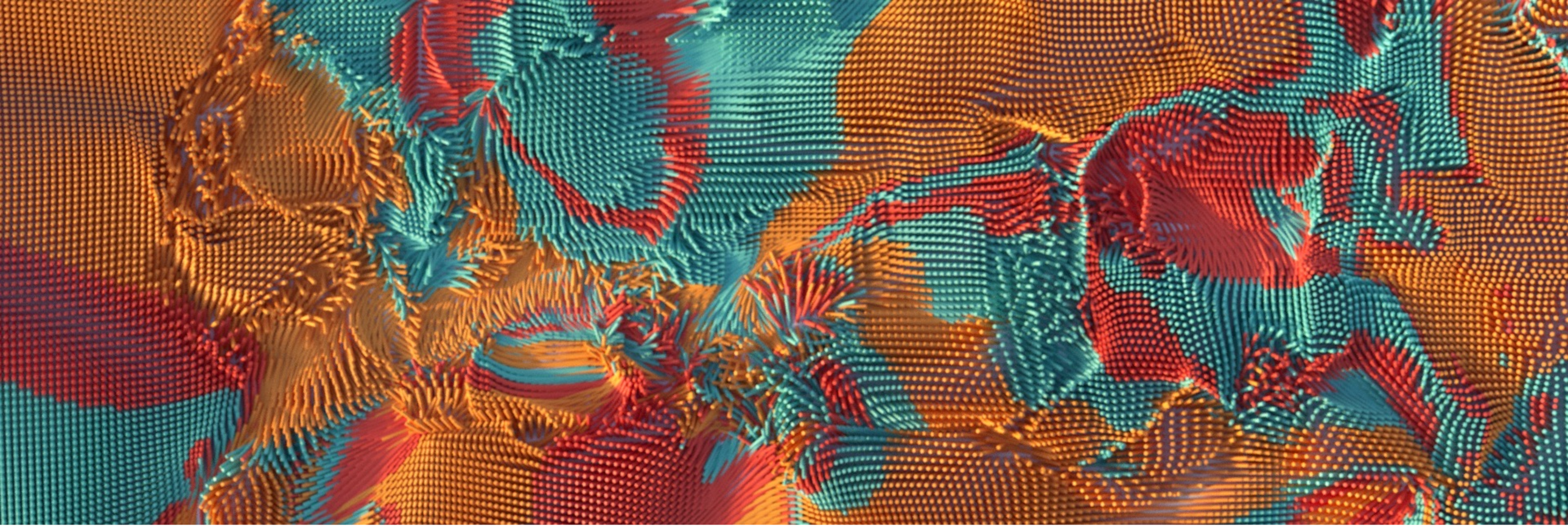
Building your triage process & training your investigators

Building A Reliable Triage Process

- Set clear standards for initial triage investigation
- Create standardized rubrics to triage decisions
- Document standard routing procedures and workflows
- Automate notifications and progress tracking
- Periodically review triage decisions to drive accountability and find opportunities for continuous learning

Training Investigators

- Is it specific?
  - Is a person, location, or time mentioned?
  - Is a method of action described?
- Do they have the means?
  - Can they plausibly execute on the threat they describe?
- Are there connections to prior threats, known actor groups, or open cases?
- Consider the broader social context



Pillar
03

Investigation & Assessment

Threat Investigations

Go Wide

Expand your investigation to gain the broadest understanding, assess a complete timeline, and maximize context:

- Look into broader activity of a person, profile, or account
- Identify relationships to groups and other actors
- Expand on the threat topic in the context of your business

Dig Deep

Focus intensely on the important points of interest:

- Identify the actors
- Dig into each actor and group
- Dig into agendas
- Aim for quality evidence-level data
- Document and track in detail

Real-life Threat Investigations

Initial Alert

Alert from OSINT monitoring tool received, due to combination of company location + violent language on Twitter.

Triage

Triage quickly determines that this is critical; a named target, a promise to **"smash her head in"** with a heavy object, and an imminent timeline **"next time I see her"**

Escalation

Immediate escalations and notifications occur to the investigative team and management.

Initial Investigation – Actor & Target

- Rapid background on the threat maker profile determines the high likelihood of being an employee at a company location.
- Threat target mentioned by first name, and is determined to likely be another employee at the same location.

First Response

Immediate response initiated, per playbook.

Deeper Investigation

Deeper investigation, interviews, and assessments are conducted with appropriate outcomes.

Real-life Threat Investigations

Initial Alert

Tip submitted to a Facebook group, planning to disrupt business operations.

Triage

Triage quickly determines that this is significant; the group had a strong agenda with many followers and was planning to target multiple company locations over a period of time.

Investigation

Rapid investigation determines a rough schedule, possible locations and a list of organizers.

Investigation Continued

Comprehensive investigation into the group's activity, past protests, and members uncover a profile to work with.

Investigation Continued

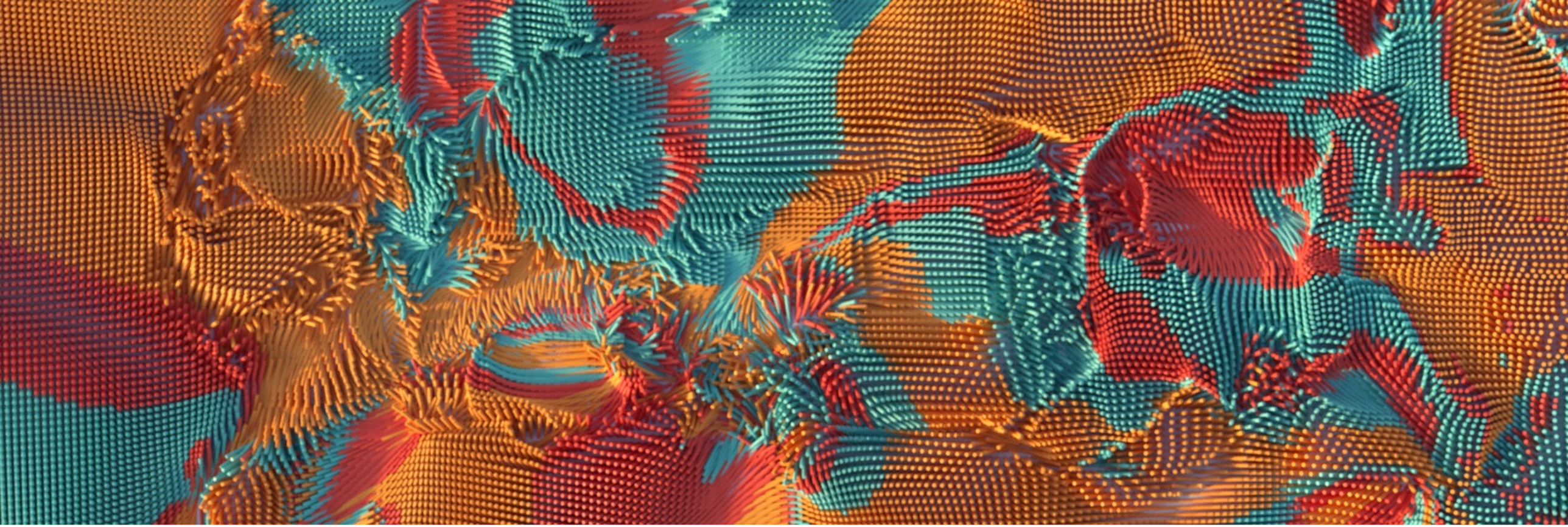
A deep investigation into organizers allows you to profile each one and provide proactive alerts / BOLOs to our sites with photos, vehicles, etc.

Response

Immediate response involves active monitoring of group, internal communications and training to prepare for protest activity and consultations with law enforcement.

Developing a reliable assessment process

- **Have a consistent methodology for assessing common threat types**
  - RAGE-V
  - WAVR-21
  - MOSAIC
- **Document your decision making**
  - Learn from successful mitigations
  - Protect from litigation when things go poorly
- **It's rarely one and done**



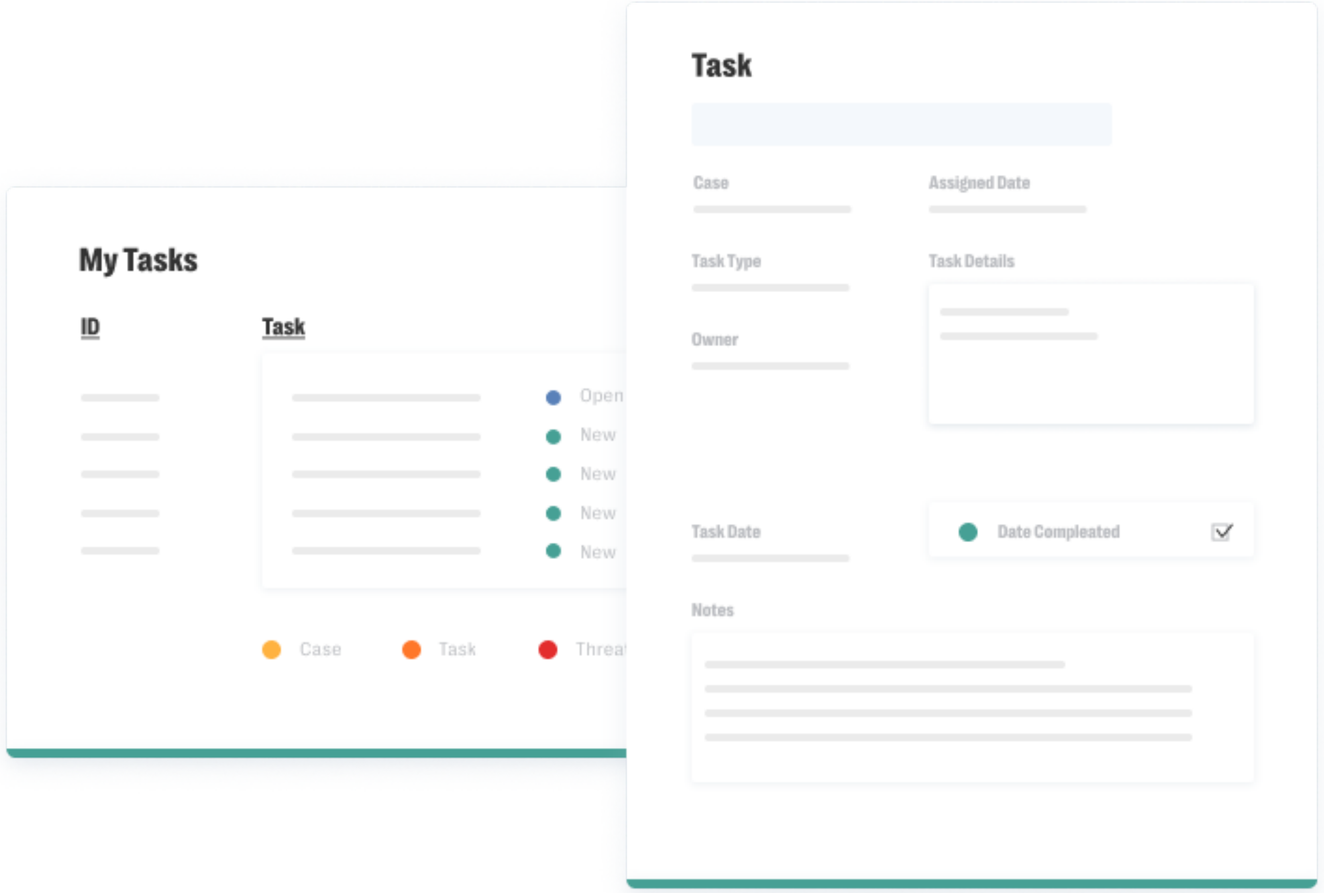
Pillar
04

Response & Mitigation

Immediate response

The set of actions you can take as soon as you have just enough information to .

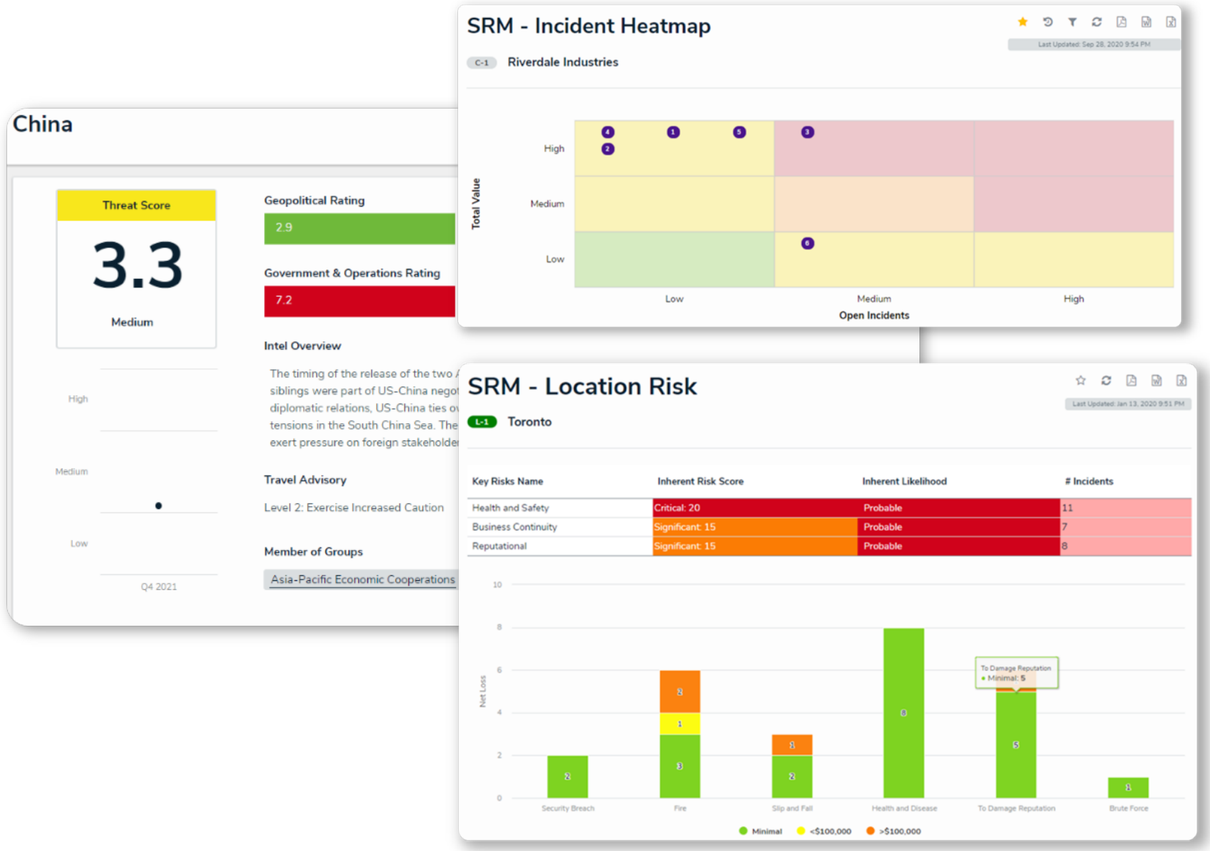
- Develop a playbook to reduce ambiguity and inaction
- This is a reactive component, where the aim is to be able to be quick, efficient, and impactful in the early stages
- Often includes short-term changes in security posture, opportunity denial, law enforcement support



Long-term mitigation

The strategic controls you implement, informed by trends and patterns over time that aim to reduce exposure and impact.

- Capturing good data over time is crucial in doing this well
- Keep track of changes and measure impacts through your data, such as reduction in incidents, the severity of incidents, improved detection, faster responses, etc.
- These are often program-level changes, such as implementing training programs for staff, policy changes, new and/or improved processes, etc.



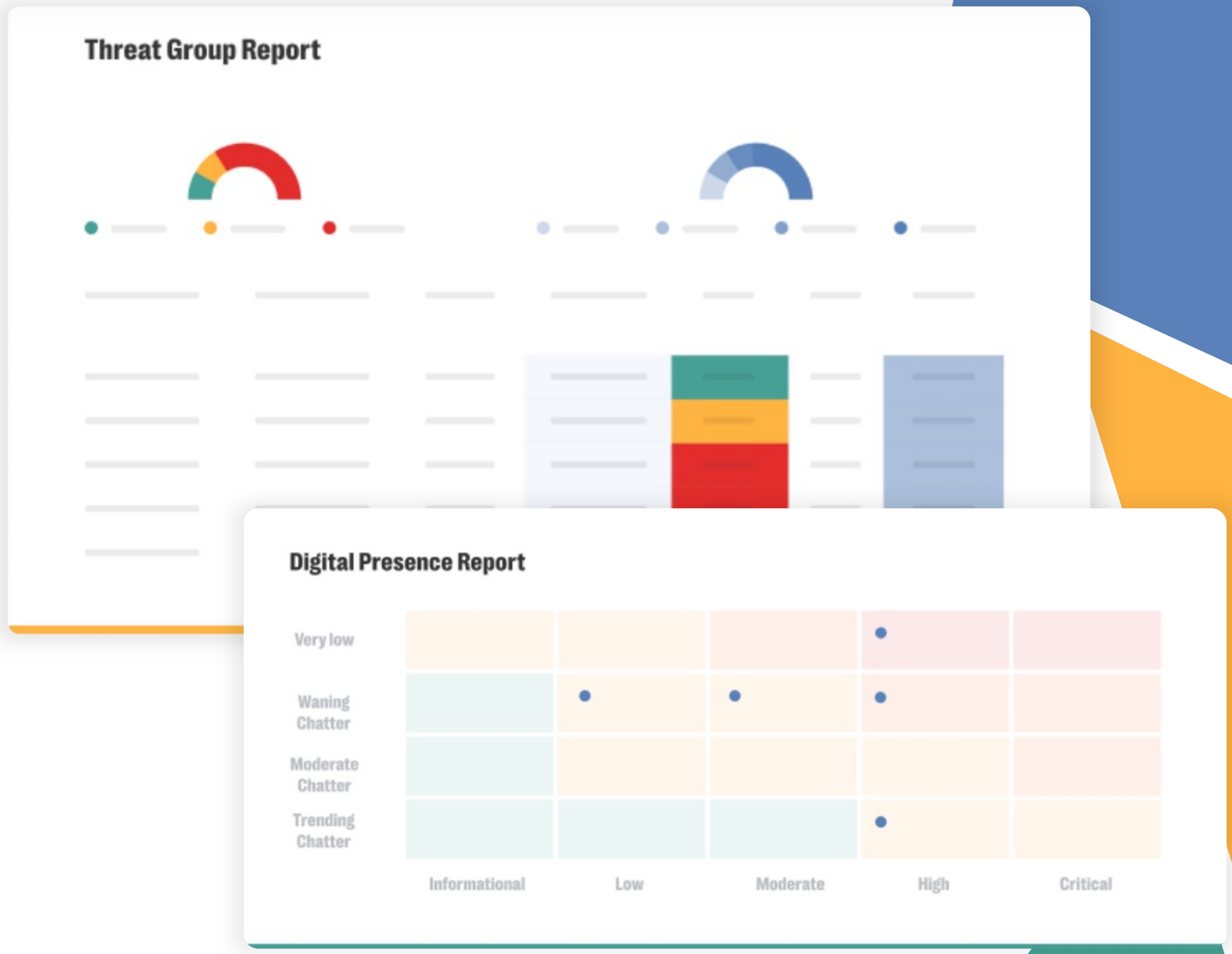
Operational and strategic reporting

Key Operational Reports:

- Threats in progress (triage queue, open)
- Short-term threat volume trend (week-over-week)
- Open cases
- Action plans status

Strategic Reports:

- Threats by month / year (with severity)
- Threats by type and category
- Threats against asset type & asset
- Threat performance measures



Top Threat Protection Challenges + Resolver's Solution

Top challenges we hear from our prospects

- **Connecting siloed threat intel:** Managing siloed threat intelligence from multiple sources and systems is cumbersome and fragmented.
- **Understanding threat actors:** The ability to rapidly assess and paint a thorough picture of threat actors is an essential capability, but teams find the process time-consuming and error prone.
- **Completing threat investigations:** To accurately assess threats, a comprehensive investigation is needed. But many teams lack the tools to ensure consistent high-quality investigations.
- **Driving threat mitigation:** If threat intelligence does not materialize into risk reduction, the whole program fails. But many threat teams struggle to ensure the right steps are taken after a threat is identified.

Our Promise

Connecting siloed threat intel: Managing siloed threat intelligence from multiple sources and systems is cumbersome and fragmented.

Understanding threat actors: The ability to rapidly assess and paint a thorough picture of threat actors is an essential capability, but teams find the process time consuming and error prone.

Completing threat investigations: To accurately assess threats, a comprehensive investigation is needed. But many teams lack the tools to ensure consistent high-quality investigations.

Driving threat mitigation: If threat intelligence does not materialize into risk reduction, the whole program fails. But many threat teams struggle to ensure the right steps are taken after a threat is identified.

Integrated threat intelligence

Robust threat actor profiles

Stronger investigations

Greater impact

Resolver’s Threat Protection Capabilities

Threat Intel Collection

- OSINT
- Reporting & Comms Systems
- Dark & Deep Web
- Entry & Exception Reporting Systems

Triage

- Data Tagging
- Automated Alerts & Workflows

Investigation

- Link analysis
- PoI Enrichment
- Evidence management
- Built-in best practice workflows & guidance
- Fully configurable

Threat Scoring

- Pre-built methodologies
- Assess threats
- Contextually determine risk
- Automate notifications and workflows

Act & Report

- Orchestrate your end-to-end response
- Track progress
- Report on outcomes

Whatever your needs, Resolver has a solution.

Workflow Automation

Process Automation

Data Warehousing

Integrations

Analytics

Automated Reporting

Resolver.
A KROLL BUSINESS

Want to learn more? Let’s talk.

BOOK A DEMO

1 (888) 316-6747 | See risk. Discover value.