USE CASE

Incident Response

CAVELO

Incident response is a playbook and process that businesses follow to manage a cyber incident or data breach. It's the first step to incident recovery. But like many cybersecurity functions, incident response capabilities vary widely depending on how established a business is and its level of security maturity.

THE CHALLENGE

Large enterprises with ample resources have well-staffed teams that monitor and react to cyber incidents. Team members specialize in the operations, legal and communications functions businesses need to react and handle incidents from incident discovery to public disclosure. Unlike large enterprises, midsize companies lack a dedicated budget, staff and in many cases, the foundational processes required to respond to cyber incidents. As a result, they're often caught off guard when an incident happens and struggle to respond, or resort to external support, losing precious time.

Cyber incidents happen on a regular basis and target businesses large and small. All companies need an incident response plan in place to be able to respond to incidents as they happen, limit damage and minimize downtime.

Risks of limited or non-existent incident response capabilities:

- Regulatory Non-compliance
- Reputational Risk
- Legal Action
- Data Loss
- System Downtime
- Lost Production Time
- Costly Data Recovery Fines
- Financial Losses Due to Ransoms

 | info@cavelo.com | www.cavelo.com

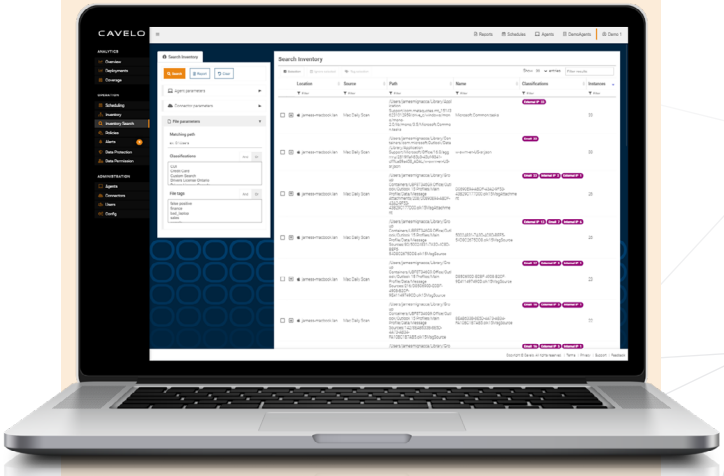
Let the Cavelo platform support your incident response program.

Here's how:

1. Understand where your sensitive data lives on the network, how it's protected, where it's been used and who has access to it.

2. Respond faster when an asset goes missing or has been compromised by getting the insights you need into the asset in question, the data it contains and who accessed it.

3. Leverage real data to make critical and time-sensitive response and remediation decisions.



THE SOLUTION

Traditional incident response is a reactive process to repair any damage caused by a cyber incident. All of the processes, tools and technology used in incident response plans are designed to identify what happened and what data was compromised. The proliferation of data across company networks makes it harder for businesses to understand what data types they have, who has access to data and how their data is used. Without an accurate data inventory identifying whether data was accessed or compromised can be a frustrating and drawn-out process.

All businesses need to adopt a proactive approach to incident response that starts by discovering, classifying and tracking sensitive data that's used and stored within the organization. Ensuring an up-to-date data inventory supports:

- ✓ The creation of an incident response plan that's specific to your organization, its data types, unique regulatory drivers and reporting requirements
- ✓ Ongoing reporting requirements
- ✓ Full visibility and an accurate inventory of sensitive data within the organization
- ✓ Confidence in your team's ability to respond to and manage cyber incidents
- ✓ In-house or third-party forensics investigations
- ✓ Faster time to event mitigation
- ✓ Reputation management

LEARN MORE