A Five-Stage Guide to Incident Response For Modern Organizations

Most organizations will face a serious security incident. Many will not see it coming.

Security teams often learn about incidents late. Sometimes from customers. Sometimes from law enforcement. In ransomware cases, the first signal may be locked systems and a demand message. When that happens, teams are under pressure to act fast, often without enough context.

The Verizon 2025 Data Breach Investigations Report analyzed more than 22,000 security incidents and 12,195 confirmed breaches across 139 countries. Credential abuse remained the most common initial access vector, used in 22% of breaches. Exploited vulnerabilities followed closely at 20%, up 34% year over year. Ransomware appeared in 44% of breaches, and 30% involved a third party.

Without a documented incident response plan, teams risk shutting down the wrong systems, losing forensic evidence, or delaying required notifications. Each of those mistakes increases business impact.

An incident response plan gives security operations teams a repeatable way to detect, investigate, contain, and recover from incidents while protecting the business.

Business Impact at a Glance

According to the IBM Cost of a Data Breach Report 2025:

- The global average cost of a data breach is $4.44 million.
- The average breach lifecycle is 241 days from identification through containment.

Faster detection and response directly reduce disruption, investigation time, and downstream cost.

$4.44M	241 days
Average Cost of a Data Breach	Average Time to Identify and Contain a Breach

What Is an Incident Response Plan?

Incident response is a structured approach to handling security incidents and confirmed breaches.

An incident response plan is a living document. It defines:

- How incidents are identified and prioritized
- Who is responsible for each response step
- How evidence is preserved
- When and how stakeholders are notified
- How systems are restored and risk is reduced

A strong plan helps teams:

- Understand incident scope sooner
- Limit operational disruption
- Coordinate security, legal, and communications teams
- Restore systems safely
- Apply lessons learned to prevent repeat incidents

Frameworks such as NIST SP 800-61 provide useful guidance, but every organization must tailor its plan to its environment, data, and tolerance.

Event, Incident, or Breach?

Clear definitions prevent overreaction and missed reporting obligations.

- **Event:** An observable change in a system, user, or network. Many events are benign. Some require investigation.
- **Incident:** A security event that threatens confidentiality, integrity, or availability.
- **Breach:** A confirmed incident where data exposure has occurred.

Not every incident becomes a breach. Not every breach requires public disclosure. Your incident response plan should clearly define:

- When legal counsel is engaged
- Who approves notifications
- Which laws and regulations apply by region

The Five Stages of a Comprehensive Incident Response Plan

Figure 1.

A structured incident response lifecycle helps security operations teams prepare for incidents, identify and investigate threats, contain active risk, communicate effectively, and restore systems while reducing business impact.

1. Prepare

Preparation determines response quality.

Key actions include:

- Assembling a cross-functional incident response team
- Defining escalation paths and decision authority
- Prioritizing critical systems and data
- Documenting contact details and communication workflows
- Running tabletop and red-team exercises

Behavioral baselines matter. Knowing what "normal" looks like for users, service accounts, and systems makes deviations easier to detect.

2. Detect and Analyze

Incidents surface through people, alerts, logs, and third parties.

Security teams analyze:

- Authentication activity
- Endpoint and network signals
- Cloud and application logs
- User and service account behavior

Credential abuse continues to drive breaches. In the 2025 DBIR, stolen or misused credentials were the initial access vector in 22% of confirmed breaches.

Behavioral analytics and risk-based investigation help teams understand:

- Scope
- Attack paths
- Techniques used
- Assets at risk

Correlating activity across identities, devices, and time allows teams to move from alerts to understanding.

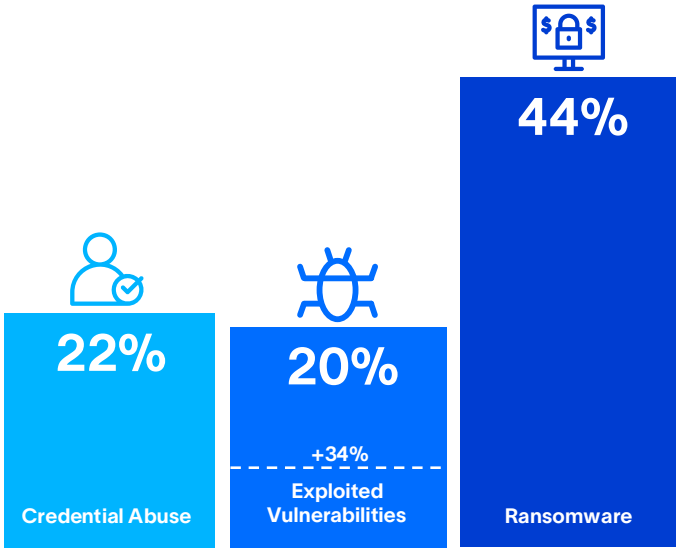

Figure 2.

Credential abuse (22%) and exploited vulnerabilities (20%) were the most common initial access vectors in confirmed breaches. Exploited vulnerabilities increased 34% year over year as an initial access method in the 2025 DBIR.

3. Contain and Eradicate

Containment limits damage while preserving evidence.

Actions may include:

- Isolating affected systems
- Disabling compromised accounts
- Blocking malicious activity
- Preserving forensic artifacts
- Removing persistence mechanisms

Overreaction causes unnecessary downtime. Underreaction allows spread. A documented plan keeps responses measured and repeatable.

4. Respond

Response extends beyond technology.

Teams coordinate with:

- Legal and compliance
- Communications and public relations
- Executives
- Customers and partners
- Law enforcement when required

Preapproved messaging and notification workflows reduce delays and prevent inconsistent statements under pressure.

5. Recover

Recovery confirms the incident is resolved and reduces future risk.

Key steps include:

- Validating systems before returning them to production
- Completing root cause analysis
- Closing gaps that enabled the incident
- Updating the incident response plan
- Training teams based on lessons learned

Failure to complete recovery work leaves organizations exposed to repeat incidents.

Why You Need an Incident Response Plan Today and Tomorrow

Incidents are inevitable. Disorder is not.

The Cost of a Data Breach Report shows that faster identification and containment reduce breach costs and disruption. The report also recommends regularly testing incident response plans, defining clear roles, and running crisis simulations to improve outcomes.

Your incident response plan must evolve as environments, threats, and teams change. Annual reviews and post-incident updates keep it effective.

How Exabeam Helps Security Operations Teams Apply These Findings

Findings from the 2025 Verizon and IBM reports point to a consistent theme: most breaches begin with compromised identities, exploited system behavior, or a combination of both.

Exabeam helps security operations teams apply these findings by focusing on how users, service accounts, and automated agents behave over time. Behavioral analytics establishes a baseline of normal activity, then surfaces meaningful deviations tied to credential misuse, unusual access patterns, and lateral movement.

This identity-centric approach extends beyond human users. As organizations adopt automation and AI agents that authenticate, access systems, and act on behalf of users, those non-human identities require the same level of monitoring and context. Exabeam supports visibility across human and non-human identities so security teams can detect risky behavior early and investigate incidents faster.

By prioritizing activity based on risk and context, security teams can focus their time on higher-risk behavior, reduce investigation effort, and limit the impact of security incidents.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

exabeam™

Learn more at
www.exabeam.com →