Frontiers in Emerging Engineering & Technologies (Open Access)

Volume 02, Issue 11, November 2025,
DOI: - https://doi.org/10.64917/feet/Volume02Issue11-01 PageNo.01-06

Rapid Incident Response and Digital Forensics at Scale: A Comprehensive Framework for Enterprise Cyber Resilience

Bhumit Dhandhukiya
Security Operations Analyst Propel Holdings, Toronto, Ontario, Canada

RECEIVED - 10-08-2025, **RECEIVED REVISED VERSION** - 10-26-2025, **ACCEPTED**- 10-28-2025, **PUBLISHED**- 11-01-2025

Abstract
Large, distributed IT environments make incident response (IR) and digital forensics difficult due to alert volume, heterogeneous infrastructure, and data scale. This paper presents a conceptual framework that integrates Security Orchestration, Automation and Response (SOAR) and scalable forensic pipelines to accelerate containment while maintaining evidentiary rigor. The approach synthesizes standards and practice, illustrates automation with Extended Detection and Response (XDR) play- books, and describes distributed evidence collection and timeline analysis suitable for thousands of endpoints. The framework highlights team roles, communication patterns, and metrics that organizations can use to realize measurable improvements in response speed and analysis throughput.

Keywords: Incident response, digital forensics, SOAR, XDR, CSIRT, SOC, automation, cyber resilience, cloud forensics, DFIR

1. Introduction

A swift and coordinated response is essential to minimize damage during cyber incidents in large enterprises [1]– [3]. However, IR at scale faces persistent challenges: high alert volumes, complex hybrid infrastructure, unclear cross-team processes, skill gaps, and vast forensic data sets [4]– [7].

Research Gap. While widely adopted guidance (e.g., NIST SP 800–61) specifies IR phases, previous work rarely operationalizes (i) the end-to-end integration of SOAR-based automation with IR processes and (ii) scalable, enterprise-wide forensic pipelines that span on-premises and cloud systems with repeatable performance guarantees. Academic studies discuss the need for scalable forensic methods and cloud evidence acquisition, but do not consolidate these elements into a single deployable framework for large enterprises [7], [25], [26].

Contribution. This paper demonstrates a unified framework that: (1) translates IR phases into automated playbooks in SOAR/XDR; (2) specifies distributed collection and big-data timeline analysis for digital forensics at scale; and (3) defines the roles of the Computer Security Incident Response Team (CSIRT), the collaboration of the Security Operations Center (SOC) and metrics for continuous improvement.

2. Methodology

Nature of the Research. This work is a conceptual synthesis and prescriptive framework, derived from recognized standards (e.g., NIST), authoritative playbooks (e.g., CISA) and documented practices from SOAR/XDR deployments and open-source digital forensics and incident response (DFIR) tools [2], [3], [8]–[11], [14]–[17], [23], [24].

Scope and Validation. Validation is illustrative rather than experimental: the framework components map to concrete technologies (e.g. SOAR playbooks, Velociraptor collections, Timesketch-style timelines) and to CSIRT operating models commonly used in large enterprises. Design choices are cor- roborated by peer-reviewed evidence on the need for scalable forensics and cloud acquisition [7], [25]–[27]. Organizations can further evaluate the framework using IR metrics (e.g., mean time

to detect/contain/recover and events-per-second in forensic pipelines).

3. Challenges In Large-Scale Incident Response

Operating on an enterprise scale introduces: alert overload and detection gaps; heterogeneous hybrid estates (on-premises, multi-cloud, SaaS); unclear roles/processes under stress; lim- ited resources/skills; and massive forensic data volumes that overwhelm traditional tools [4]–[7], [16].

4. Automating Incident Response with Soar Playbooks

Security Orchestration, Automation, and Response (SOAR) platforms execute standardized playbooks to perform repeat- able containment and enrichment at machine speed [8], [10]– [12]. In practice, SOAR often integrates with Extended De- tection and Response (XDR) platforms to trigger endpoint isolation, network blocking, identity actions, and evidence collection across thousands of assets, reducing human error and creating a full audit trail [9], [23].

5. Incident Response Life Cycle

A NIST-aligned lifecycle—Preparation, Detection, Con- tainment, Eradication, Recovery, Lessons Learned—structures actions and deliverables, with automation codifying transitions and escalations [3], [12].

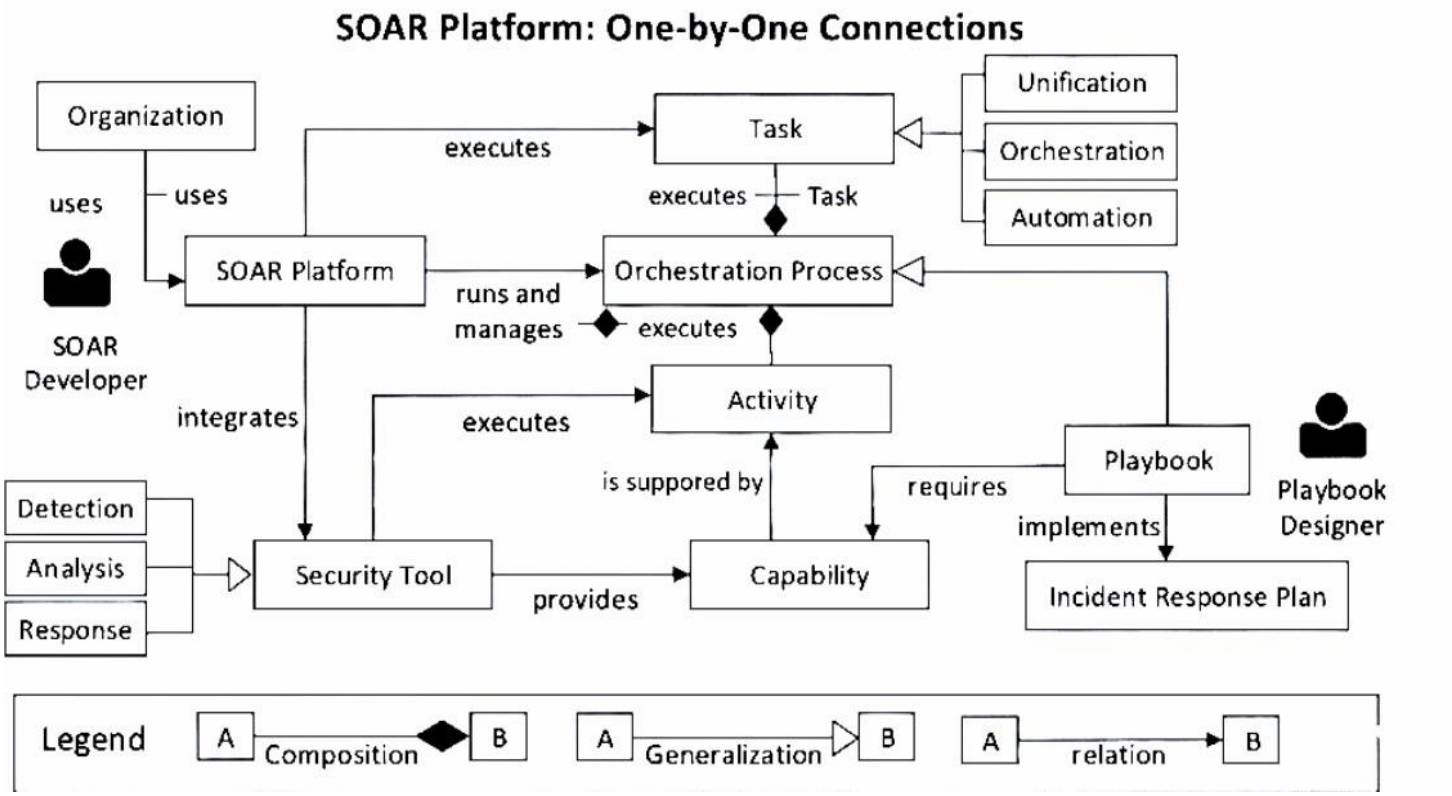

Fig. 1. SOAR Platform Architecture (adapted from [8]). Conceptual archi- tecture showing integrations, orchestration logic, and analyst interfaces.

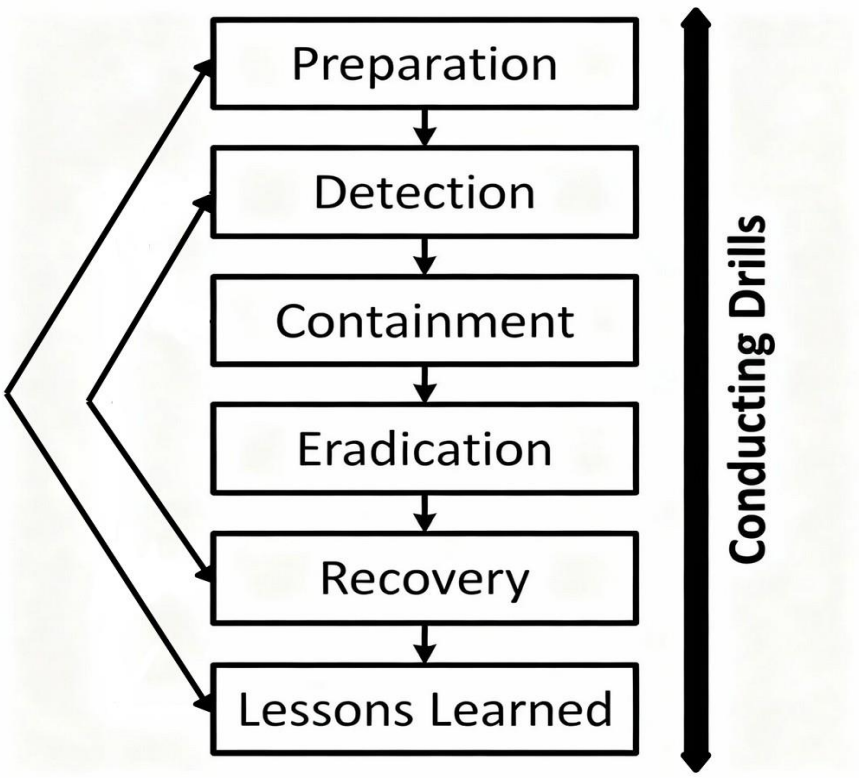

Fig. 2. Incident Response Life Cycle (adapted from [3], [12]). Phases mapped to automated playbook steps and escalation criteria.

6. Enhancing digital forensics tools and Processes

Traditional per-host imaging and manual log review do not scale to hundreds or thousands of systems [7], [25]. This paper demonstrates three pillars for scalable DFIR:

A. Distributed Endpoint Collection

Open-source tools such as Velociraptor allow targeted acquisition (system logs, memory, browser data) on Windows / Linux / macOS at enterprise scale, allowing proactive searches and rapid collection without full-disk imaging [14].

B. Cloud Forensics

Cloud environments require acquisition of VM snapshots, platform logs, and container images with chain-of-custody controls. Academic work details trust models and tool efficacy

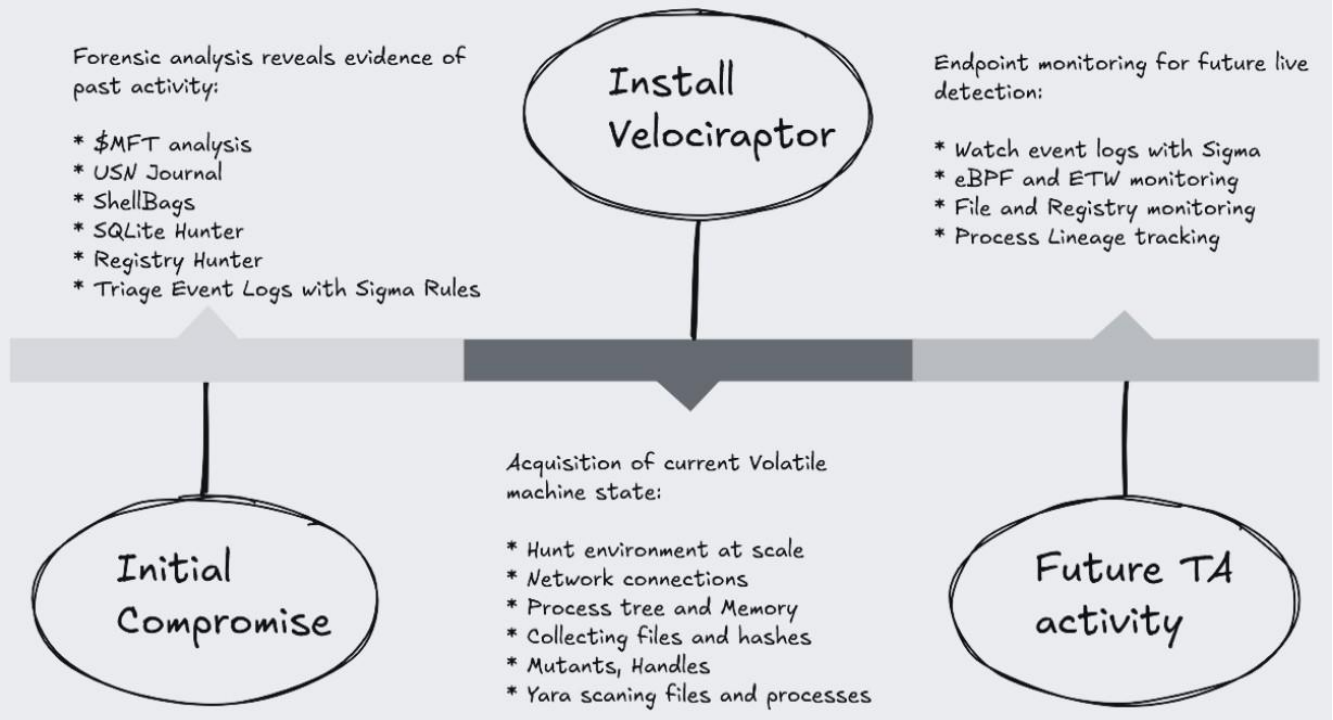

Fig. 3. Scalable DFIR Pipeline (adapted from [14]). Distributed collection feeds a centralized analysis platform for timeline generation and cross-host correlation.

for infrastructure-as-a-service evidence acquisition, informing the procedures embedded in this framework [15], [26].

C. Scalable Timeline Analysis

Centralized, horizontally scalable platforms (e.g., Elasticsearch-backed timelines akin to Timesketch) correlate events across hosts and accounts. Research underscores the need for scalable models and data handling to keep pace with enterprise-scale investigations [7], [25].

7. COORDINATING RESPONSE TEAMS AND COMMUNICATION

A well-defined CSIRT with clear role definitions (incident commander, technical leads/analysts, IT operations, legal and communications) and SOC collaboration improves decision- making under pressure [18]–[22]. Modern case-management tied to SOAR provides a shared "single pane of glass," live tasking, and a defensible audit trail [23], [24].

8. Best Practices and Recommendations

- **Invest in Automation**. Develop, version, and test modular SOAR/XDR playbooks; enforce logging for audits [8], [10]– [12], [23].
- **Establish Scalable Forensics**. Pre-deploy distributed col- lection, artifact baselines, and cloud-specific acquisition runbooks [14]–[16], [25], [26].
- **Define Clear Roles**. Document CSIRT responsibilities, escalation paths, and executive notification thresholds; exer- cise via tabletops [18], [19], [23], [24].
- **Measure and Improve**. Track mean time to detect/contain/recover (MTTD/MTTC/MTTR), events-per-second ingested, and cases-per-analyst to drive continuous improvement.
- **Prepare for Scale**. Design for parallel containment across endpoints, identities, and cloud assets; assume multiple concurrent incidents across regions.

9. Limitations And Future Directions (Discussion)

Limitations. This paper presents a consolidated framework rather than controlled empirical evaluation; tool performance

and integration depth vary by environment. Figures are con- ceptual and emphasize architecture over vendor-specific nu- ances.

Future Directions. Promising areas include AI-assisted SOAR, where large-scale correlation recommends or executes safe, reversible actions; automated forensic triage using ma- chine learning to prioritize hosts, users,

and artifacts; cloud- native evidentiary provenance to standardize chain-of-custody; and privacy-preserving analytics to balance rapid response with regulatory constraints [7], [25]–[27].

10. Conclusion

This paper demonstrates a practical framework that unifies SOAR-driven playbooks, distributed evidence collection, and big-data timeline analysis with CSIRT-centered gover- nance. Organizations can measure benefits using established IR metrics: shorter MTTC/MTTR via automated containment and enrichment, higher analysis throughput (events-per-second indexed and queries-per-analyst), and improved auditability through end-to-end logging [4], [7], [10], [23]. By investing in automation, scalable forensics, and clear roles, large enter- prises can materially reduce incident impact and strengthen cyber resilience.

References

1. Atlassian, “Incident Response: Best Practices for Quick Resolution,” 2023.
2. Cybersecurity and Infrastructure Security Agency (CISA), “Federal Government Cybersecurity Incident and Vulnerability Response Play- books,” 2021.
3. National Institute of Standards and Technology (NIST), “Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide,” 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
4. Swimlane, “Orchestrating Incident Response at Scale,” 2022.
5. Hunt & Hackett, “Turning Incident Response Challenges into Scalable Solutions,” 2025.
6. Exabeam, “Incident Responder Product Brief,” 2023.
7. V. Roussev, “Digital forensics at scale,” IEEE Transactions on Informa- tion Forensics and Security, 2020.
8. C. Islam, M. A. Babar, and S. Nepal, “Architecture-Centric Support for Integrating Security Tools in a SOAR Platform,” in Proc. IEEE CSCloud, 2020. Available: https://doi.org/10.1007/978-3-030-58923-3 11
9. Coretelligent, “Automated Response Playbooks,” 2024.
10. Atlassian, “Automating IR Playbooks,” 2023.
11. Atlassian, “Playbook Automation Best Practices,” 2023.
12. Exabeam, “SANS Incident Response: 6-Step Process & Critical Best Practices,” 2023. [Online]. Available: https://www.exabeam.com/explainers/incident-response/sans-incident-response-6-step-process-critical-best-practices/
13. ResearchGate, “Scaling Android Forensics,” 2023.
14. Velociraptor, “Documentation and Overview.” [Online]. Available: https://docs.velociraptor.app/docs/overview/
15. Cloud Security Alliance, “Cloud Forensics Best Practices,” 2023.
16. Hunt & Hackett, “Timeline Scalability Solutions,” 2025.
17. Hunt & Hackett, “Timesketch Enhancement Project,” 2025.
18. NIST, “CSIRT Role Definitions,” 2012.
19. CSIRT Services, “Incident Commander Best Practices,” 2023.
20. Security Operations, “Technical Lead Responsibilities,” 2023.
21. IT Operations, “Infrastructure Support During Incidents,” 2023.
22. Legal & Compliance, “Incident Communication Protocols,” 2023.
23. Exabeam, “Case Management Features,” 2023.
24. Atlassian, “Tabletop Exercises and Drills,” 2023.
25. S. Garfinkel, “Digital Forensics Research: The Next 10 Years,” Digital Investigation, vol. 7 (Supplement), pp. S64–S73, 2010.
26. J. Dykstra and A. T. Sherman, “Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques,” Digital Investigation, vol. 9 (Supplement), pp. S90–S98, 2012.
27. E. Casey, M. Ferraro, and L. T. Nguyen, “Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence,” Journal of

Forensic Sciences, vol. 54, no. 6, pp. 1353–1364, 2009.

28. B. Martini and K.-K. R. Choo, “Cloud Storage Forensics: ownCloud as a Case Study,” Digital Investigation, vol. 10, pp. 287–299, 2013.