TAG CYBER

opentext™

The Importance of Digital Forensics for Effective Enterprise Incident Response

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber
Distinguished Research Professor, NYU

Modernization of incident response capabilities has become a critical focus of enterprise security with on-going shifts-right in the protection landscape. Digital forensic investigation support is shown to be an essential component of incident response and guidance is offered on how to optimize the interaction, especially as commercial platforms and tools are selected by CISO-led teams.

Introduction to Enterprise Incident Response

The modern Chief Information Security Officer (CISO) understands the importance of incident response in the context of an overall enterprise risk management strategy. Common strategies to perform a so-called "shift right" transition in emphasis on the prevent-detect-respond scale underscore how critically essential it has become for CISO-led teams to have effective tools, processes, and procedures to support their incident response program.

Luckily, this new emphasis builds on a mature base. Incident response has been an element of security programs since their inception, and most working professionals understand how to handle an on-going case or exploit incident. What might not have been as clear at the outset, however, but that has become quite obvious today is the critical role that digital forensic investigation capabilities play in assuring that incidents are responded to properly.

Traditional digital forensic investigations involved simple tools to create image copies of simple devices such as PCs and mobile phones for the purposes of answering simple questions about usage. Today, these early methods have evolved to include detailed analysis and investigation of more complex infrastructure, systems, applications, and devices that sprawl across multi-cloud networks and that must handle off-network, third-party, and other cases.

In this report, we provide guidance for enterprise security teams on the evolution of investigation in enterprise incident response, and how to best integrate digital forensic investigation platforms into their incident response programs. This is done by connecting the future goals and objectives of both types of initiatives together into an effective future state where both response and investigation benefit from the mutual synergy. A set of questions is offered for enterprise teams to ask when selecting both incident response and forensic platforms to optimize this interaction.

Investigation as a Component of Enterprise Incident Response

The most commonly cited guide for incident response comes from the US National Institute for Standards and Technology (NIST). Their special publication on incident handling offers detailed and effective guidance for practitioners on how to set up, manage, organize, and operate incident response programs. Furthermore, NIST recommends an incident response lifecycle that has formed the basis for many enterprise programs in place today (see Figure 1).

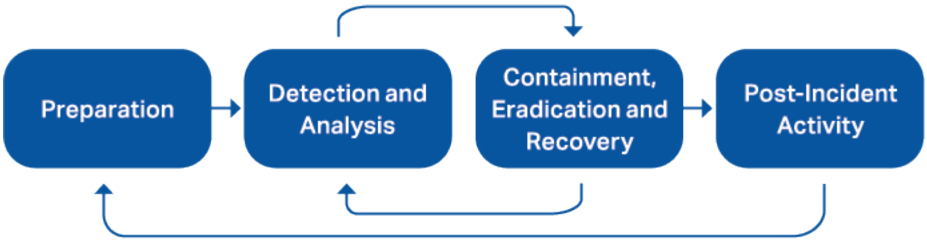


Figure 1. NIST SP 800-61 Incident Response Lifecycle

This NIST guidance is complemented by recommendations in a separate special publication for how to integrate digital forensics into incident response [2]. The NIST work accurately reflects the foundational role that digital forensics plays in the overall incident response lifecycle. It also serves to help enterprise teams recognize that as incident response has had to adapt to modern hybrid multi-cloud infrastructure, the corresponding forensic methods have had to adapt as well. This report builds on the NIST guidance.

Investigation-Related Capabilities for Enterprise Incident Response

To support modern incident response, forensic investigative methods must be adapted to address digital transformation. This includes support for zero trust networks, massive work-from-home remote access, workload hosting in distributed multi-cloud, increasing dependence on mobile apps and infrastructure, and increased use of Agile delivery of software through CI/CD pipelines. All of these advances require expert support from the forensic platform in use.

To address these on-going evolutionary changes in the context of security incident handling, modern digital forensic platforms, and their associated processes, must be flexible and adaptable to the new response environment. In establishing (or evolving) a digital forensic capability that can properly integrate with incident response, the following requirements must be addressed by the enterprise security team:

Roles and Responsibilities

Clarity is required in the roles and responsibilities for the forensic and response teams – recognizing that there will likely be some overlap in the individuals involved. This implies that some team members might play dual roles during an incident.

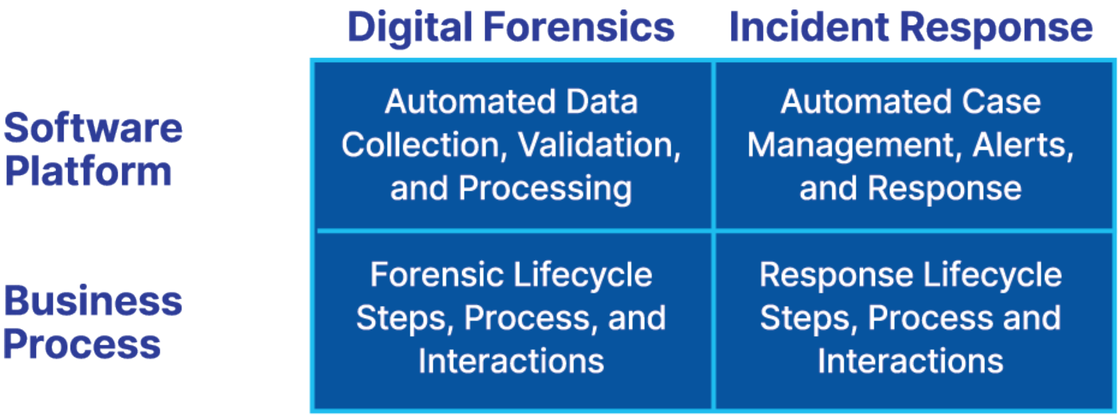
Lifecycle Coverage

Digital forensic and incident response capabilities must be designed to include full lifecycle coverage starting with the continuous integration/continuous delivery (CI/CD) pipeline up to the restoration and recovery processes.

Expanded Scope

The biggest adjustment for modern forensic teams involves expanded scope from analysis of locally-controlled devices to analysis of assets located across a zero trust architecture.
Most response teams have already made this transition.

Security leadership teams must also recognize the interdependencies that exist between platforms and processes in the context of both response and forensics. When these factors are taken into account, a simple conceptual decision model emerges that can help managers optimize how they approach both tasks. This model is shown in Figure 2 below.



	Digital Forensics	Incident Response
Software Platform	Automated Data Collection, Validation, and Processing	Automated Case Management, Alerts, and Response
Business Process	Forensic Lifecycle Steps, Process, and Interactions	Response Lifecycle Steps, Process and Interactions

Figure 2. Conceptual Model for Response and Forensics

The key issue in the application of the conceptual model involves the interaction and interdependencies that exist between the cells of the matrix. For example, software platforms for forensics and response must include means for sharing (likely across APIs) and business processes for each task must also be coordinated (likely via automated workflow). Such integration can be done through platforms with comprehensive coverage or can be done post-deployment by enterprise teams.

Market Landscape for Modern Enterprise Forensic Investigation

Enterprise teams should have a clear understanding of the specific digital forensic requirements that must be supported during incident response. As such, it is helpful to provide a simple guide for security practitioners to use in establishing completeness of coverage for their selected forensic platform. The section below offers a set of questions to ask when selecting a forensic tool that will integrate with the local incident response ecosystem.

Does the platform support file forensics during incident response?

The forensic investigation of collected text and binary files are an essential component of the incident response lifecycle. Whether pulled from a mobile device, PC, or other system, files serve as the most important unit of data for the investigator. This is especially true during the containment and eradication phases of security incident response.

Does the platform support operating system forensics during incident response?

Operating systems also provide valuable evidence to forensic investigators during response. The collection and analysis of data directly from the operating system has always been a key activity for investigators, especially in cases where a targeted suspect has tried to cover up evidence by deleting files or other activity.

Does the platform support network forensics during incident response?

Emphasis on the local and wide areas network has grown for both digital forensics and also incident response. With new emphasis on zero trust architectures, identifying networks or data locations of interest is less obvious, and should include the public-facing repositories, as well as the private networks of suppliers, partners, and even customers of a business.

Does the platform support forensic collection from non-traditional sources such as social media?

Evidence for modern enterprise forensic cases is increasingly located in non-traditional sources such as social media. This implies that the selected forensic platform must include tools or interfaces that can help to identify, locate, and extract such data for investigative purposes. This capability will continue to evolve as technology advances and users evolve to new on-line forums and systems.

Does the platform support application forensics during incident response?

The role of applications, both web and mobile ecosystem based, has now aligned with the broadest goals of any organization. Applications are the means by which data is obtained in a business, so forensic and response activities will necessarily need to include good collection, analysis, and reporting tools that work on legacy, commercial, and SaaS applications.

Does the platform support cloud forensics during incident response?

Cloud infrastructure has emerged as one of the most important aspects of enterprise IT and security. As such, both forensic platforms and incident response ecosystems must include means for addressing cases in public, private, or hybrid cloud. This also includes SaaS-based infrastructure, and should allow for interactions, if necessary, with commercial cloud security teams and their systems.

Does the platform include interfaces for integration with incident response systems?

The ability to integrate with automated incident response tools is an important requirement for modern digital forensic platforms. This is likely done through application programming interfaces (APIs) since manual integration can slow down collection and analysis. Standards for interactions between forensic and response tools have not emerged, but are likely to be seen in coming years.

References

[1] Computer Security Incident Handling Guide, NIST Special Publication SP800-61, Rev. 2 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[2] Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication SP 800-86, 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf