DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR): AN INTRODUCTION

Digital forensics and incident response is an important part of business and law enforcement operations. It is a philosophy supported by today's advanced technology to offer a comprehensive solution for IT security professionals who seek to provide fully secure coverage of a corporation's internal systems.

For this reason, many businesses are turning to DFIR to ensure the security of their most vulnerable and critical platform technology, like cloud services, devices and more. In the following article, we'll review DFIR, including:

- What is DFIR?
- What are the common capabilities of it
- Digital forensics vs. physical forensics
- The challenge of securing endpoints

This content is designed to help readers learn about DFIR capabilities, how to identify incidents within their own company and how to manage threats with an understanding of process, technique and communication.

What is Digital Forensics and Incident Response?

Digital forensics is a division of computer forensics that focuses on examining the digital components of an individual or business to determine if illegal action has been taken, either by the owner of the equipment or through a vicious cyberattack.

Computer forensics represents the skill set that IT professionals use to examine hard-drives and computing devices. However, in a digital business climate, it's important to expand consideration of threats to other digital properties like networks, memory, digital artifacts and more. In this way, digital forensics helps IT professionals identify instances of cybercrime like malware and hacking.

Incident response refers to the complementary set of processes that occur when an incident has been identified. In incident response, it's important that communication is clear and accessible, that all parties involved are notified by an incident response manager for the organization and, further, that steps are identified to resolve the issue.

During digital forensics and incident response, IT professionals might be tasked with malware analysis. Malware can be reverse-engineered by software professionals to learn more about how it operates, how it was produced and who made it.

What Capabilities are Common in DFIR?

Digital forensic technology solutions help clients support DFIR operations. Here are some of the capabilities you can expect from a DFIR software solution:

- Data acquisition that spans a number of sources, multiple devices and systems
- System transparency that offers clear visibility into actions and administrative processes
- Investigation capabilities that are comprehensive and compliant
- Reporting including features like robust visualization
- Automating iterative processes that help incident managers find all instances of artifacts, faster, with less guesswork

Six Steps of Incident Response

Companies large and small can benefit from a smooth DFIR process. For companies who must assess risk and mitigate threats, it's important to understand the steps associated with incident response. The six common steps are:

1. **Preparing:** Companies can be prepared to handle incident response with policies in place, incident managers defined and platform software identified.
2. **Identifying:** During the identification phase, IT professionals detect the incident, the kind of attack that's occurred, the risk involved and more.
3. **Containing:** Next, incident managers work to quickly contain the threat so that it doesn't continue to spread through adjacent systems.
4. **Remediating:** A plan is established to correct the issue. Forensic analysis is applied to artifacts to determine the best way to resolve.
5. **Incident recovery:** Following established policies, the company begins to resume regular operations. During this phase, monitoring and reporting on the incident is continuous and ongoing.

6. **Reporting and communication:** The incident manager must communicate with stakeholders, end-users and the public to report on progress of the incident while providing transparency.

Digital Forensics vs Physical Forensics

Physical forensics is the act of investigating a crime by examining and analyzing physical evidence like fingerprints, DNA and other clues that might be left a crime scene. It is primarily used in law enforcement, and corporations have little need for physical forensics.

Digital forensics, on the other hand, serves both law enforcement and enterprise businesses looking to investigate attacks on their digital properties. In law enforcement, digital forensics specialists are increasingly becoming in higher demand as cybercrime rises. In corporate security, businesses rely on these professionals to ensure their business and customer data remains secure and useable.

The Challenge of Securing Endpoints

One challenge that all digital forensics professionals face, whether in IT security or physical forensics, is securing endpoints. In the digital landscape of enterprise businesses, endpoints occur where one system ends and another begins. This could refer to cloud platforms, networks, devices and more. Managing the security of endpoints is a top priority for cybersecurity professionals today.

A comprehensive DFIR system helps enterprise businesses secure these vulnerable areas of their multi-platform systems. This is especially important for large corporations because their vulnerability and risk increases exponentially when a high-volume of data must be sifted through to reach the most important alerts.

Cloud Considerations

With a growing number of companies relying on cloud technology and the constant evolution of digital business, there are several considerations that should be made when thinking about the future of DFIR.

For one, current trends in business have many businesses operating partially and fully in the cloud. For companies who work with cloud technology, agility and the ability to scale quickly are imperative to keeping up with the competition and being successful. Many large, recognizable companies use development platforms that operate fully in the cloud, and they must be aware of how to use DFIR to mitigate risk and solve issues.

In a cloud environment, responders must ask quickly and decisively if they are going to resolve the threat before lasting damage occurs for a company. This requires responders to find artifacts left behind by hackers deploying malware and other threats. Once an artifact is found, there is a manual process that typically occurs where the IT professional will then try to locate the artifact on other iterations of the cloud platform until they believe they have contained the threat. However, this is not a foolproof method.

It's for this reason that companies in the cloud need to implement DFIR solutions to ensure the success of finding and collecting artifacts and managing threats.

BMC: End-to-End Security Management

For businesses trying to mitigate threats and stay ahead of the competition, it's important to implement DFIR processes that help them analyze, communicate and recover from threats.

BMC has a large suite of the most innovative security products to meet your company's needs. These include products geared at assessing risk and remaining compliant. In addition, BMC is your end-to-end security management partner for DFIR solutions and capabilities.

For more information on how BMC can help you with security, browse these security offerings and contact BMC today.