CISO MAG

beyond cybersecurity

Volume 5 | Issue 06 | June 2021

"Public GitHub is often a blind spot in the security team's perimeter"

Jérémy Thomas
Co-founder and CEO
GitGuardian

54

UNDER THE SPOTLIGHT

IMPLEMENTING

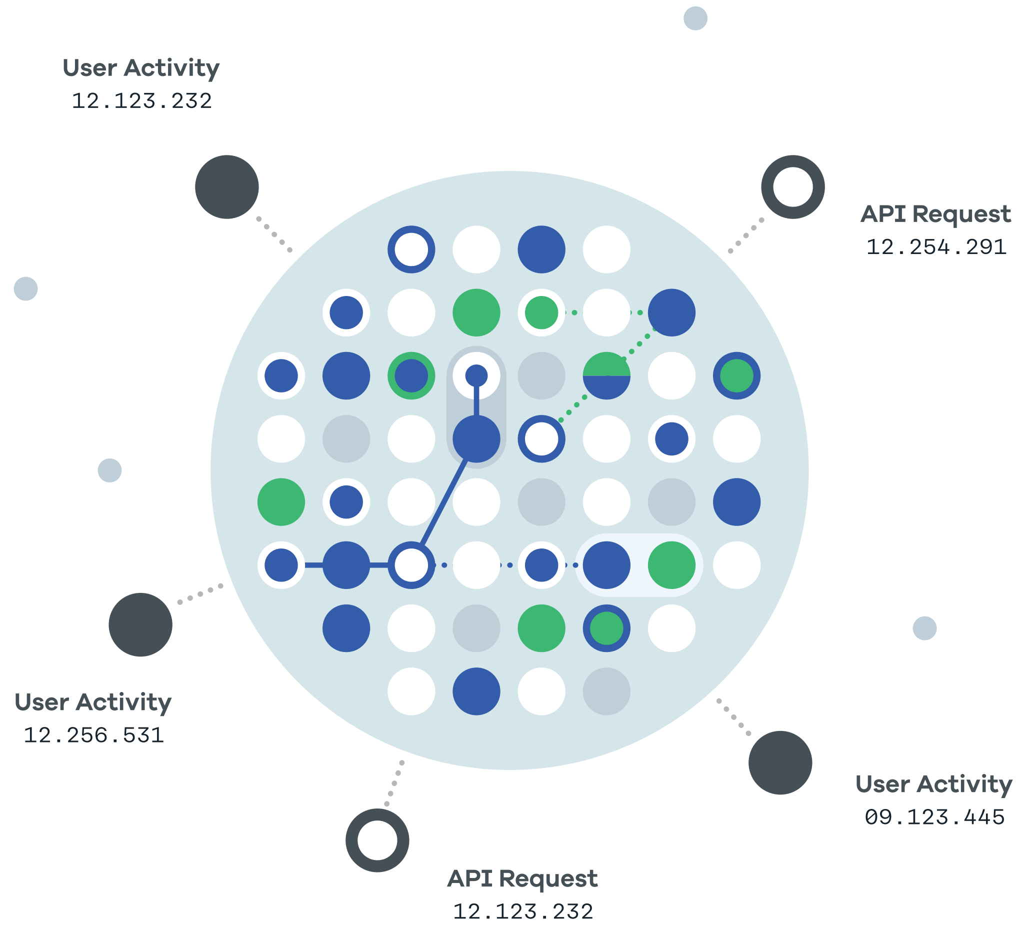
DIGITAL FORENSICS

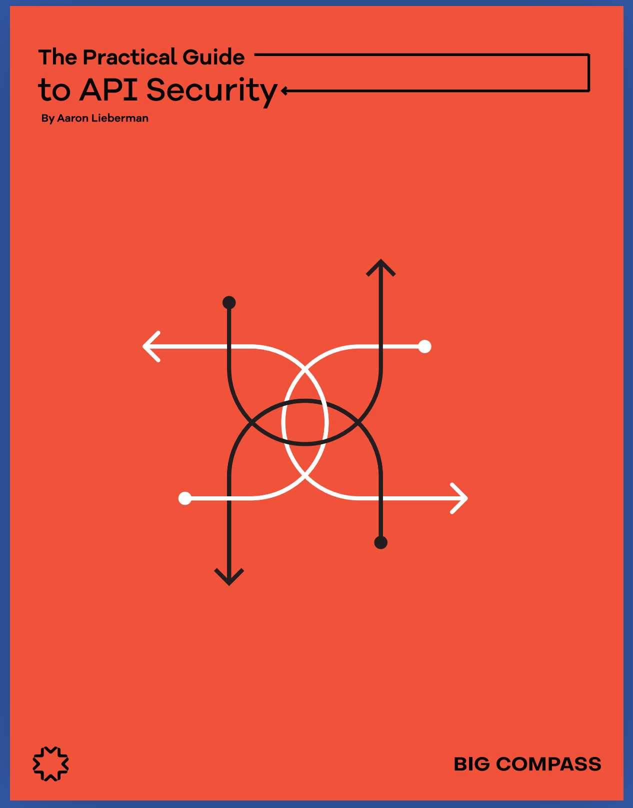
IN EMERGING TECHNOLOGIES

TRACEABLE_

Traceable enables security to manage their application and API risks given the continuous pace of change and modern threats to applications.

Know your application DNA




The Practical Guide to API Security

By Aaron Lieberman

BIG COMPASS

Download the practical guide to API Security

Learn how to secure your API's. This practical guide shares best practices and insights into API security. **Scan or visit** Traceable.ai/CISOMag

TRACEABLE_

CISO MAG
beyond cybersecurity

Volume 5 | Issue 06
June 2021

President & CEO
Jay Bavisi

Editorial
Editor-in-Chief
Brian Pereira*
brian.p@eccouncil.org

Assistant Editor
Augustin Kurian
augustin.k@eccouncil.org

Sr. Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Sr. Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Sub Editor
Pooja Tikekar
pooja.v@eccouncil.org

Management
Senior Vice President
Karan Henrik
karan.henrik@eccouncil.org

Director of Marketing
Nandakishore
nandakishore.p@eccouncil.org

General Manager - Marketing
Seema Bhatia
seema.b@eccouncil.org

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Head - Research & Content
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Manager - Digital Marketing
Rajashakher Intha
rajashakher.i@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer
Jeevana Rao Jinaga
jeevana.r@eccouncil.org

Manager – Marketing and Operations
Munazza Khan
munazza.k@eccouncil.org

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,

EDITOR'S NOTE

DIGITAL FORENSICS EDUCATION MUST KEEP UP WITH EMERGING TECHNOLOGIES

Brian Pereira
Editor-in-Chief

"There is nothing like first-hand evidence."
- Sherlock Holmes

If the brilliant detective **Sherlock Holmes** and his dependable and trustworthy assistant **Dr. Watson** were alive and practicing today, they would have to contend with crime in the digital world. They would be up against cybercriminals working across borders who use sophisticated obfuscation and stealth techniques. That would make their endeavor to collect artefacts and first-hand evidence so much more difficult!

As personal computers became popular in the 1980s, criminals started using PCs for crime. Records of their nefarious activities were stored on hard disks and floppy disks. Tech-savvy criminals used computers to perform forgery, money laundering, or data theft. Computer Forensics Science emerged as a practice to investigate and extract evidence from personal computers and associated media like floppy disk, hard disk, and CD-ROM. This digital evidence could be used in court to support cases.

Until then, forensics was straightforward. Investigators had to locate the media and extract the data. They ran into a wall if the files were password protected or encrypted, but experts soon found a way around that challenge.

Then computers were connected to the networks, and eventually to the Internet. And the trail got longer and ran into a maze. So, we had a new branch, Network Forensics.

As technology evolved through the years, cybercrime extended to the Web, the cloud, and mobile devices. Malware became more sophisticated, and today we have ransomware.

Smartphones with watertight encryption came along, and that posed a huge challenge to forensics investigators. Do you remember the Apple iPhone incident a few years ago, when the FBI asked Apple to unlock the iPhone of a criminal? Apple refused. The tussle between the FBI and Apple was holding up the investigation until a third-party finally figured out how to unlock the iPhone.

Today, forensic experts travel to different countries to find digital evidence, as cybercrime is performed across borders. These digital forensic experts are the modern-day version of Holmes investigating clues left by criminals.

Emerging technologies and borderless cybercrime have made Digital Forensics more challenging than ever.

So how do we counter all this with a completely different strategy?

SURVEY & REPORT

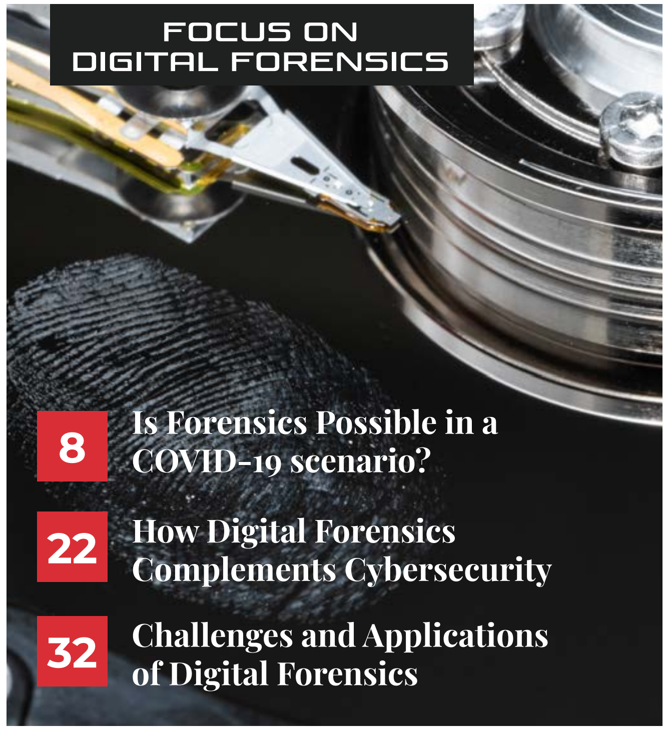
To better understand the challenges and state of readiness in implementing Digital Forensics in emerging technologies, ***CISO MAG***, in collaboration with EC-Council's CHFI group (Computer Hacking and Forensic Investigation), launched a Technology Trends Survey in April 2021. The resulting report included in this issue offers an in-depth analysis of how important it is to incorporate the effects of digital forensics on emerging technologies into the curriculum of digital forensic education.

The **key findings** of the **survey,** as well as the insights provided by experts in our **Focus on Forensics** section, will be an eyeopener for those seeking training and a career in Digital Forensics.

And it surely is a career with a lot of opportunities!

INDEX

Contents



FOCUS ON DIGITAL FORENSICS

BUZZ

UNDER THE SPOTLIGHT

INSIGHT

COVER STORY

SURVEY

KNOWLEDGE HUB

TABLE TALK

FOCUS ON
DIGITAL FORENSICS

Is Forensics Possible in a COVID-19 scenario?

Narendra Sahoo
Founder and Director
VISTA InfoSec

The COVID-19 pandemic has created havoc not just in the lives of people but also rocked the business world globally. With countries going into lockdown, businesses are today forced to adapt to the situation and operate remotely. With this, businesses are confronted with new challenges and threats. Although organizations around the globe have adopted the work-from-home operating model, this has opened doors to malicious cyberattacks. With the new working norms and companies accelerating their digital transformation, cybersecurity is now a major concern.

While the entire world is focusing on health, the economy, and restoring normalcy, criminals are constantly capitalizing on the situation to stage a well-planned cyberattack. Not only does the incident of cyberattack have severe reputational, legal, operational, and compliance implications, it also severely impacts the forensic investigation. Speaking more on this, we have explained in the article the challenges of remote working, pre-requisites to prevent incidents of the breach, the protocols to be followed in case of a data breach, and all the nitty-gritty of cyber forensics. The article provides insight on the impact of remote working on Cybersecurity, and the process of cyber forensics in case of a breach.

What happens in Cyber Forensics?

Handling a data breach incident in a normal scenario is very different from the current situation for both the organization and the cyber forensic team. Before the pandemic, when businesses were running in a controlled environment, even in case of a data breach, immediate response, measures to contain, and investigations helped lower the impact. However, now in the pandemic situation, with the remote working model, the situation is completely different. Not only has this increased the risk of a cyberattack, but it has also hampered the process of investigation and containing the situation in case of a data breach. But, before we get into the details of the challenges faced in cyber forensics during the pandemic, let us first understand the process of a cyber forensics investigation.

Cyber Forensics Investigation

Before the pandemic, when a data breach incident occurred, organizations had to follow a specific protocol to respond and contain the incident. With that, a cyber forensic team investigates the situation at the location and helps the organization respond, recover and resolve the incident. The process of handling the incident involves two primary steps which include:

- Responding and Containing Incidents
- Investigating the Incident and Collecting Evidence

While the approach taken by the organization may vary based on their priorities, severity of the incident, and impact of the incident, there are certain basic protocols organizations must follow. Given below is a list of protocols that organizations should follow in case of a data breach. Once there is a breach, the organization should follow a few essential steps immediately to limit the impact of the breach.

Protocol to be followed in a Data Breach Incident

Step 1: Survey the damage

Once the organization discovers the data breach incident, the Information Security Officer along with the designated information security team should conduct an internal investigation. This is to first determine whether an incident has happened and to access the impact of the incident on critical business functions. They further need to conduct an in-depth investigation to identify the attacker/source of the attack, discover the exploited security vulnerabilities, identify immediate steps that can be taken to limit the loss, and determine steps for resolution and improvements. If an attack is confirmed, it is well advised to hire external professionals to investigate and take steps.

Step 2: Contain the Situation

Once the organization determines the impact of the incident, security vulnerabilities, and the attackers they should take steps to contain the damage. This should include steps like:

- Isolating the compromised network
- Filter or block traffic
- Re-route network traffic
- Temporarily disable remote access capability and wireless access points (situation-based)

- Change Access Control credentials
- Segregate all hardware devices from the infected system or network
- Isolate and quarantine identified malware rather than deleting it (for future analysis and evidence)
- Preserve firewall settings, firewall logs, system logs, and security logs for future analysis and evidence

Step 3: Record and file details

Once the survey is conducted and situations are contained, the information security team must maintain a written log of all the actions taken to respond to the breach. The information that should be collected and filed must include:

- Details of the affected systems
- Compromised network and accounts
- Services disrupted due to the breach
- Data and network affected by the breach
- Amount and type of damage done to the systems

Other details that should be documented must include details like how you learned about the breach, the date, and time you were notified, how were you notified, all actions taken between now and the end of the incident, date and time you isolated systems infected, and disconnected from the Internet, disabled remote access, changed credentials/passwords, and system hardening or any other remediation steps taken over time.

Step 4: Inform the Regulators

In case of a breach, the organization should immediately report the incident to law enforcement or regulators. The notifiable breach should be reported at the earliest but not later than 72 hours after being aware of the breach. The duration depends primarily on the local regulatory framework, compliance requirements, and client SLA. Reporting should be done only by approved official channels and personnel. All other personnel should be explicitly prevented from sharing any information with anyone, whether internal or external to the organization.

When reporting the incident of the breach, the nization will have to provide the following regulator:

of data breach
als affected