EC-Council

CYBER BRIEF

MAR 2021

Develop a passion for learning. If you do, you will never cease to grow.

- Anthony J. D'angelo

The beginning of the new financial year is a great time to analyze our biggest strengths and weaknesses on the cybersecurity front. The March Cyber Brief places a special focus on the need for diversity and inclusion in cybersecurity, which also emphasizing on the various new threat areas that need more attention. We hope that this issue will address those questions about cybersecurity that have remained unanswered, until now.

Access EC-Council's Cyber Brief - Feb 2021 here »

Chief Information Security Officers

Webinar

Mansi Thapar

IT Leader, Head – Information Security
at Jaquar Group

HOW TO NAVIGATE YOUR FIRST 90 DAYS AS A CISO

WATCH NOW

Blog

BUSINESS INFORMATION SECURITY OFFICER (BISO) – ALL YOU NEED TO KNOW

A Business Information Security Officer (BISO) is a senior security leader assigned to lead a group or business unit's security policy...

READ MORE

Blog

WHAT IS IDENTITY AND ACCESS MANAGEMENT (IAM)?

In enterprise IT, Identity and Access Management (IAM) is about identifying and...

READ MORE

Blog

REGULATORY COMPLIANCE: HOW TO STAY ON THE RIGHT SIDE OF THE LAW

Every organization faces the key requirement of adhering to government-set guidelines and...

READ MORE

Blog

WHAT IS COMPLIANCE TRAINING? DOES IT REALLY MATTER?

How often have you heard the term compliance training and...

READ MORE

Blog

WHAT IS CISO? ROLES, RESPONSIBILITY, CAREER, SALARY AND REQUIREMENT FOR BECOMING CISO

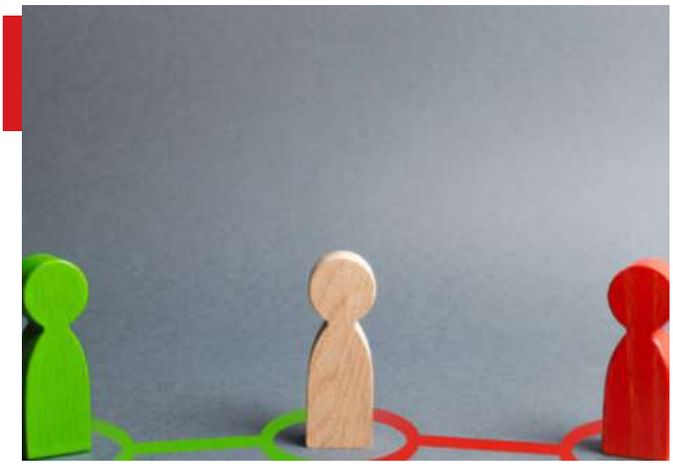
Have you ever wondered what is CISO? What is their Job?...

READ MORE

Ancillary Page

What Is Risk Management?

READ MORE



Blog

WHAT IS VENDOR RISK MANAGEMENT (VRM) AND WHY WE NEED THEM?

Third-party services are crucial to every organization...

READ MORE

Whitepaper

WHY ORGANIZATIONS NEED STRONG CYBERSECURITY RISK MANAGEMENT CAPABILITIES

With the increase in usage of network and cloud technology...

READ MORE

EC-Council

Infographics

CYBERSECURITY INCIDENT RESPONSE

5 DO'S & DON'TS OF EFFECTIVE INCIDENT RESPONSE

DO'S AND DON'TS

DO'S

- Collect volatile data and other critical artifacts from the system using forensic tools
- Collect external intelligence based on Identified Indicators of Compromise (IOC)
- Secure systems and other media for forensic collection
- Gather appropriate logs at both network & end point level
- Communicate with potential customers and stakeholders

DON'TS

- Panicking makes things worse
- Never shut down compromised systems
- Never discuss the incident with others unless otherwise directed
- Never use domain admin credentials to access the systems environment
- Never execute any non-forensic software on compromised systems

READ MORE

Slideshare

HOW TO TROUBLESHOOT SECURITY INCIDENTS IN A CLOUD ENVIRONMENT?

READ MORE

Blog

WHAT IS INCIDENT RESPONSE LIFE CYCLE? EVERYTHING YOU NEED TO KNOW

Incident response is a plan for methodically responding to a cybersecurity incident...

READ MORE

Blog

HOW TO USE OSINT TOOLS FOR BETTER INCIDENT RESPONSE

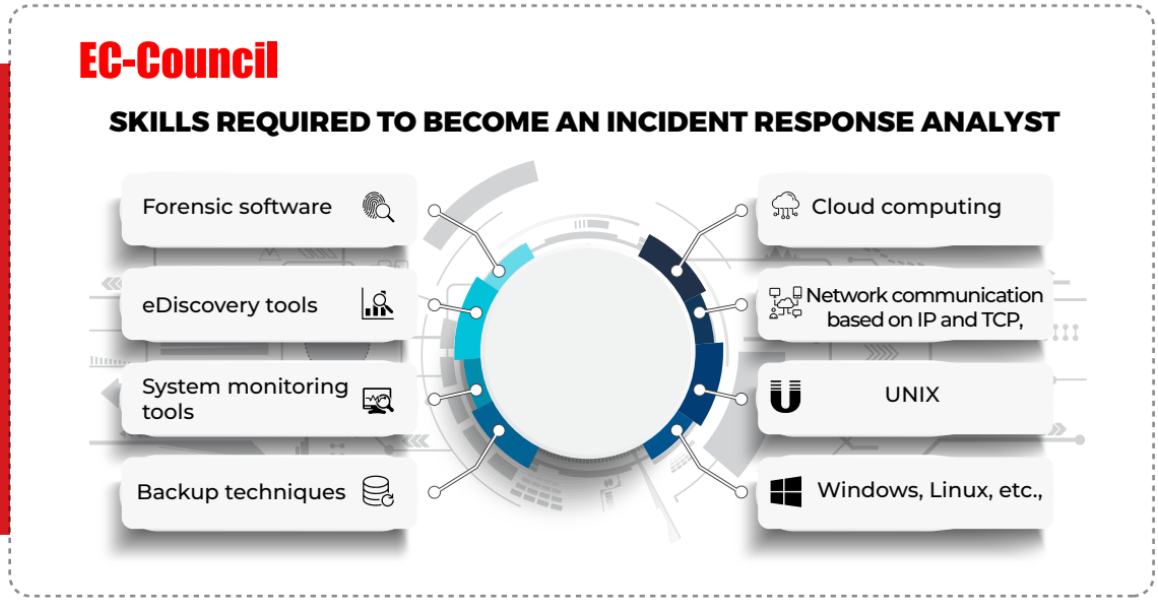
Open-source intelligence (OSINT) is vital to understand incident response in today's cyber world...

READ MORE

Infographics

SKILL REQUIRED TO BECOME A SUC-CESSFUL INCIDENT RESPONSE ANALYST

READ MORE



Blog

WHAT ARE THE TOP CLOUD COMPUTING THREATS AND HOW TO AVOID THEM?

An estimated 70% of businesses are using...

READ MORE

DO YOU KNOW HOW TO RESPOND TO AN INSIDER THREAT?

This is the era of technology, competition...

READ MORE

CLOUD INCIDENT RE-SPONSE AND BEST PRACTICES

Most businesses have started moving their...

READ MORE

Ancillary Page

PHASES TO BUILD A ROBUST INCIDENT RESPONSE PLAN

READ MORE

Whitepaper

INCIDENT HANDLING AND RESPONSE FOR BEGINNERS: A STEP-BY-STEP GUIDE

Computer security incident response systems have not just become a backbone of IT enterprises...

READ MORE

Blog

WHAT IS INCIDENT MANAGEMENT? HOW DOES IT HELP?

Imagine a scenario where internet connectivity is lost for a day due to a denial of service attack.

READ MORE

Blog

WHAT ARE THE TYPES OF INCIDENT SECURITY AND HOW CAN YOU MITIGATE SUCH RISKS?

Detecting incident security events as soon as...

READ MORE

Blog

WHAT ARE THE RESPONSIBILITIES OF A SUCCESSFUL INCIDENT RESPONSE TEAM?

There are many risk and threat management...

READ MORE

Blog

HOW TO CREATE A SUCCESSFUL INCIDENT RESPONSE PLAN

The threat landscape is evolving every day...

READ MORE

Blog

WHAT IS CENTRALIZED LOGGING AND WHY IS IT IMPORTANT?

In the event of a cybersecurity breach, logs play a crucial role in various activities...

READ MORE

Blog

WHAT IS THE ROLE OF A THREAT INTELLIGENCE PLATFORM IN A SUCCESSFUL SOC?

The rise of cybersecurity threats and the large volume of data involved...

READ MORE

Blog

WHAT IS SOC 2 TYPE 2 CERTIFICATION?

Data security has always been important for organizations, especially so for business...

READ MORE

Infographics

EC-Council

CSA Certified SOC Analyst

Simplified SOC Analyst Roles

ALERTS BY:

- IT Dept's
- Help Desk (Users)
- Security Intelligence Platform

TIER 1 ANALYST (Triage)

- Monitor event logs
- Basic Investigation and Mitigation
- Opens tickets, closes false positives

TIER 2 ANALYST (Investigation)

- Finding nature of threat
- Co-ordinate a response to remediate the issue
- Mitigation / recommends changes

TIER 3 ANALYST (Threat Hunting)

- Support incident response & looks for Forensic & telemetry data
- Prevention
- Mitigation / recommends changes
- Threat Hunting
- Counter intelligence
- Malware Reverser

READ MORE

Blog

WHAT IS A SOC AND HOW DOES A SUCCESSFUL SOC WORK?

The primary function of a Security Operations Center (SOC) is to prevent...

READ MORE

Blog

TOP 8 CHALLENGES FOR SOC TEAMS IN 2021

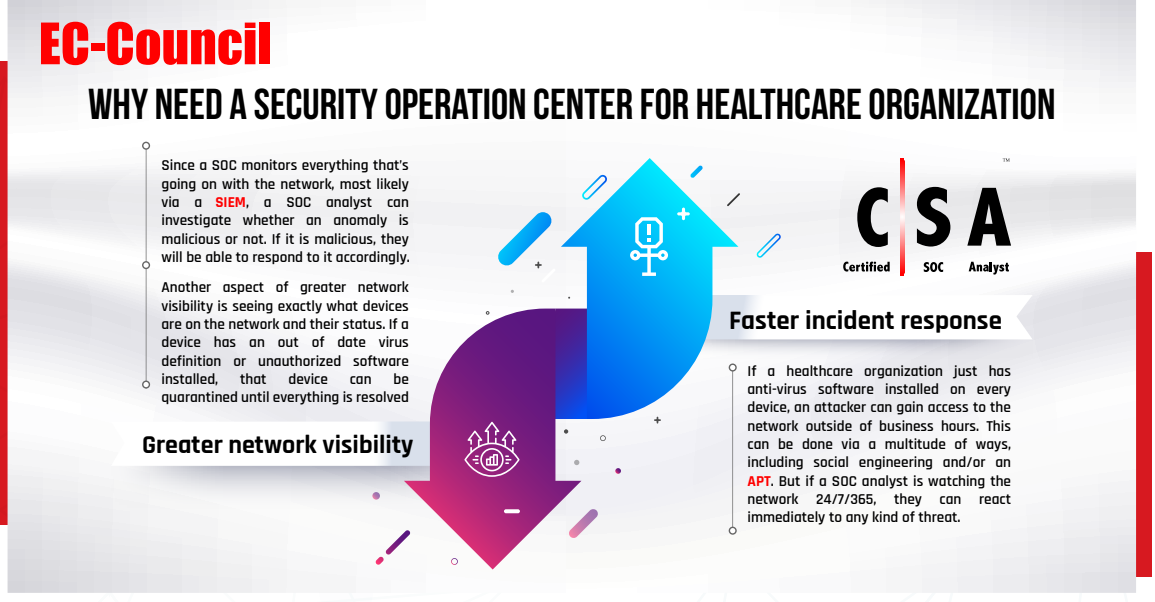
Data protection is a major challenge for organizations working online...

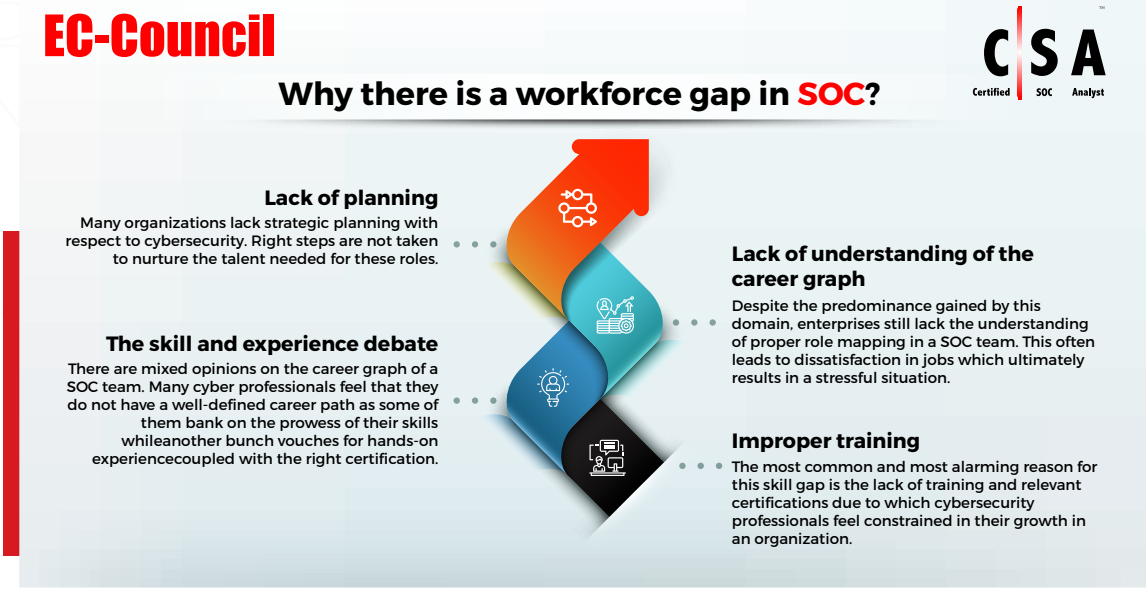
READ MORE

Infographics

WHY DO YOU NEED SECURITY OPERATIONS CENTRE FOR HEALTHCARE ORGANIZATIONS?

READ MORE

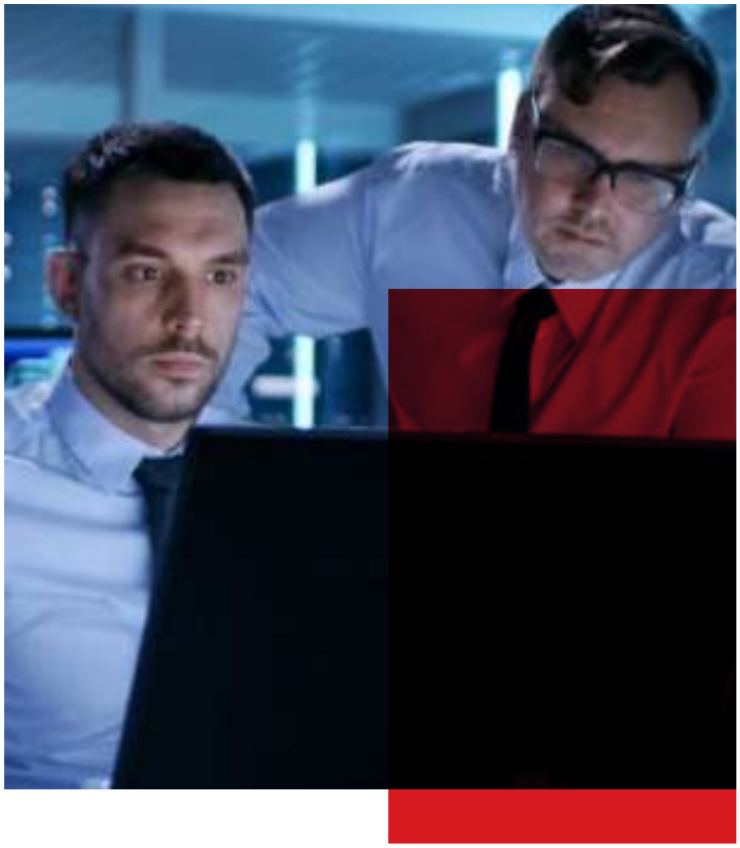




Infographics

WHY THERE IS A WORKFORCE GAPIN SOC

READ MORE



Blog

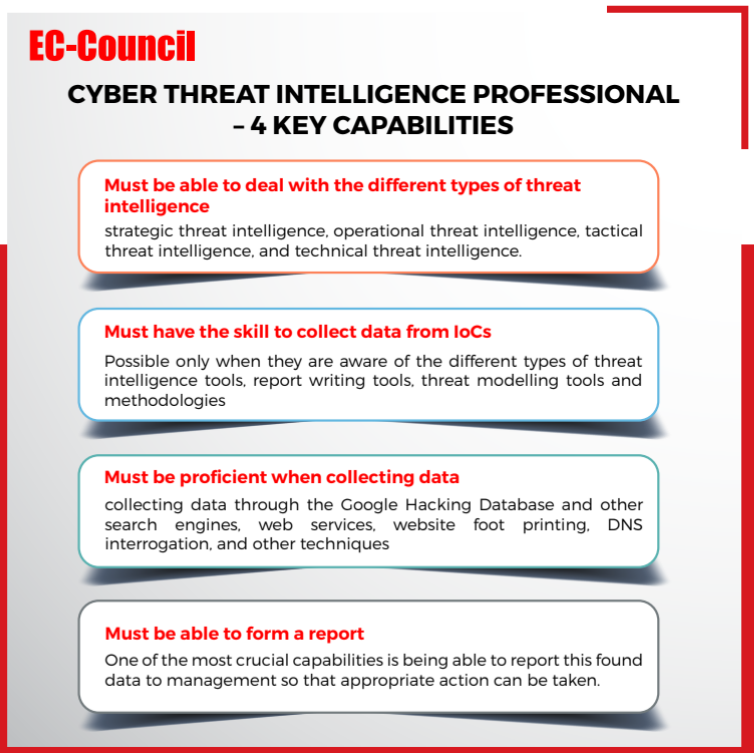
3 PRIMARY ELEMENTS OF A CYBER-SECURITY OPERATIONS CENTER

With so many headlines talking about the rise of cyber threats, it's no surprise that organizations are looking to create Cybersecurity Operations Centers

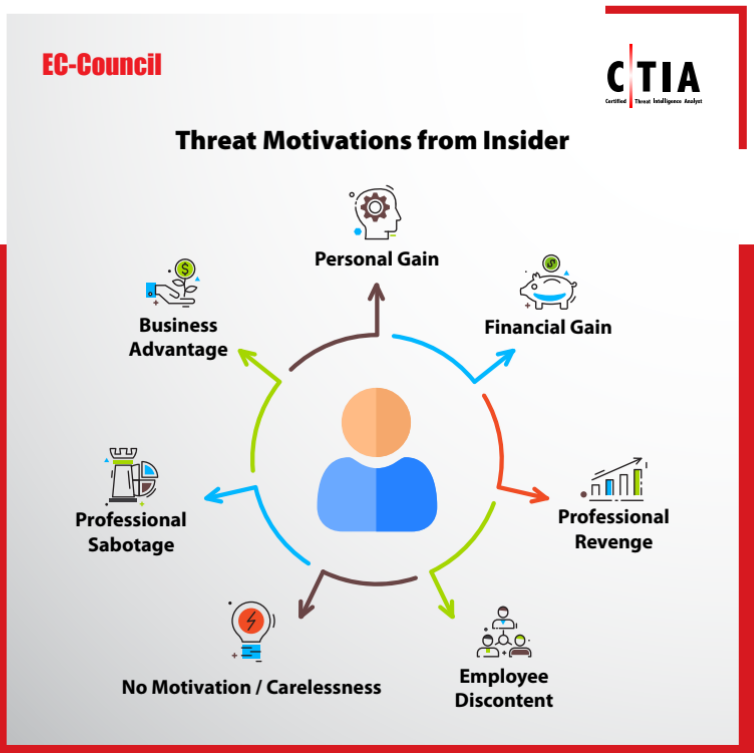
READ MORE

Threat Intelligence Analysts

Infographics



Infographics



CYBER THREAT INTELLIGENCE PROFESSIONALS – 4 KEY CAPABILITIES

READ MORE

COMMON INSIDER THREAT MOTIVATIONS

READ MORE

Slideshare

6 Most Popular Threat Modeling Methodologies

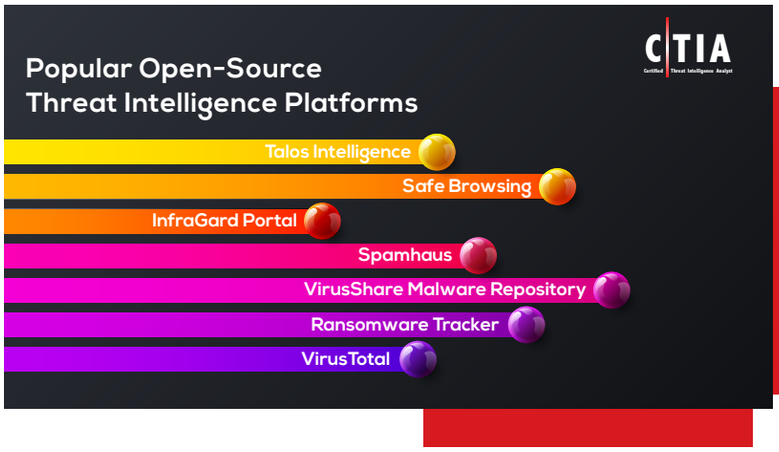
READ MORE

Blog

PROTECT YOUR SECTOR: THE IMPORTANCE OF THREAT SHARING

Essentially, threat intelligence is the compiled data that can be circulated...

READ MORE



Infographics

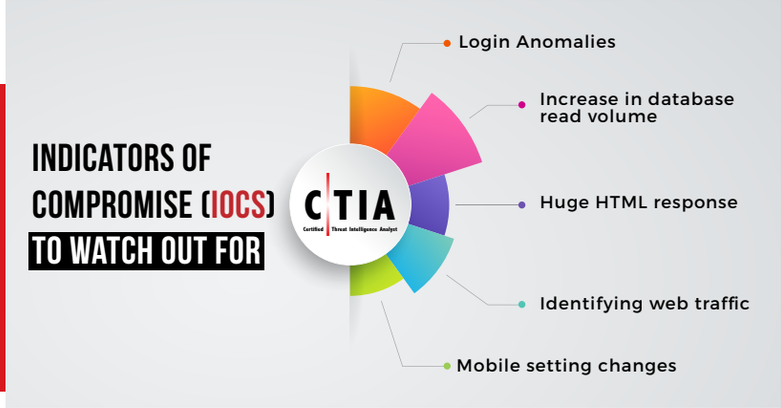
POPULAR OPEN-SOURCE THREAT INTERLLIGENCE PLATFORMS

READ MORE

Infographics

INDICATORS OF COMPROMISE (IOCS)TO WATCH OUT FOR

READ MORE



Forensic Investigators

Slideshare

How to become a Digital Forensics Investigator

READ MORE

Infographics

4 Ways Digital Forensics Helps Solve Cybercrimes

READ MORE

Blog

DO YOU KNOW WHAT IOT FORENSICS IS AND HOW IT

With the introduction of the Internet of Things (IoT)...

READ MORE

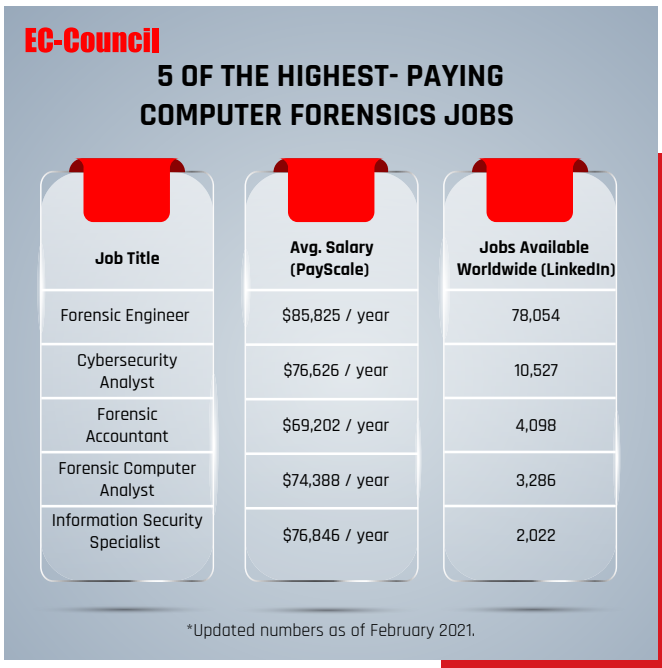
Blog

5 SKILLS YOU NEED TO BECOME A CYBER FORENSICS EXPERT

Does the word "investigation" give you goosebumps?...

READ MORE

Infographics

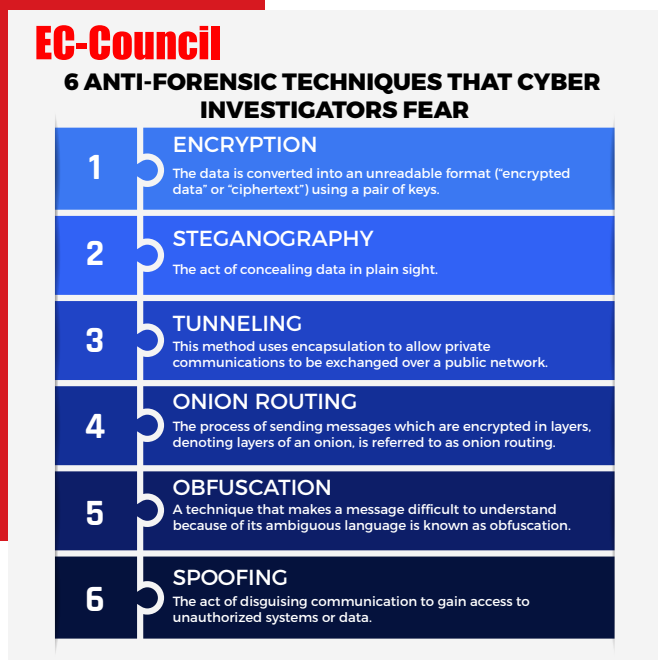


Job Title	Avg. Salary (PayScale)	Jobs Available Worldwide (LinkedIn)
Forensic Engineer	$85,825 / year	78,054
Cybersecurity Analyst	$76,626 / year	10,527
Forensic Accountant	$69,202 / year	4,098
Forensic Computer Analyst	$74,388 / year	3,286
Information Security Specialist	$76,846 / year	2,022

How to become a Digital Forensics Investigator

READ MORE

Infographics



How to become a Digital Forensics Investigator

READ MORE

Network Defenders

Blog

5 REASONS WHY AN IT/NETWORK ADMINISTRATOR SHOULD THINK BEYOND MCSE

IT/network administration has always been...

READ MORE

Blog

3 ADVANTAGES A NETWORK DEFENDER HAS OVER A NETWORK ADMIN

The internet and wireless connectivity have so much...

READ MORE

Blog

5 NETWORK SECURITY BASICS FOR A SAFE REMOTE WORK CULTURE IN 2021

Remote work is a risky affair. While it has proven...

READ MORE

Penetration Tester

Blog

9 SECURITY RISKS THAT WEB APPLICATION PENETRATION TESTING CAN FIX

Website penetration testing is the most secure...

READ MORE

Blog

WHY KNOWLEDGE OF NMAP IS IMPORTANT TO LAND GOOD PENETRATION TESTING JOBS

Penetration testing is one of the most popular career...

READ MORE

Blog

WHY CPENT IS THE MOST COMPREHENSIVE PENETRATION TESTING CERTIFICATION PROGRAM

If there is one practice that businesses have started...

READ MORE

Blog

3 MISTAKES YOU SHOULD AVOID WHILE CREATING A PENETRATION TESTING REPORT

In a world where cybersecurity threats are looming...

READ MORE

Blog

HOW PENETRATION TESTING CERTIFICATION CAN BOOST YOUR CAREER AS AN IT PROFESSIONAL

The last five years have seen an exponential rise...

READ MORE

Whitepaper

HOW TO SECURE YOUR CONTAINERS: A CLOSER LOOK AT DOCKER AND KUBERNETES

Containers technology is currently trending in the...

READ MORE

Ethical Hackers

Blog

INTRODUCTION TO ETHICAL HACKING AND PENETRATION TESTING

The demand for ethical hackers has grown in the last few years...

READ MORE

Blog

PRETEXTING IN CYBERSECURITY: WHY THIS SOCIAL ENGINEERING THREAT IS DANGEROUS

Social engineering attacks have increased as circumstances have changed...

READ MORE

Slideshare

Certified Ethical Hacker CEH v11

READ MORE

Blog

BEST PLATFORMS TO LEARN THE BASICS OF HACKING AND PENETRATION TESTING

5 TIPS TO SELECT THE BEST ETHICAL HACKING TOOLS

CYBERSECURITY THREATS: WHAT ARE DDOS ATTACKS AND HOW CAN YOU AVOID THEM?

Cybersecurity has emerged as one of the...

READ MORE

Ethical hacking has become a popular career...

READ MORE

Cybersecurity threats have become more...

READ MORE

Webinar

Irene Corpuz

Co-founder of the Women in Cyber Security Middle East (WiCSME)

Why Risk Management Techniques Are Important in Ethical Hacking

WATCH NOW

Blockchain Professionals

Blog

4 REASONS WHY DESIGNERS NEED BLOCKCHAIN AND FAST

In the last few years, the blockchain industry has been...

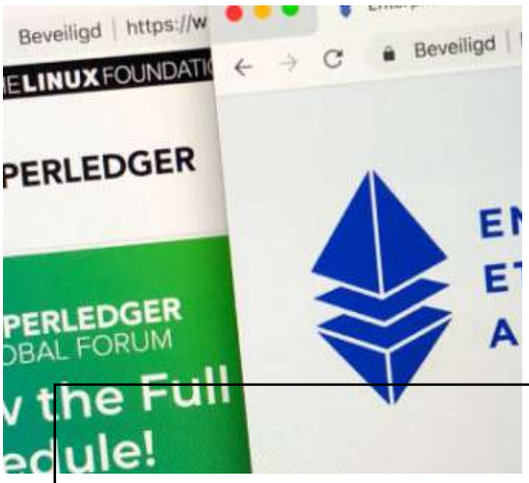
READ MORE

Blog

5 SKILLS THAT YOU NEED TO BECOME A BLOCKCHAIN DEVELOPER

Blockchain technology is gradually revolutionizing...

READ MORE

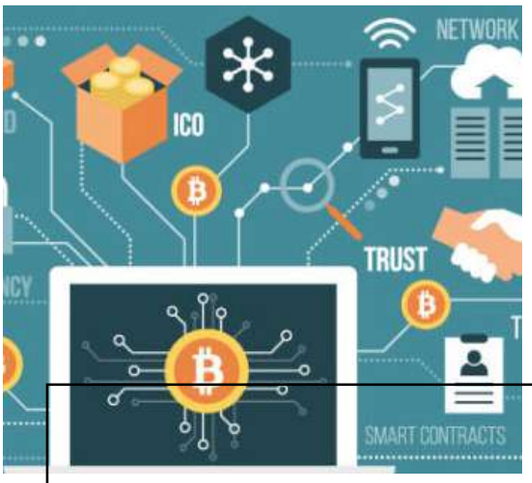


Blog

HYPERLEDGER VS ETHEREUM – WHICH BLOCKCHAIN PLATFORM IS GOOD FOR YOUR BUSINESS?

Blockchain is a revolutionary concept developed...

READ MORE



Blog

TOP 4 BLOCKCHAIN RISKS A CIO SHOULD KNOW

Enterprises in every sector are trying to adopt blockchain...

READ MORE

Blog

DESIGNING FOR BLOCKCHAIN: THE 5 PRINCIPLES YOU NEED TO KNOW

Blockchain is now regarded as

Blog

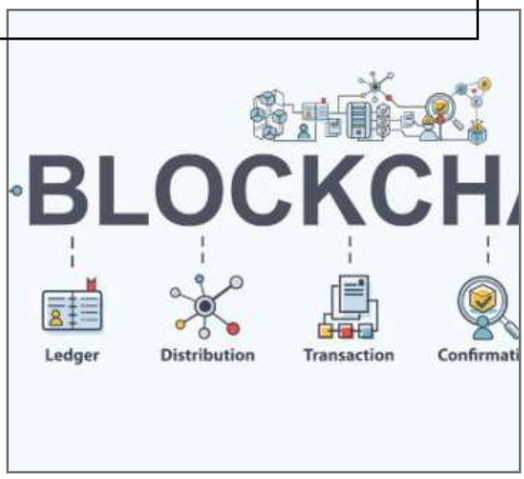
TOP 5 ENTERPRISE BLOCKCHAIN PROTOCOLS YOU NEED TO KNOW

Blockchain technology has serious stuff...

READ MORE

reached a milestone...

READ MORE



Whitepaper

HOW BLOCKCHAIN MAKES IOT MORE SECURE

IoT technology is increasingly connecting multiple...

READ MORE

Whitepaper

WHAT ARE FORKS AND COORDINATION IN BLOCKCHAIN?

Blockchain is a continuously developing technology...

READ MORE

CISO MAG Interviews

Interviews

Don't be afraid to ask about opportunities; fortune favors the bold

READ MORE

Interviews

Never let anyone have you think that you cannot achieve something because you are a woman

READ MORE

Interviews

Empowering Marginalized Voices in a Digital World

READ MORE

Interviews

I personally believe girls are naturally blessed analysts and can make great research scholars

READ MORE

News

WhatsApp Trialing Encrypted Chat Backups?

WhatsApp has been feeling the heat of governments...

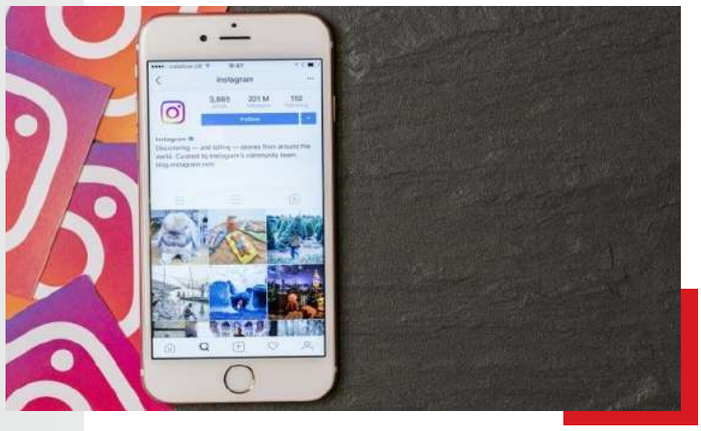
READ MORE

News

Wait! Read This Before You Post a Story on Instagram

Instagram is currently hands-down one of the most popular...

READ MORE



News

The Pandemic-hit World Witnessed a 150% Growth of Ransomware

READ MORE

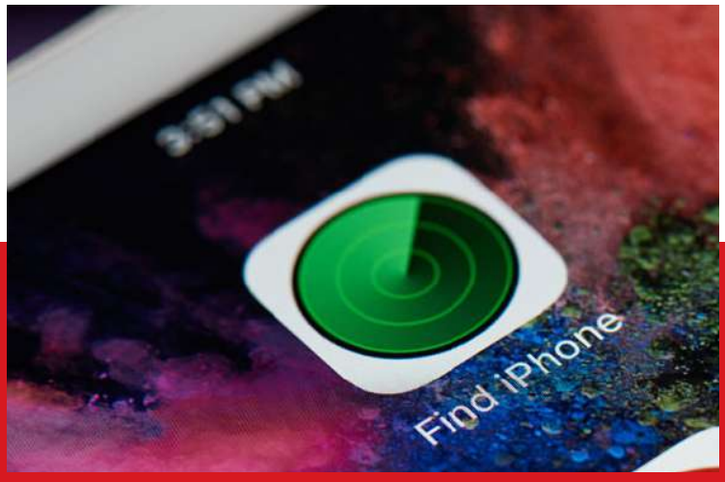
News

Is Google reCAPTCHA Really Secure?

Several cybersecurity experts have reported an increase...

READ MORE

News



iOS Call Recording App Allowed Snooping-in on Users Conversations

Researchers found a security vulnerability in the iOS...

READ MORE

News

NimzaLoader: Malware Written in Rare Programming Language

Security experts uncovered a new kind of phishing campaign in which threat...

READ MORE

News

Smart City Project in India Receives a Ransomware Jolt

Based on an IBM security report, India had recently gained...

READ MORE

Operation Diànxùn: Chinese Cyber Espionage Campaign Targeting 5G Operators

Cybersecurity experts discovered a cyber espionage campaign targeting telecom...

READ MORE

News

News

Indian Transport Sector on Hackers' Radar; CERT-In Warns

As a country with the second-largest population and the third-largest economy...

READ MORE

Mamba Ransomware is Weaponizing DiskCryptor: FBI

The FBI is warning users and organizations about the Mamba ransomware...

READ MORE

News

ECCU

EC-Council Foundation Fellowship (ECCFF)

An openhanded tuition assistance for students pursuing a Bachelor of Science in Cyber Security (BSCS) or a Master of Science in Cyber Security (MSCS) with a minimum of 3.5 GPA.

LEARN MORE

President's Scholarship for Women in Cybersecurity

A women-oriented program that financially assists female undergraduate and graduate students to complete their education.

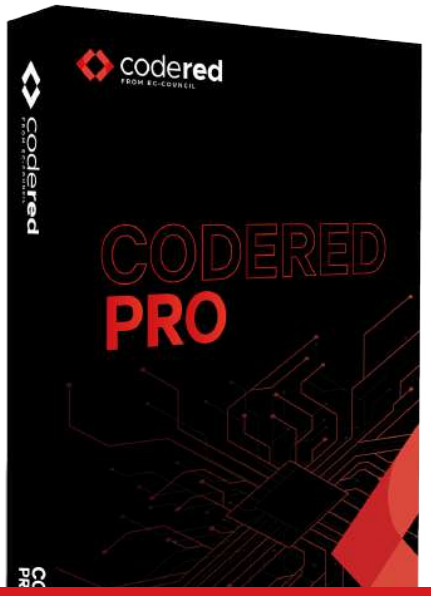
LEARN MORE

CodeRed v2: The Experience Keeps Getting Better and Better

Enhance your learning experience and truly take your career to the next level with our latest features!

Library: Access over 150+ courses based on your preferences.

READ MORE



Pro: Gain unlimited access to our premium courses.

READ MORE

Bundles: Pre-curated bundles created by our expert content team.

READ MORE

Microdegrees: 200+ hours of premium videos and labs.

READ MORE

START YOUR LEARNING JOURNEY NOW!

Brought to You by EC-Council