Jump-start Your SOC Analyst Career

A Roadmap to Cybersecurity Success

—

Second Edition

—

Tyler Wall
Jarrett Rodrick

Foreword by Stephen Northcutt, Founder of SANS Technology Institute and GIAC Certifications

Apress®

Jump-start Your SOC Analyst Career

A Roadmap to Cybersecurity Success

Second Edition

Tyler Wall
Jarrett Rodrick

Foreword by Stephen Northcutt, Founder of SANS Technology Institute and GIAC Certifications

Apress®

Jump-start Your SOC Analyst Career: A Roadmap to Cybersecurity Success, Second Edition

Tyler Wall
Cumming, GA, USA

Jarrett Rodrick
Melissa, TX, USA

ISBN-13 (pbk): 979-8-8688-0344-4
ISBN-13 (electronic): 979-8-8688-0345-1
https://doi.org/10.1007/979-8-8688-0345-1

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Project Manager: Jessica Vakili

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, Suite 4600, New York, NY 10004-1562, USA. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

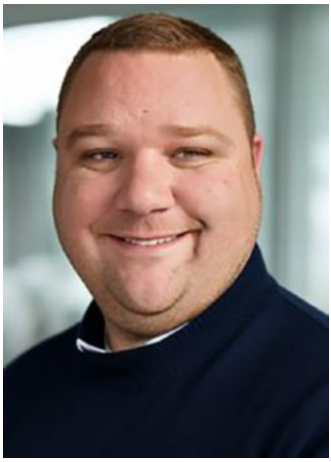
Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub. For more detailed information, please visit https://www.apress.com/gp/services/source-code.

If disposing of this product, please recycle the paper

This book is dedicated to our wives, Heidi and Stacey.

Table of Contents

About the Author

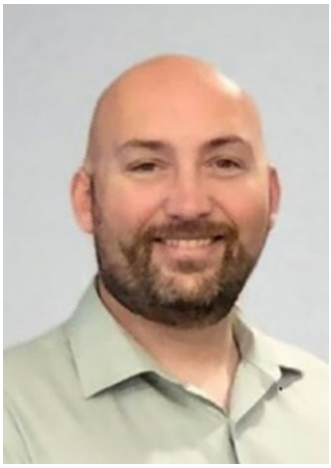


Tyler Wall is CEO of Cyber NOW Education, which specializes in global cybersecurity training and certification that's accessible and affordable. He is an accomplished security professional with a decade of experience in security operations at some of the world's largest corporations.

Tyler's education includes Master of Science in Cybersecurity Management from Purdue University, CISSP, CEH, CSSK, Terraform Associate, CFSR, LRPA, Security+, Network+, and A+.

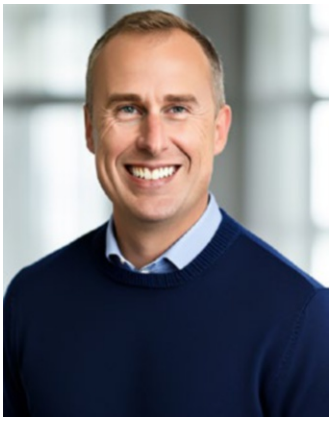
He enjoys spending time with his son and being creative.

About the Coauthor



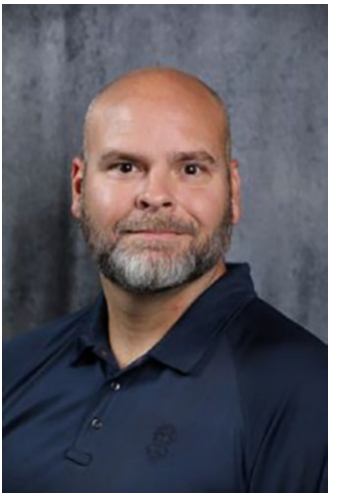
Jarrett Rodrick is the Senior Manager of Security Operations at Omnissa and was formerly the Senior Manager of the Security Operation Center at VMware. He is a retired Cyber Network Defender and Cyber Warfare Specialist from the US Army and has over eleven years of Defensive Cyber Operations experience between US Army Cyber Command and leading world-class security programs at Fortune 100 companies. Jarrett's education includes a Bachelor of Science in Applied Cybersecurity from SANS Technology Institute and 17 GIAC cybersecurity certifications. Jarrett lives in Melissa, Texas, and enjoys golfing with his son and board games with his family.

About the Contributing Authors



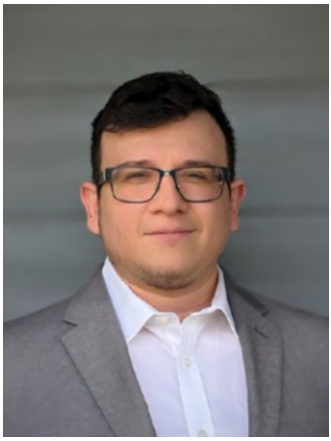
Matthew Peterson is an aspiring SOC analyst with over ten years of experience in financial services and a rich background in software development, AI, and graphic design. He holds a master's degree in Global Management from the Thunderbird School of Global Management and a graduate certificate from the Pacific Coast Banking School. In this book, Matthew has channeled his expertise into creating the graphical theme and authoring Chapter 6, "SOC in the Clouds," where he excels at translating complex technical concepts into clear, engaging visuals and storytelling.

Residing in Scottsdale, Arizona, Matthew enjoys spending quality time playing baseball with his boys, balancing his professional achievements with family life.



Jason Tunis is the Manager of Security Automation at the world's largest credit union. He spends his time focused primarily on security and fraud incident response, threat intelligence, and security automation and orchestration. Jason is a seasoned cyber security professional with over 15 years of experience, and his certifications include CISSP and GSLC. He lives in the Midwest with his wife and three children.

About the Technical Reviewer



Before **Zach Garcia** started his career in cybersecurity, it was just his hobby. He has always been curious about how things work and loves to think creatively about interesting ways to improve security (…sometimes by breaking it).

His career has taken him across the spectrum: from Digital Forensics, Incident Response (IR) roles, and reverse engineering malware to writing malware and penetration testing across a number of sectors. Unquenchable curiosity combined with his love for puzzles and people are what fuel his passion for the industry. In Zach's spare time he likes to garden, spend time with family, and hack every smart device he can get his hands on.

Acknowledgments

First, I would like to acknowledge my wife, Heidi Wall, for loving me unconditionally. I would also like to acknowledge my mom, Karen Hodges, for reading to me as a young child and being the light of education in my life along with my late grandmother Viriginia Gross Stebbins. I would like to acknowledge Matthew Peterson, aspiring SOC analyst (Phoenix, AZ), for his wonderful work for the graphics in this book. All the graphics in the book are custom designed by him. I would like to acknowledge Zach Garcia, my former manager, who has been in my corner since the day I met him and joined this project to become the technical reviewer. He caught a lot of things I missed during the review. I would like to acknowledge all the SOC story writers, and may their career be fulfilling and become an inspiration to others all around the world. I would like to acknowledge Michael Archuleta, videographer, for his tiresome work at Cyber NOW Education and for helping to bring Cyber NOW Education into the light.

—Tyler Wall

First and most important, I'd like to thank my beautiful and loving wife, Stacey. Your constant supply of love and patience has provided me with the needed support to become the cyber professional I am today. Thank you! I'd also like to thank the countless Soldiers and Army Leaders I've had the pleasure to learn from in my 16-year career. From my Drill Sergeants at Fort Knox to the Senior Officers at the Cyber Protection Brigade, you've all played a pivotal role in my development. Thank you! Finally, I'd like to thank VMware, for taking a chance on a soon-to-retire Soldier and offering me a career outside of the Army. I truly couldn't have asked for a better company to work for. Thank you!

—Jarrett Rodrick

Foreword by Stephen Northcutt, Founder of the SANS Technology Institute and GIAC Certifications

The Security Operations Center, SOC, detects, analyzes, and responds to cybersecurity adverse events in as close to real time as possible and they do it 24 hours a day, every day. That is a daunting challenge requiring resources, management, and solid process. And there is no point setting off down that path unless you understand the mission and vision which leads to the significance and relevance of this book. In its pages, we learn what a SOC is, how it works, why it is important, and how to enter the field. In today's digital landscape, where threats lurk around every virtual corner, the SOC stands as a bastion of defense, responsible for monitoring, investigating, triage, and remediating adverse security events.

Tyler and Jarrett have the knowledge, experience, and the passion to delve into the depths of this vital organizational security component and understand the pivotal role it plays within organizations. Whether it operates internally or outsourced to Managed Security Services Providers (MSSPs), the SOC has the critical task of safeguarding digital assets against an ever-evolving array of cyber threats.

Throughout this book, the authors unravel the intricacies of SOC operations, exploring how its scope of responsibility varies based on staffing models. The authors provide all the foundational information, even if you are completely new to cybersecurity. If you find yourself

saying, "I've seen that before," be certain to take the quizzes at the back of the chapter to distinguish "you have seen it" from "yes, you know it." From the elevated privileges of internal SOCs, empowering swift remedial actions during incidents, to the diligent oversight maintained by MSSPs over multiple enterprise networks, each SOC approach carries its distinct advantages and challenges.

They thoroughly cover the cloud-based Security Operations Center (SOC) as well as how it plays a vital role in addressing the inherent security risks associated with cloud computing. Recognizing these risks is crucial for developing effective mitigation strategies to safeguard your data in the cloud. Despite the clear benefits of cloud computing, such as scalability and flexibility, it would not be wise to embrace cloud adoption without a thorough understanding of the associated security risks.

A cloud-based SOC leverages advanced technologies and monitoring capabilities to detect and respond to security threats in real-time, ensuring the protection of sensitive data and critical assets. By centralizing security operations in the cloud, organizations can enhance visibility, streamline incident response processes, and maintain compliance with regulatory requirements. Furthermore, a cloud-based SOC enables proactive threat hunting and continuous monitoring, empowering organizations to stay ahead of evolving cyber threats and mitigate risks effectively.

You can't read an article about technology without hearing about AI, but cloud-based solutions are where digital assistants are going to be developed first and fastest. If you are not in a cloud solution, the authors clearly have experience in using general-purpose LLM tools to increase the capability of a local SOC and provide tips and examples.

One of the most valuable takeaways from the book is the chapter on analysis: How do you teach people how to solve problems they have never seen before? You have to lay out a process or methodology and walk them through it and you are going to see that unfold for you. This model is the result of countless hours of doing analysis under time pressure.

It was clear to me after reading the book, the authors want you to succeed. The information is there and it is clearly and carefully explained. I hope you enjoy the journey.

Godspeed, S.

Introduction

Welcome to the wonderful world of *Jump-start Your SOC Analyst Career*! You picked this book up because you want to get into the action! Into the money! Into the challenges that lie ahead! We will tell you how wonderful and rewarding this career is, but first let us say something about infosec. If you get into the cybersecurity industry and you aren't connected to the community, you are missing out. There are all kinds of micro infosec communities and communities for special groups of people, but in contrast, there are communities that want to include everyone. There are extremely esoteric communities filled with mystery and secrets, there are communities for just CISOs and communities for just engineers, there is a military community, communities for the government sector, a community of breakers and makers alike… if there is only one common trait that people coming into security want, it is a sense of community – and infosec has it! It is really hard to relate to people in the normal world sometimes, especially if you are starting out and keyboarding alone. We promise you there are many other people that want to keyboard alone next to you. It happens all the time at conferences! There are so many amazing people in the community, and sometimes they don't always get along, but in 3–6 months, it will be like it never happened. Our goal for this book is to get you in the chair in the SOC you dream about and open your eyes that no matter who you are, cybersecurity is for you.

This book will cover what you need to know that we have deemed to be important to know as a SOC analyst. There are a lot of open jobs in cybersecurity, but there are also a lot of candidates that want those jobs. The challenge is that there are not a lot of the right kind of candidates to fill them. We explain to you what the right kind of candidate is and give you

the knowledge to prepare you for interviews. We can't promise to take you from technical zero to hero in the pages of this book. As an author, I want you to trust me, and I will tell you how to be successful with this book, but you need to have a baseline of technical skills. Ideally by the point you pick up this book, you will have been learning IT skills for a while. The combined contributions of the creators of this book, Tyler Wall and Jarrett Rodrick, and chapter authors Matthew Peterson and Jason Tunis, are orchestrated to give you, the reader, the advantage. Ending this book are six stories from people who have traversed the path of a SOC analyst.

The roadmap to cybersecurity success is long, and it's not an easy road at times. It isn't a straight vertical path for some either. It winds, it narrows, and it goes all over the place. To be successful in cybersecurity can mean a lot of things to a lot of people. For some, that might mean holding the torch and power of a CISO, but if you really think hard about that path, it may not make sense for you. There are technical professionals that make more than a CISO, and their jobs are much more stable. Their heads aren't on a chopping block every time something goes bad. That is not to say that being a CISO and leading a security team isn't rewarding; I just illustrate the example to explain that paths and end goals are different from geek to geek according to personal aspirations, but the very first step to a rewarding career is always the same: getting a foot into this industry. Out of all the steps in cybersecurity, it is the most important. The foundation of a cybersecurity career can happen in the very first year as a SOC analyst. The first year as a SOC analyst is very overwhelming, and like drinking through a fire hose, expect to be satisfied but extremely uncomfortable. What is in this book will help you start your career as a SOC analyst and empower you to launch on day one.

Get ready for a rewarding career in cybersecurity…, and on day one, pick a good chair.

To the reader:

This book includes a free certification by passing an exam on the topics covered in this book. Once you are finished with this book, visit this website and take the JYSAC exam:

www.cybernoweducation.com/challenge-page/jysac-exam

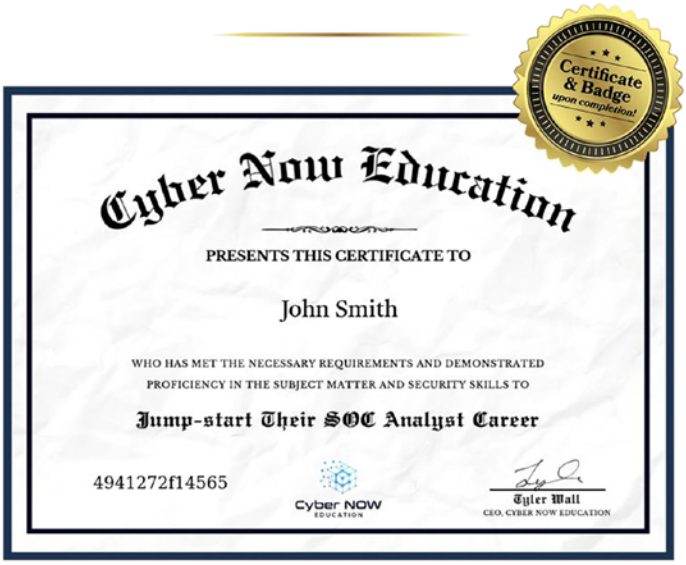
If you successfully pass the exam, fill out the form to receive your certificate:

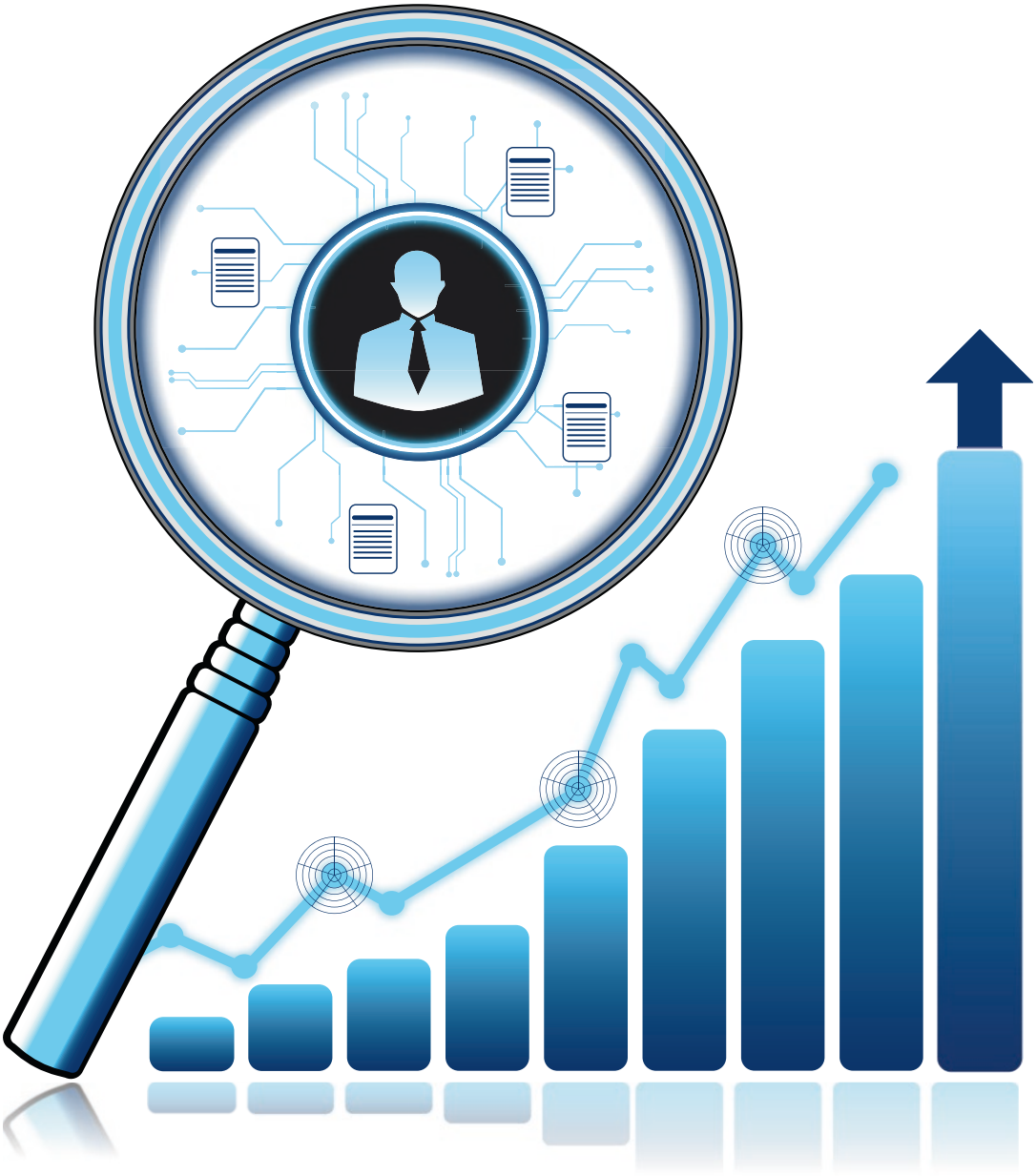
www.cybernoweducation.com/credentials

A team member from **Cyber NOW Education** will review your exam and a certificate will be awarded to you to share on your social media channels. It's a great way to clearly let everyone know your intentions to break into this challenging career no matter the obstacles.

Are you ready to Jump-start Your SOC Analyst Career?

Good luck and have fun with it.
Tyler Wall, MSc., CISSP, CEH, CFSR, CCSK, LRPA, Sec+, Net+, A+
tyler@cybernoweducation.com





CHAPTER 1

The Demand for Cybersecurity and SOC Analysts

In this chapter, we'll discuss the demand for cybersecurity professionals at three different levels, starting with the demand for cybersecurity workers, then address the demand for cybersecurity analysts, and finally, the demand for security operations center (SOC) analysts.

Cybersecurity During a Crisis

Early in 2020, the world began suffering from a viral pandemic known as COVID-19. The world shut down, and people were ordered to shelter in place in their homes. Many jobs were lost or furloughed until the quarantine was lifted, but many employers were able to transition to a "work from home" structure. As a result, Internet service providers saw long and enduring spikes in traffic, and the demand for videoconferencing soared to new heights. The United States Department of Homeland Security designated cybersecurity personnel as an essential workforce for continued infrastructure viability, and the need for cybersecurity workers

T. Wall and J. Rodrick, *Jump-start Your SOC Analyst Career*,
https://doi.org/10.1007/979-8-8688-0345-1_1

was higher than ever. During this period, there was already a shortage of nearly 500,000 cybersecurity jobs in the United States alone, and the industry needed to grow by 62% to meet the demand.[1]

Having a current shortage in the cybersecurity workforce combined with a crisis such as the COVID-19 pandemic, a cyberwar, or any other emergency increases the demand for cybersecurity workers. The shortage of cyber workers gets even worse, and the cybersecurity workforce is drained even further. There is no solution but to work longer and harder. Cybersecurity workers' physical and mental health takes a toll as the stress and hours worked increase. There is no fast fix or solution for training new cybersecurity workers, so the result is an extra-taxed workforce.

During the COVID-19 pandemic, the world rushed to continue to be productive while working at home. While the US government shut down businesses everywhere except those deemed as "essential" for some time, cybersecurity was one of these professions considered essential, and the already high demand for skilled workers grew overnight.[2]

What did the industry learn from the pandemic? COVID-19 proved that a vast workforce could be productive while working remotely. For years, US companies have taken steps to be more environmentally friendly. Whether it's sustainable power for their warehouses, recycling programs, or alternative fuel for delivery vehicles, thousands of companies are embracing sustainable resources around the world. Now that an at-home workforce was feasible, companies embraced this as an opportunity to decrease greenhouse emissions, increase employee happiness… and, you know, reduce operational costs. Since then, working from home has become a part of life for some SOC Analysts.

[1] www.isc2.org/Research/Workforce-Study

[2] https://workingnation.com/covid-19-cybersecurity-and-it-workers-are-essential-in-demand-employees/

This does not guarantee that all companies have embraced the benefits of working from home. According to a study done near the end of 2023 by JLL,[3] employees of Fortune 100 companies work an average of 2.96 days in the office per week. This is the hybrid model, and many companies are adopting it as their new norm post COVID-19.

Demand for Cybersecurity Analysts

Today, we find ourselves in a global cyberwar. Every industry, in every country, is actively targeted by cyber criminals, state-sponsored hackers, and companies engaging in corporate espionage. That might sound like the plot to a low-budget movie starring your favorite 1990s action star, but the truth is everyone's a target. Even more troubling is the fact that it didn't start with COVID-19; this has been going on for decades. It's only been in the last ten years that companies have identified the need for higher investments in cybersecurity.

High-profile compromises have served a hard lesson for industries globally. In November 2014, Sony Pictures Entertainment announced they were the victim of a data breach. Analysts from *Reuters.com* estimated the compromise would cost Sony more than $75 million in recovery costs and lost revenue. The Capital One breach in August 2019 resulted in the theft of 100 million consumer credit applications. Attacks like these two have driven home the requirement for a dedicated cybersecurity workforce.

In fact, according to the US Bureau of Labor Statistics, the Information Security Analyst occupation is projected to grow 32% from 2022 to 2023 in the United States, compared to 12% growth for other computer-related

[3] www.us.jll.com/en/trends-and-insights/research/office-market-statistics-tren

occupations and 0.3% total growth for all occupations.[4] One significant benefit for those considering a move into cybersecurity is the relatively low bar for entry into the career field.

For decades the narrative has been "Go to college, earn a 4-year degree, get a career." This book will dedicate a chapter (Chapter 10) to covering the different entry paths into cybersecurity analyst positions. But for now, know that college is not the only path into a great career, and some high-level degree programs are a waste of time and money completely for an entry-level role.

When companies embrace the need for cybersecurity, it usually begins with the Security Operations Center or SOC for short. The SOC is responsible for triage, investigation, and response to cybersecurity incidents. This concept is not new. Military and law enforcement agencies have been using Tactical Operations Centers to coordinate operations during conflicts for decades. And like the TOC, the SOC serves as the Command and Control hub for first responders to cybersecurity incidents.

ds

Definition A cybersecurity incident is an adverse network event in an information system or network or the threat of the occurrence of such an event according to the SANS institute.[5]

The SOC isn't the only team dedicated to responding to cybersecurity incidents. Many companies have dedicated Digital Forensics and Incident Response teams to support the SOC in investigations and response.

[4] www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[5] www.sans.org/security-resources/glossary-of-terms