MGT551: **Building and Leading Security Operations Centers**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Collect the most important logs and network data
- Create playbooks and use cases
- Use threat intelligence to focus your budget and detection efforts
- Implement threat hunting and active defense strategies
- Develop efficient alert triage and investigation workflow
- Create effective incident response processes
- Implement metrics and goals to improve the SOC
- Conduct effective team member hiring, training, and retention, and prevent burnout
- Assess your SOC through purple team testing and adversary emulation

"This is a great management course for both those in start-up SOCs as well as established SOCs. As a newer leader myself, I found a lot of value in the leadership training as well."

—Joel Kociemba, **Bechtel**

Information technology is so tightly woven into the fabric of modern business that cyber risk has become business risk. SOC teams are facing more pressure than ever before to help manage this risk by identifying and responding to threats across a diverse set of infrastructures, business processes, and users. Furthermore, SOC managers are in the unique position of having to bridge the gap between business processes and the highly technical work that goes on in the SOC. Managers must show alignment to the business and demonstrate real value - a challenge when the threats are constantly changing and sometimes unseen. How do we know our security teams are aligned to the unique threats facing our organization? How do we get consistent results and prove that we can identify and respond to threats in time to minimize business impact? And how can we build an empowering, learning environment where analysts can be creative and solve problems while focusing on the mission at hand?

MGT551 bridges this gap by giving students the technical means to build an effective defense and the management tools to build an effective team. From section one of this training, students will learn how to design their defenses around their unique organizational requirements and risk profile. They will learn how to combine SOC staff, processes, and technology in a way that promotes measurable results and covers all manner of infrastructure and business processes. Most importantly, they will learn how to keep the SOC growing, evolving, and improving over time.

Throughout this course, students can expect to learn key factors for success in managing a Security Operations Center (SOC), including:

- Collecting the most important logs and network data
- Building, training, and empowering a diverse team
- Creating playbooks and managing detection use cases
- Using threat intelligence to focus your budget and detection efforts
- Threat hunting and active defense strategies
- Efficient alert triage and investigation workflow
- Incident response planning and execution
- Choosing metrics and long-term strategy to improve the SOC
- Team member training, retention, and prevention of burnout
- SOC assessment through capacity planning, purple team testing, and adversary emulation

Section Descriptions

SECTION 1: SOC Design and Operational Planning

MGT551 starts with the critical elements necessary to build your Security Operations Center: understanding your enemies, planning your requirements, making a physical space, building your team, and deploying a core toolset. Throughout this course section, students will learn how to build a strong foundation upon which an SOC can operate, focusing first on the most important users and data, and tailoring defense plans to threats most likely to impact your organization. Through workflow optimization, information organization, and data collection, you will learn how to ensure that your security operations will hit the ground running as efficiently as possible while protecting privileged SOC users and data. Exercises show how to implement these concepts through threat group and asset profiling, mapping likely attack paths into your environment, and implementing use cases repeatable playbooks to identify the threats and attack vectors you have identified.

TOPICS: Introduction; SOC Functions; SOC Planning; Team Creation, Hiring, and Training; Building the SOC; SOC Tools and Technology; SOC Enclave and Networking

SECTION 2: SOC Telemetry and Analysis

Section 2 of MGT551 focuses on expanding our understanding of attacker tactics, techniques, and procedures and how we might identify them in our environment. We will discuss defensive theory and mental models that can guide our assessment and planning efforts, data collection and monitoring priorities, and cyber threat intelligence collection. We will also cover more specialized security monitoring use cases like DevOps, supply chain, insider threat, and business e-mail compromise. Exercises include using the MITRE ATT&CK framework to plan security data collection and writing solid threat intelligence requirements for relevant, timely information that answers your most pressing defensive questions.

TOPICS: Cyber Defense Theory and Mental Models; Prevention and the Future of Security; SOC Data Collection; Other Monitoring Use Case; Using MITRE ATT&CK to Plan Collection; Cyber Threat Intelligence; Practical Collection Concerns

SECTION 3: Attack Detection, Hunting, and Triage

Section 3 of MGT551 is all about improving detections. We begin with effective triage and analysis and then move to more effective alerting mechanisms, starting with the fundamentals of analytic design. We will discuss detection engineering as a core SOC discipline to be planned, tracked, and measured. You will learn a repeatable, data-driven approach to SOC capacity planning and apply that process in a hands-on exercise using custom tools that you can take back to your own environment. We will also cover the different types of proactive threat hunting, see a structured approach that results in measurable improvements to your detection capability, and apply that approach in a hands-on threat hunting lab. Finally, we will look at active defense concepts and their role in a mature security operations capability. Taking the tools, processes, and concepts from Section 3 of MGT551 back to your SOC will ensure that no (virtual) stone in your environment remains unturned.

TOPICS: Efficient Alert Triage; Capacity Planning; Detection Engineering; Analytic and Analysis Frameworks and Tools; Threat Hunting; Active Defense

SECTION 4: Incident Response

From toolsets to proven frameworks to tips and tricks learned in countless real-world scenarios, section four covers the full response cycle, from preparation to identification to containment, eradication, and recovery, for operations managers. The fourth section of MGT551 begins with the fundamentals of investigation: effective triage, investigative mindset, and tools for avoiding bias. Then the focus turns to preparing your environment to be defended by deploying security controls, identifying high-value assets and users, and designing playbooks to guide your response efforts. Finally, we will review best of breed incident response tools and free frameworks to guide your planning. Lab exercises in section four include incident response playbook design using the free RE&CT framework, investigation review and quality control, and tabletop exercise development.

TOPICS: Incident Response (IR) Planning; Preparation; Identification, Containment, and Eradication; Recovery and Post-Incident; Incident Response in the Cloud; Dealing with a Breach; IR Tools; Continuous Improvement

SECTION 5: Metrics, Automation, and Continuous Improvement

The fifth and final section of MGT551 is all about measuring and improving security operations. We focus on three areas: developing and improving people, measuring SOC performance, and continuous validation through assessment and adversary emulation. We will also cover some of the more challenging elements of managing people in a dynamic and often high-pressure environment: building the right culture, addressing damaging behaviors, and handling common pitfalls of daily operations. By demonstrating value through structured testing and fostering a culture of learning, collaboration, and continuous improvement, we can ensure long term growth and success. In section five, you ll receive the tools, techniques, and insights to do just that. Hands-on exercises will include building skills self-assessments and training plans for your analysts, designing SOC metrics, and continuous assessment and validation.

TOPICS: Staff Retention and Mitigation of Burnout; Metrics, Goals, and Effective Execution; Measurement and Prioritization Issues; Strategic Planning and Communications; Analytic Testing and Adversary Emulation; Automation and Analyst Engagement

Who Should Attend

This course is intended for those who are looking to build a Security Operations Center for the first time or improve the one their organization is already running.

Ideal student job roles for this course include:

- Security Operations Center managers or leads
- Security directors
- New Security Operations team members
- Lead/senior SOC analysts
- Technical CISOs and security directors

"Directly applicable content and I have written down so many ideas."

—Garry Byrne, **Tesco Plc**

"I would recommend this course to anyone running a security operations team. I'd further recommend it to more experienced analysts so they can begin to see the bigger picture."

—Robert Wilson,
University of South Carolina