




Enhancing DoD OSINT Capabilities Through Comprehensive SANS Training and Expertise

January 2025



SANS | **GIAC**
CERTIFICATIONS





We at the SANS Institute greatly commend the Department of Defense's forward-thinking OSINT Strategy for 2024–2028 and the pivotal role it will play in advancing national security and intelligence operations. As a global leader in cybersecurity training and certifications, SANS stands ready to provide tailored training solutions and support to enhance the skills and capabilities of your OSINT teams. On the following pages, we detail how SANS courses and programs can directly align with and advance each of the strategic goals laid out in the OSINT strategy.

STRATEGIC GOAL 1: Enhance Decision-Maker and Warfighter Situational Awareness

The goal of providing timely and customized OSINT products and data for decision-makers and warfighters is critical for maintaining operational superiority. To meet this goal, SANS offers cutting-edge courses that equip intelligence professionals with the skills to collect, analyze, and disseminate actionable intelligence at scale.

Integrating Advanced Technologies into OSINT Workflows

AIS247: AI Security Essentials for Business Leaders™ and

SEC595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™

These courses will train your OSINT professionals on how to harness the power of artificial intelligence (AI) and machine learning (ML) to automate and scale OSINT collection, processing, and reporting. By leveraging these capabilities, DoD OSINT teams can sift through vast quantities of open-source data, identifying relevant intelligence and generating insights in real time, a key objective outlined in the OSINT strategy.

SEC573: Automating Information Security with Python™

This course provides practical programming skills that allow OSINT professionals to automate repetitive tasks, including the gathering and processing of OSINT data from various open sources, enhancing efficiency and reducing the time needed for manual analysis.

Data-Centric Operations and Timely Reporting

SANS courses such as **FOR578: Cyber Threat Intelligence™**

This course offer hands-on experience in gathering OSINT and transforming it into threat intelligence products that can be rapidly disseminated to decision-makers through collaboration with analysts/targeting organizations; producing timely, fused, all-sourced intelligence. This aligns with the strategy's emphasis on delivering customized, serialized OSINT products to support the rapid decision-making needs of military and intelligence leaders, while empowering cyber operations conducted within and outside the intelligence community.

STRATEGIC GOAL 2: Maximize the Intelligence Value of Open Source Information

One of the key challenges highlighted in the strategy is maximizing the intelligence value of open-source information through advanced analysis, sharing, and collaboration across disciplines. SANS provides a comprehensive suite of training that focuses on both the technical skills and methodologies required to extract maximum value from OSINT.

Developing Hybrid, Multi-Disciplinary Teams

SEC497: Practical Open-Source Intelligence (OSINT)™ and
SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™

These courses are tailored to equip intelligence analysts with both foundational and advanced OSINT gathering and analysis techniques as well as provide hands-on experience utilizing AI throughout the intelligence cycle. Trainees will learn to harvest critical data from a wide array of open-source platforms, analyze it effectively, and develop intelligence reports that inform and guide decision-making processes across intelligence disciplines. This course empowers the mission force with detailed knowledge of full-spectrum cyberspace operations and furthers the understanding of cyber intelligence/information collection capabilities and repositories.

FOR578: Cyber Threat Intelligence™

This course provides a deep dive into integrating OSINT with other intelligence streams (such as signals intelligence or geospatial intelligence), which is crucial for multi-disciplinary collaboration. It helps participants learn to create actionable intelligence products that complement other forms of intelligence, fulfilling the goal of creating hybrid intelligence solutions within the Defense Intelligence Enterprise (DIE).

Additionally, SANS offers Industrial Control System courses that current branches within DoD and other departments utilize to assist in coverage of Critical Infrastructure. These course offerings could lead to a definite advantage to the OSINT community with understanding the numerous possible CRIT avenues, greatly increasing the range and ability to interpret different intelligence that is gathered. Having analysts familiar with what the traffic or potential vulnerabilities would increase the defensive posture.



ICS410: ICS/SCADA Security Essentials™

This course is designed to equip students with essential skills and knowledge that directly enhance the DoD's OSINT gathering capabilities. By fostering an understanding of internet protocols and their application in ICS/SCADA environments, this course enables participants to identify vulnerabilities and threats to the DoD Information Network and critical infrastructure. The focus on human-computer interaction principles and emerging communication technologies further supports advanced analytical methods for OSINT. Additionally, the course provides robust training in extracting, analyzing, and leveraging metadata, ensuring that defense personnel can efficiently gather actionable intelligence in the dynamic field of cybersecurity and infrastructure protection.

ICS515: ICS Visibility, Detection, and Response™

This course focuses on identifying and evaluating threat critical capabilities, requirements, and vulnerabilities, provides invaluable skills for the OSINT gathering community of the DoD. By equipping participants with expertise in monitoring and reporting validated threat activities, this course enables them to produce actionable intelligence and assessments that inform leadership decisions, refine objectives, and support operational planning. Additionally, the course emphasizes cyber operations support and anticipatory tactics, which are crucial for emulating and mitigating potential threat actions. Through training in intelligence analysis and operational support, ICS515 enhances the OSINT community's ability to address evolving challenges, ensuring timely and effective responses to both strategic and tactical needs.

Optimizing Sharing and Collaboration Technologies

SEC566: Implementing and Auditing CIS Controls™

This course helps intelligence personnel implement and assess cybersecurity controls within their organizations, ensuring secure sharing of OSINT-related technologies across various branches of the intelligence community. This directly addresses the goal of fostering broader collaboration and optimizing the sharing of tools, technologies, and data sources to enrich intelligence value while laying the foundation for network navigation through education of infrastructures, network traffic analysis, and attack vectors.

STRATEGIC GOAL 3: Expand the Open Source Aperture Internally and Externally

As outlined in the strategy, expanding the open-source aperture internally within the DoD and externally with allied partners is critical for a more unified global intelligence approach. SANS offers both technical and strategic courses that will help your teams to not only leverage internal data sources more effectively but also foster international collaboration.

Training for Broader Data Acquisition and Processing

SEC510: Public Cloud Security for AWS, Azure, and Google Cloud:

Given the increasing reliance on cloud-based platforms for OSINT collection and analysis, this course helps professionals understand how to securely gather, store, and process OSINT in the cloud while minimizing risks. This will be crucial as your teams expand the use of cloud technologies to scale data acquisition efforts across multiple sources.

Fostering International Collaboration

LDR521: Security Culture for Leaders: This course is designed to help leaders foster a security-focused culture within their organizations while promoting collaboration across borders. It will aid in establishing international partnerships, particularly with Five Eyes and allied intelligence communities, to support a globally postured OSINT collection and reporting platform.



STRATEGIC GOAL 4: Establish OSINT as a Premier Intelligence Capability and the Foundation for Other Disciplines

To achieve this strategic goal, the DoD OSINT community must professionalize its workforce, build expertise, and institutionalize training. SANS offers comprehensive training programs and certifications to support the professional development of OSINT personnel and help establish OSINT as a cornerstone of intelligence operations.

Professionalizing the OSINT Workforce

GOSI: GIAC Open Source Intelligence Certification

This certification program provides an in-depth education in OSINT collection, analysis, and reporting. By institutionalizing this training across the DoD OSINT workforce, you can ensure that personnel are equipped with standardized skills and best practices that align with DoD's mission.

LDR514: Security Strategic Planning, Policy, and Leadership™

This course helps OSINT leaders develop the strategic planning and leadership skills needed to guide their teams and operations. It covers topics such as risk management, policy development, and aligning intelligence objectives with broader organizational goals. These leadership capabilities are crucial for institutionalizing OSINT training and establishing governance structures that will support the long-term success of your intelligence programs.

Additional Courses to be considered.

SEC301: Introduction to Cyber Security™

This course provides foundational cybersecurity knowledge, emphasizing network-level attack vectors, cyber threats, and vulnerabilities, which directly enhance the OSINT community's ability to identify and mitigate potential risks within the DoD. By grounding participants in fundamental concepts such as Internet addressing, cyber operations, and network architecture, SEC301 builds a versatile skill set critical for identifying threats like spoofing or DDoS attacks. These capabilities empower OSINT practitioners to expand their intelligence analysis and collection strategies effectively. Moreover, the course establishes a robust framework, supporting interdisciplinary collaboration across cybersecurity, operations, and intelligence disciplines, thereby amplifying DoD intelligence capabilities and resilience.

SEC450: Blue Team Fundamentals: Security Operations and Analysis™

This course provides advanced education in cybersecurity operations, focusing on the integration of defense strategies and offensive tactics to address modern cyber threats. This course emphasizes in-depth knowledge of network vulnerabilities, attack vectors, and mitigation techniques while exploring real-world scenarios involving threat actors and their methodologies, such as DDoS attacks, spoofing, and brute force techniques. Participants gain expertise in advanced concepts like network defense architecture, incident response, and threat intelligence sharing, ensuring they are well-prepared to handle sophisticated cybersecurity challenges.

For the OSINT community within the DoD, SEC450 offers critical skills that enhance the capability to identify, analyze, and preempt cyber threats while supporting strategic decision-making. The course not only provides the technical depth needed for OSINT practitioners to expand their intelligence capabilities but also establishes foundational knowledge that bridges cybersecurity with other intelligence disciplines, fostering a cohesive and resilient approach to national defense.



STRATEGIC GOAL 5: Synchronize OSINT with Publicly and Commercially Available Information Activities

To address the goal of synchronizing OSINT efforts with publicly available information (PAI) and commercially available information (CAI) sources, SANS provides training that ensures OSINT professionals are well-versed in handling, securing, and integrating commercial data sources into their intelligence workflows.

Advanced Data Integration Techniques

FOR578: Cyber Threat Intelligence™

This course covers methodologies for integrating data from PAI/CAI sources into OSINT workflows, ensuring that intelligence teams can securely and effectively leverage commercially available information to enrich their intelligence products.

Leveraging Multi-Intelligence Collection Management

SEC566: Implementing and Auditing CIS Controls™ and *FOR509: Enterprise Cloud Forensics and Incident Response™*

These courses provide the necessary skills to manage data and tools from commercial sources, ensuring they are securely integrated into broader OSINT efforts while complying with DoD and industry standards.



SANS Institute is committed to providing world-class training that directly aligns with the strategic goals outlined in the Department of Defense’s OSINT Strategy for 2024–2028. By leveraging our comprehensive training programs, the DoD OSINT community can enhance its capabilities in collecting, analyzing, and reporting OSINT, while also professionalizing its workforce and fostering greater collaboration across the intelligence enterprise.

We look forward to collaborating with you to support your mission of establishing OSINT as a premier intelligence capability for the Department of Defense.

SANS | GIAC

CERTIFICATIONS

