NOVARTIS

# Dir. DDIT ISC CSOC Content Engineering

Job ID
REQ-10027408
Nov 06, 2024
India

## Sommario

As a Content Engineer, you will be responsible for planning, developing, testing, and tuning content for security platforms like SIEM, DLP, and EDR. You will provide expertise to optimize data onboarding, define and measure performance KPIs, and deliver reports to CSOC stakeholders. You will collaborate with stakeholders to align on initiatives, gather feedback, and improve services continuously. Additionally, you will research new tools to enhance cyber threat detection and response, and monitor content health to detect any issues impacting CSOC performance.

## About the Role

**Major accountabilities:**

- Talent and Growth.
- Manage and mentor associates and team leaders.
- Plan and implement technical and nontechnical development strategies for continuous development of CSOC analysts and leaders strategy and direction.
- Content engineering service involves planning, developing, testing, operationalizing, and tuning content for detection, investigation, and reporting from security platforms like SIEM, DLP, EDR, etc.
- Provide subject matter expertise, oversight, and feedback to optimize data onboarded into the SIEM.
- Content engineering service involves planning, developing, testing, operationalizing, and tuning content for detection, investigation, and reporting from security platforms like SIEM, DLP, EDR, etc.
- Provide subject matter expertise, oversight, and feedback to optimize data onboarded into the SIEM.
- Define and measure performance and effectiveness KPIs; develop and deliver timely reporting to CSOC stakeholders and senior leaders.
- Interface with other CSOC stakeholders to align on initiatives; proactively gather feedback; adjust and improve service continuously.
- Research new tools and techniques to improve overall CSOC ability to monitor, detect, and respond to cyber threats.
- Monitor health of content to detect outages, spikes, or other anomalies that may impact CSOC performance.

**Key performance indicators:**

- Review and evaluate SIEM team performance.
- Effectively and efficiently design and implement process automations, create supporting technical documentation and redundancy controls.
- Accurately troubleshoot to diagnose and resolve problems with process automations, case management issues, scripts, and other custom solutions that support CSOC operations.

- Identify technology and process gaps that affect CSOC services; develop solutions and make recommendations for continuous improvement.
- Good cultural orientation and strong influencer of information risk management, information security, IT security, to be embedded across IT, OT and Medical Technologies.

**Minimum Requirements:**
**Experience:**

- 10+ Years work experience.
- Strong Team Management skills.
- Good general security knowledge.
- Strong knowledge of security tools (DLP, XDR, SIEM, Firewalls).
- Experience in scripting and Automation for Security tools.
- Experience SIEM alert creation, SOAR playbook development.
- Experience in reporting to and communicating with senior level management (with and without IT background, with and without in-depth risk management background) on incident response topics.
- Strong written and verbal communication and presentation abilities, with the capacity to effectively convey information risk-related and incident response concepts to both technical and non-technical stakeholders.
- Exceptional interpersonal and collaborative skills, fostering effective communication and cooperation with diverse individuals and teams.
- Exceptional understanding and knowledge of general IT infrastructure technology and systems.
- Proven experience to initiate and manage projects that will affect CSOC services.

**Skills:**

- Understanding of SIEM architecture components, including technology integrations.
- Firsthand experience of Security tools like Splunk, Sentinel, XDR, DLP.
- Direct experience managing Data ingestion pipeline through Cribl.
- Understanding of security systems (such as AV, IPS, Proxy, FW).
- Security use-case design and development.
- Understanding of SOAR and Development experience in python (SDKs).
- An understanding of error messages and logs displayed by various software.
- Ability to troubleshoot, diagnose and solve issues independently.
- Self-learner, ability to document learning as experience is gained.
- Understanding of network protocols and topologies.
- Strong technical troubleshooting and analytical skills.
- A knowledge of the MITRE ATT&CK framework is beneficial.
- Ability to prioritise workload.
- Excellent written and spoken English.
- Team Management.
- Calm and logical approach.

**Languages :**

- English.

**Why Novartis:** Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together? https://www.novartis.com/about/strategy/people-and-culture

**Join our Novartis Network:** Not the right Novartis role for you? Sign up to our talent community to stay connected and learn about suitable career opportunities as soon as they come up: https://talentnetwork.novartis.com/network

**Benefits and Rewards:** Read our handbook to learn about all the ways we'll help you thrive personally and professionally: https://www.novartis.com/careers/benefits-rewards

Divisione
Operations
Business Unit
CTS
Posizione
India
Sito
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10027408

## Dir. DDIT ISC CSOC Content Engineering

Apply to Job

---

**Source URL:** *https://prod1.adacap.com/careers/career-search/job/details/req-10027408-dir-ddit-isc-csoc-content-engineering*

**List of links present in page**

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://talentnetwork.novartis.com/network
3. https://www.novartis.com/careers/benefits-rewards
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Dir-DDIT-ISC-CSOC-Content-Engineering_REQ-10027408
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Dir-DDIT-ISC-CSOC-Content-Engineering_REQ-10027408