Security Automation Engineering

Job ID
REQ-10041231
Mar 06, 2025
Mexico

Summary

CSOC Engineering will be an integral part of the Novartis Cyber Security Operations Center (CSOC). The CSOC is an advanced global team passionate about the active defence against the most sophisticated cyber threats and attacks. By leveraging various tools and resources, the CSOC Engineer will help to proactively detect, investigate, and mitigate both emerging and persistent threats that pose a risk to Novartis' networks, systems, users, and applications.

The main objective of the CSOC Engineering is to design, develop, implement, and manage dataflow pipelines and integrate them with SIEM platforms such as Sentinel and Splunk. The Data onboarded to SIEM will be Crucial for CSOC Analysts and the content development and SOAR Engineers to develop monitoring alerts and automation playbooks.

Collaboration with internal and external stakeholders, including Novartis' internal teams, external vendors, and Product/Platform engineers, will be a crucial aspect of this role. The CSOC Engineer will work closely with Application owners to understand and integrate various datasources. This may involve utilizing services such as Cribl, Syslog NG, Azure Monitoring Agent, Universal Forwarder to list a few.

Furthermore, the CSOC Engineering Lead will work in close partnership with the CSOC stakeholders, including TDR, THR, Forensic, Content Development, and SOAR teams. Their expertise and collaboration will be instrumental in quickly resolving any Data onboarding requests or resolve any issues with the detection rule on security tool such as SIEM, DLP, EDR.

Overall, the CSOC Engineering role is pivotal in ensuring the proactive defence of Novartis' critical assets, systems, and infrastructure against the ever-evolving landscape of cyber threats.

About the Role

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- **SOAR**
- Identify and implement automation opportunities by continuously analyzing security operations workflows

to optimize existing playbooks and introduce new automation.

- Work closely with automation consumers, CSOC analysts, and security teams to gather requirements and ensure automations align with security best practices and business objectives.
- Validate vendor-provided SOAR integrations to ensure expected functionality and compatibility with security tools.
- Design and develop custom case management solutions to improve security investigations, incident tracking, and response efficiency.
- Partner with CSOC engineers, Threat Hunters, and Analysts to develop and implement automation solutions tailored to operational needs.
- Develop, maintain, and enhance custom SOAR integrations to extend automation capabilities and support evolving security needs.
- Define, measure, and track automation effectiveness, adoption rates, and impact on CSOC efficiency. Present ROI and operational improvements to leadership.
- Ensure that automation delivers tangible business value and reduces the burden on security teams.
- Monitor the health, reliability, and performance of the SOAR platform, ensuring automation jobs run as expected, troubleshooting issues proactively, and minimizing system downtime.
- Enable faster detection, response, and remediation of security incidents by refining automated workflows, integrating threat intelligence, and improving case management processes.
- Maintain detailed documentation for automation workflows, playbooks, integrations, and troubleshooting procedures.
- Foster a culture of continuous improvement by regularly refining automation logic, eliminating inefficiencies, and ensuring SOAR workflows remain aligned with evolving threat landscapes and security priorities.
- Provide 24x7 on-call support on a rotational basis, including weekends, to ensure system stability and incident response readiness.

KEY PERFORMANCE INDICATORS / MEASURES OF SUCCESS

- **Automation Efficiency**: Drive the automation of manual security operations processes within SOAR to enhance response times and reduce analyst workload.
- **Integration Success**: Implement and maintain seamless integrations between SOAR and various security tools, including SIEM, EDR, threat intelligence platforms, and case management systems.
- **Incident Response Optimization**: Improve incident handling by reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) through SOAR-driven automation.
- **Error Reduction & Accuracy**: Minimize false positives and workflow misconfigurations by refining automation logic and validation processes.

- **Case Management & CSOC Productivity**: Enhance CC analysts' efficiency by automating repetitive tasks, improving case management, and optimizing investigation workflows.
- **Health Monitoring & System Reliability**: Continuously monitor SOAR platform health, automation performance, and API integrations to ensure high availability, timely issue resolution, and minimal system downtime.
- **User Adoption & Feedback**: Foster adoption of SOAR automation by ensuring automations are user-friendly, effective, and well-received by security teams, with measurable satisfaction scores and usability feedback.
- **Continuous Improvement & Innovation**: Identify gaps in security processes and technologies, recommend improvements, and contribute to the ongoing enhancement of CSOC services through automation and orchestration.

PERSONAL CONSIDERATIONS

As the role is part of a global organization, willingness for required traveling and flexible work hours is important.

EDUCATION / EXPERIENCE

EDUCATION

- **Essential:**
- University working and thinking level, degree in business/technical/scientific area or comparable education/experience.
- **Desirable:**
- Advanced training/certification on Security tools like Splunk, Sentinel, XDR, DLP
- SANS certifications (for security analyst/SIEM)
- Cloud Security Engineering certification (Azure/AWS)

EXPERIENCE

- 4+ Years work experience.
- Effective communication skills.
- Good general security knowledge.
- SOAR platforms (e.g., Splunk Phantom, Palo Alto Cortex XSOAR, IBM Resilient, etc.)
- Enterprise security operations and incident response
- Scripting and automation (e.g., Python, shell scripts).
- Interacting with APIs and parsing API output

- Strong knowledge of security tools (DLP, XDR, SIEM, Firewalls).
- Ability to work both independently and as part of a team in a fast-paced, dynamic environment.
- Ability to prioritize individual/group work in a high-activity and time-bound environment
- Flexible to provide coverage in US morning hours on a need-basis, and as required
- Support, guide and mentor peer team members in technical and functional matters
- Strong written, verbal and presentation skills to work effectively across teams
- Sense of urgency and attention to detail
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills.
- Experience in configuring Data collection Endpoints, connectors and parsers.
- Experience in Security Engineering tasks such as 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.
- 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.

PRODUCT/MARKET/CUSTOMER KNOWLEDGE

- Good understanding of pharmaceutical industry. Good understanding and knowledge of business processes in a global pharmaceutical industry.

SKILLS/JOB RELATED KNOWLEDGE

- Firsthand experience on SOAR platforms (e.g., Splunk Phantom, Palo Alto Cortex XSOAR, IBM Resilient, etc.)
- Strong scripting skills (Python, Java, shell).
- Experience with APIs (calling, authentication, parsing JSON/XML).
- Development experience with Python SDKs for integrations.
- Ability to analyze logs and troubleshoot errors.
- Understanding of network protocols (TCP/IP, DNS, HTTP, firewalls).
- Strong technical troubleshooting and analytical skills.
- Incident Response Lifecycle knowledge (detection, containment, eradication, recovery)
- Experience with SIEM & SOC operations (Splunk, Sentinel).
- Knowledge of MITRE ATT&CK & cyber kill chain

- Familiarity with log analysis, threat hunting, forensics.
- Ability to write clear documentation for playbooks and integrations.
- Experience with CI/CD & Git for automation deployment.
- Strong understanding of case management workflows.
- Excellent communication skills (written & verbal).
- Calm, logical, detail-oriented problem-solving.

NETWORKS

- High level of personal integrity, and the ability to professionally handle confidential matters and exude the appropriate level of judgment and maturity.
- Ability to manage competing priorities, and seeking consensus when stakeholders have different or even contradicting opinions.

OTHER

- Fluency (written and spoken) in English

CORE COMPETENCIES

Customer/Quality Focus

Assigns highest priority to customer satisfaction. Listens to customer and creates solutions for unmet customer needs. Established effective relationships with customers and gains their trust and respect.

- Defines quality standards to ensure customer satisfaction.
- Creates and supports world-class quality standards to ensure customer satisfaction.

Fast, Action-Oriented

Is action-oriented and full of energy to face challenging situations. Is decisive, seizes opportunities and ensures fast implementation. Strives for simplicity and clarity. Avoids 'bureaucracy'.

- Alerts others to potential risks and opportunities.
- Keeps organizational processes simple and efficient.
- Takes acceptable/calculated risks by adopting new or unknown directions.

Results Driven

Can be relied upon to succeed targets successfully. Does better than the competition. Pushes self and others for results.

- Anticipates potential barriers to achievement of shared goals.
- Pushes self and others to see new ways of achieving results (e.g., better business model).
- Uses feasibility and ROI analyses to ensure results.
- Keeps pace with new developments in the industry.

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

Division
Operations
Business Unit
CTS
Location
Mexico
Site
INSURGENTES
Company / Legal Entity
MX06 (FCRS = MX006) Novartis Farmacéutica S.A. de C.V.
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10041231

Security Automation Engineering

Apply to Job

Source URL: *https://uat2.novartis.de/de-de/careers/career-search/job/details/req-10041231-security-automation-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/INSURGENTES/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10041231
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10041231