NOVARTIS

Assoc. Dir. DDIT ISC CSOC Engineering - Cloud

Job ID
REQ-10090086

十月 16, 2026

India

摘要

We are seeking a hands-on Cloud Detection Engineer to help shape the future of cloud security monitoring at Novartis. You will design, build, validate and continuously improve detection capabilities across Azure, AWS and other strategic cloud platforms while being a key partner with incident response and cloud security architect teams. An engineering role that combines cloud telemetry, custom detections, threat research, automation and AI-assisted investigation to create high-signal, scalable outcomes for Cyber Defense.

Role purpose:

Build a robust, AI-native cloud detection pipeline that improves correlation and investigation efficiency across multi-cloud environments. Engineer fragmented cloud telemetry into clear, actionable security outcomes with AI embedded throughout the detection engineering lifecycle. A multidimensional engineering role at the intersection of automation, cloud architecture, threat behavior analysis, detection engineering supporting analyst investigation workflows.

About the Role

Key Responsibilities

- Design and operate an AI-native cloud detection pipeline that aggregates, correlates, enriches, deduplicates and prioritizes signals before analyst investigation
- Build and tune high-fidelity detections that improve coverage across cloud control-plane, data plane and management-plane activity, identity and access, network, container and Kubernetes and security posture.
- Use lower-fidelity and behavioral signals as investigation context, while ensuring known high-confidence detections are consistently escalated for security investigation
- Integrate and correlate telemetry from WIZ, Microsoft Defender for Cloud, AWS GuardDuty, Microsoft Sentinel and other cloud-native or CNAPP sources . Apply hands-on Wiz experience to interpret posture findings, attack paths, identity and exposure context, cloud events, runtime findings and threat detections and improve detection workflows
- Develop behavioral baselines and entity-centric analytics across users, IP addresses, identities and cloud resources . Create reusable dashboards, dynamic lookups and enrichment patterns enabling rapid pivots / drilldowns from an alert to related resource, identity, inventory and historical data
- Own the detection lifecycle from threat hypothesis and telemetry assessment through development, peer review, testing, deployment, tuning, documentation and retirement
- Embed AI across the detection lifecycle to accelerate detection creation and tuning, while ensuring engineering controls and human judgment govern the outcomes
- Finetune detections using historical data, controlled simulations, purple-team exercises, attack emulation and lessons learned from incidents and threat hunts
- Use detection-as-code practices, Git, CI/CD and automated testing to deliver controlled, repeatable and auditable content changes . Partner with Threat Hunting and Response, CSOC analysts, cloud platform teams, data onboarding, threat intelligence and automation teams to close visibility gaps and operationalize detections
- Automate enrichment and triage using Python, APIs, SOAR workflows and AI-assisted approaches, with appropriate human oversight for security decisions . Measure and improve detection coverage, precision, false-positive rate, investigation volume, alert latency, data quality and analyst effort

Required Qualifications

- 8+ years of hands-on experience in cloud security, detection engineering, security analytics, threat hunting, incident response or security platform engineering
- Working knowledge of Azure and AWS security architectures, respective cloud domains and workloads
- Understanding of cloud telemetry and logging sources such as Azure Activity and Diagnostic logs, Entra ID logs, AWS CloudTrail, AWS CloudWatch and GuardDuty findings
- Experience in working with CNAPP bundles or developing and tuning detections in Wiz, Vega or cloud-native security platforms
- Proficiency in KQL and at least one scripting or programming language such as Python. CloudShell understanding is expected
- Familiarity with AI/LLM-assisted security investigation, agentic workflows or machine-learning approaches to signal enrichment and triage . Understanding of MITRE ATT&CK, MITRE

ATLAS, threat-informed defense, entity mapping, correlation, enrichment and alert prioritization
- Ability to investigate complex datasets, distinguish true security risk from operational noise and communicate engineering decisions clearly . Experience collaborating across security operations, cloud engineering and platform teams in a global environment.
- Experience with detection-as-code, Sigma or YAML-based content, Git, CI/CD, unit/integration testing and safe deployment or rollback practices . Experience with Infrastructure as Code and automation tools such as Terraform, ARM/Bicep, CloudFormation or equivalent. Background in threat intelligence, purple teaming, red teaming, incident response or cloud threat research

Desirable Requirement:

- Relevant certifications such as AZ-500, AWS Certified Security - Specialty, GIAC Cloud Security certifications, CCSP or equivalent practical expertise.
-

You ' ll receive: You can find everything you need to know about our benefits and rewards in the Novartis Life Handbook. https://www.novartis.com/careers/benefits-rewards

Commitment to Diversity and Inclusion:
Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to hear more about Novartis and our career opportunities, join the Novartis Network here:
https://talentnetwork.novartis.com/network

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

Benefits and Rewards: Learn about all the ways we ' ll help you thrive personally and professionally. Read our handbook (PDF 30 MB)

部门
Operations

Business Unit
Information Technology

地点
India

站点
Hyderabad (Office)

Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited

Functional Area
Information Technology

Job Type
Full time

Employment Type
Regular

Shift Work
No

var kPlayer = KalturaPlayer55802022 || KalturaPlayer; var config = { targetId: "kalturaplayer6ad2588a9fc91803894843", provider: { widgetId: "10m7rm1pm", partnerId: "2076321", uiConfId: "55802022" }, playback: { autoplay: false, autopause: false, muted: false, loop: false }, sources: { options: {}, startTime: 0 }, disableUserCache: "true", plugins: {}, sources: { options: {}, startTime: 0 }, ui: { showCCButton: false, settings: { showQualityMenu: true, showSpeedMenu: false }, components: { fullscreen: { disableDoubleClick: false } }, uiComponents: [{ presets: ['Playback', 'Live'], area: 'BottomBarRightControls', replaceComponent: 'Fullscreen', get: kPlayer.ui.components.Remove }] } }; // Check and add plugins only if they exist if (kPlayer.plugins["download"]) { config.plugins.download = { disable: true }; } if (kPlayer.plugins["transcript"]) { config.plugins["playkit-js-transcript"] = { position: "right", // Default: bottom;('left', 'right', 'top', 'bottom') to enable transcript. expandMode: "over", // Default:

alongside;('alongside', 'hidden', 'over') expandOnFirstPlay: false, showTime: true, downloadDisabled: false, printDisabled: false, disable: true }; } if (kPlayer.plugins["preventSeek"]) { config.plugins.preventSeek = { preventSeekForward: false, preventSeek: false }; } config.plugins.floating = { disable: true }; if (kPlayer.plugins["navigation"]) { config.plugins.navigation = { position: "right", expandMode: "over", expandOnFirstPlay: false, visible: false }; } if (kPlayer.plugins["hotspots"]) { config.plugins['playkit-js-hotspots'] = { disable: true }; } if (kPlayer.plugins["moderation"]) { config.plugins['playkit-js-moderation'] = { disable: true }; } if (kPlayer.plugins["info"]) { config.plugins['playkit-js-info'] = { disable: true }; } if (kPlayer.plugins["share"]) { config.plugins.share = { disable: true }; } config.ui.uiComponents = []; if (kPlayer.plugins["googleAnalytics"]) { config.plugins.googleTagManager = {}; config.plugins.googleTagManager.customEventsTracking = {}; config.plugins.googleTagManager.containerId = 'GTM-57RJQ5'; config.plugins.googleTagManager.customEventsTracking.custom = []; config.plugins.googleTagManager.customEventsTracking = { preset: { coreEvents: true, UIEvents: false, playlistEvents: false, castEvents: false } }; }

// Ensure the global player registry array always exists, regardless of embed type. window.kalturaPlayerVideos = window.kalturaPlayerVideos || []; try { var thumbEmbedPromise = thumbnailEmbed({config, mediaInfo: {entryId: "1dgfvmafo"}}); // thumbnailEmbed() returns a Promise that resolves with the player instance // when the user clicks the thumbnail. Use .then() to capture the player directly. thumbEmbedPromise .then(function(player) { window.kalturaPlayerVideos.push(player); // Notify kalturadatalayer.js that a new player is ready so it can // attach custom event listeners immediately, regardless of when // the user clicked the thumbnail relative to page load. document.dispatchEvent(new CustomEvent('kalturaPlayerReady', { detail: { player: player } })); }) .catch(function(error) { console.error(error); }); } catch (e) { console.error(e.message) }

Accessibility and accommodation

Novartis is committed to working with and providing reasonable accommodation to individuals with disabilities. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to perform the essential functions of a position, please send an e-mail to diversityandincl.india@novartis.com and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

Job ID
REQ-10090086

Assoc. Dir. DDIT ISC CSOC Engineering - Cloud

Apply to Job

Job ID
REQ-10090086

Assoc. Dir. DDIT ISC CSOC Engineering - Cloud

Apply to Job

Source URL:
https://prod1.novartis.com.cn/careers/career-search/job/details/req-10090086-assoc-dir-ddit-isc-csoc-

engineering-cloud

List of links present in page

1. https://www.novartis.com/careers/benefits-rewards
2. https://talentnetwork.novartis.com/network
3. https://www.novartis.com/about/strategy/people-and-culture
4. https://www.novartis.com/sites/novartiscom/files/novartis-life-handbook.pdf
5. mailto:diversityandincl.india@novartis.com
6. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-CSOC-Engineering---CloudREQ-10090086
7. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-CSOC-Engineering---CloudREQ-10090086