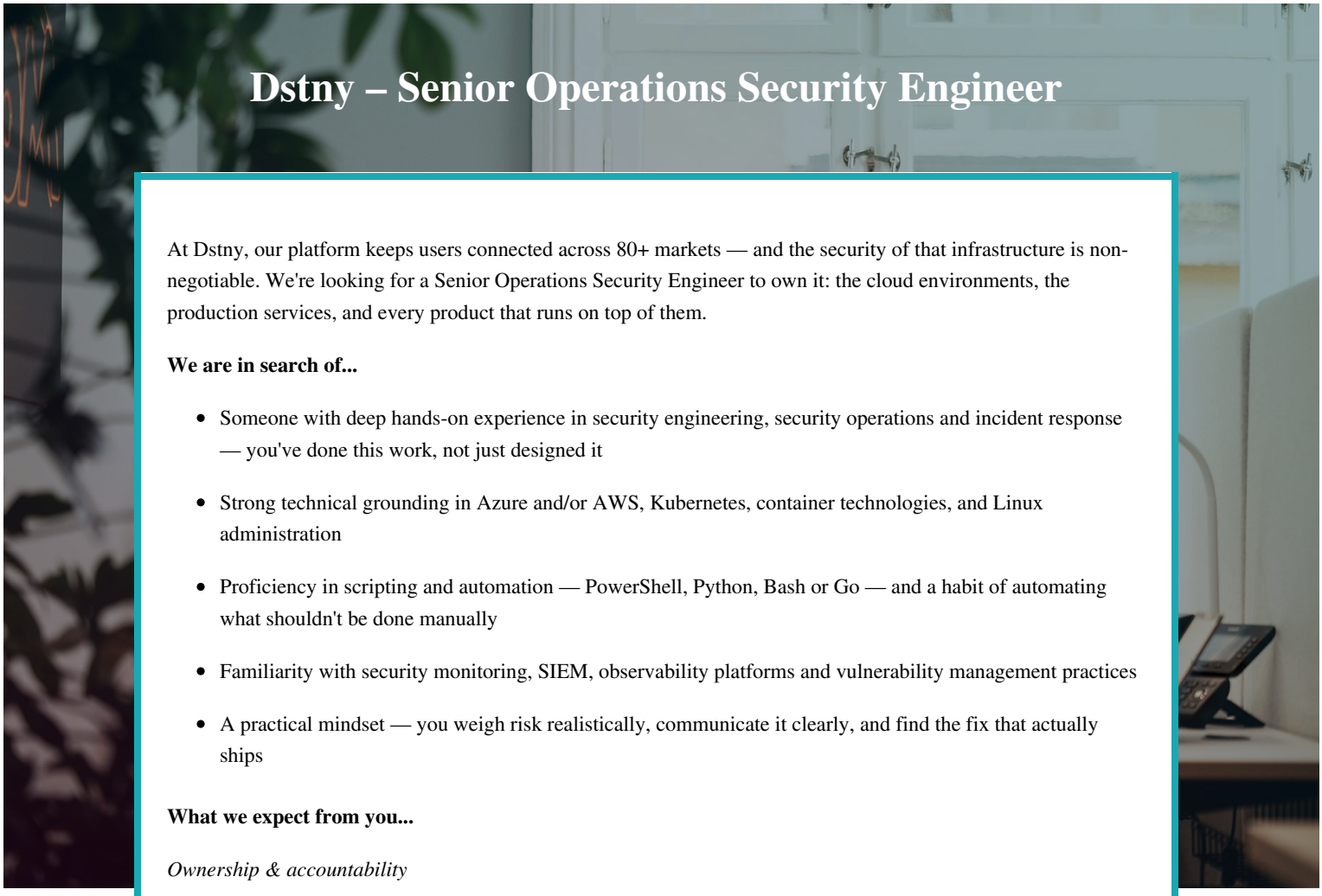

Dstny – Senior Operations Security Engineer

At Dstny, our platform keeps users connected across 80+ markets — and the security of that infrastructure is non-negotiable. We're looking for a Senior Operations Security Engineer to own it: the cloud environments, the production services, and every product that runs on top of them.

We are in search of...

- Someone with deep hands-on experience in security engineering, security operations and incident response — you've done this work, not just designed it
- Strong technical grounding in Azure and/or AWS, Kubernetes, container technologies, and Linux administration
- Proficiency in scripting and automation — PowerShell, Python, Bash or Go — and a habit of automating what shouldn't be done manually
- Familiarity with security monitoring, SIEM, observability platforms and vulnerability management practices
- A practical mindset — you weigh risk realistically, communicate it clearly, and find the fix that actually ships

What we expect from you...

Ownership & accountability

- Own the security posture of our cloud platforms and production infrastructure. That means taking accountability for the controls, the monitoring, and the outcomes — not just the tasks assigned to you. If something is at risk, you'll be the one who surfaces it and drives it to resolution.
- Own the security of the products delivered on the platform — Dstny Voice, Dstny Digital Agents, Dstny Call2Teams and Dstny Intelligence. This includes AI and digital agent services, as well as real-time communications threats like telecom fraud and SIP abuse. These are live, customer-facing services, and the accountability is real.
- Own vulnerability remediation across the platform. You'll track exposure, prioritise by risk, coordinate with engineering teams to get fixes shipped, and report on progress. Good is not having fewer vulnerabilities — good is having a programme that consistently reduces risk over time.

Actions

- Design, implement and operate security controls across Azure/AWS environments and Kubernetes platforms. You'll harden operating systems, containers and APIs, improve identity and access management, and build the detection and alerting capabilities that give us visibility before incidents become incidents.
- Lead the technical investigation and remediation of security incidents from triage through to post-incident review. You'll be hands-on in the response, coordinate across teams when needed, and make sure lessons translate into improved controls — not just a closed ticket.
- Embed security into the work of Platform Engineering, Development and Architecture teams. That means reviewing infrastructure and API designs early, providing practical guidance during projects and major platform changes, and building the kind of trusted relationship where engineers come to you before they ship, not after.

Scope

- This role sits within the Operations team and reports to the VP Platform Operations. You'll work across the full Production & Technology Organisation — engaging with Platform Engineering, Development, Architecture, Compliance and the DPO — which means broad influence and broad exposure.
- The platform is multi-tenant and carrier-grade, with a mix of modern cloud-native services and legacy products still in production. Your remit covers both. Keeping tenant isolation and service-provider channel security intact across that complexity is part of the role.
- You'll support compliance activities including ISO 27001, NIS2 and GDPR, and contribute to security standards and continuous improvement initiatives. This isn't a back-office compliance function — it's engineering-led security work that happens to intersect with regulatory requirements.

What we offer you...

- A collaborative team where your work has direct impact on a platform used by millions — we build on each other, not past each other
- An AI-first environment where intelligent tools are part of how we work every day, not a novelty
- Technically serious problems at real scale — securing a carrier-grade, multi-tenant platform that never goes down is not a trivial challenge
- A culture shaped by our ICORE values: Innovation, Commitment, Obsession for CX, Respect, and Empower — lived daily, not laminated on a wall
- Flexibility, trust and the autonomy to own your domain
- A business with real momentum — 1,000+ people across 8 countries, growing with purpose

https://dstny.com/