

DMITRII CREED

DevSecOps, SRE & Platform Lead — I make delivery fast and audit-proof

@creed22@gmail.com
Cre-eD

Tbilisi, Georgia

https://t.me/dmitriicreed

dmitriicreed



EXPERIENCE

Head of DevOps, SRE & Security (DevSecOps)

Everworker (Integrail Corp)

Aug 2025 – Present

Remote

- **Own all infrastructure, CI/CD, reliability and security** for an AI agent platform across **AWS, Azure and GCP** — greenfield, no prior tooling, process or headcount.
- **Two certifications, and I own them.** Walked in a month before **ISO/IEC 27001:2022** initial certification (Sept 2025), closed its 5 minor non-conformities, and then took **Surveillance Year 1** through with **zero findings**. **SOC 2 Type II** passed two years running, scope widened this year to add **Privacy and Availability**. Auditor: A-LIGN. The control set, the evidence automation and the pipelines under all of it are mine.
- **Built security as a platform: 19 shared actions and 8 reusable workflows** any repo plugs into. Policy-as-code (Pulumi Cross-Guard), a **107-rule Semgrep library in 5 languages**, each rule fixture-tested, SCA, container, secret and workflow-config scanning, DAST (ZAP, Nuclei, a 49-module harness), SBOM (Syft) and keyless signed provenance (Cosign/Sigstore). Everything lands in DefectDojo behind a **gate that blocks new findings**.
- **Went keyless.** Inventoried **12 long-lived AWS access keys** (one held AdministratorAccess) and migrated deployment and CI paths to **GitHub OIDC federation**, ECS task roles and SSO, with ref- and environment-scoped trust policies.
- **Cut alert noise by an order of magnitude.** Rebuilt CloudTrail security alerting with 8 detectors beyond the CIS baseline and per-detector exclusions: from **232 alarm fires in 14 days at roughly 89% false-positive** down to single-digit daily fires, with **zero false positives** across the first observation window.
- **Led incident response** on a credential-exposure and extortion attempt against the org's private source control: forensics across an **87,000-event audit export**, then org-wide access hardening managed as Pulumi IaC.
- Commissioned and drove the **independent penetration test** that satisfies the audit control: **12 findings** (1 high, 6 medium, 5 low) triaged, and the key ones turned into **DAST regression checks** so they stay tested in CI rather than being fixed once.

Head of SRE & Security (Group CTO)

Soramitsu

2019 – 2025

Remote

As Group CTO, **145 people across six countries** reported into me and I reported to the chief executive — without ever stopping the hands-on work. Owned infrastructure, SDLC and security across the group's portfolio, and ran reliability and security for **Bakong**, the National Bank of Cambodia's payment system, alongside the CBDC pilots and the group's **Web3** work. Contributor to Soramitsu's Central Banking "**CBDC Partner of the Year**" (2020).

MOST PROUD OF



Kept a national payment system alive

Led DevOps and security for **Bakong** (National Bank of Cambodia), which moved **\$150B+ in 2024**, about **330% of the country's GDP**, across 30M+ wallets. **99.999% uptime** on the systems that could not be down.



Greenfield to two certifications

ISO 27001:2022 certified, then **surveillance-audited with zero findings**. **SOC 2 Type II** passed two years running, scope widened to Privacy and Availability. No prior tooling, process or team existed when I started.



Made the pipeline the perimeter

SLSA provenance, **SBOM**, signed artifacts, workflow-config scanning and keyless **OIDC** deploys. The delivery system gets threat-modelled like production, because it is production.



Cleared for frontier-model security work

Approved under **Anthropic's Cyber Verification Program**: dual-use offensive-security work unblocked for the org, under monitoring and inside policy.

AI IN THE LOOP

- **Compliance and policy.** Rebuilt an ISMS of **29 policies** with AI-assisted drafting against the real control library. The lesson runs the other way too: the inherited AI-written policy set claimed MDM, EDR and directory services the company *did not have*, so I made verification of every named tool and role mandatory. AI drafts, evidence decides.
- **Vulnerability triage.** AI-assisted triage across SAST, SCA and container findings at org scale, with reachability and fix version checked before anything is suppressed. A suppression has to survive an auditor.
- **Adversarial review.** Every remediation change goes through a **multi-model review panel** before merge; it repeatedly

Reliability & platform:

- **Web3 and protocol delivery:** infrastructure, SDLC and security for the group's blockchain work — **Web3 Foundation** grants, **Polkadot**-ecosystem development, **Klaytn**, the **SORA** ecosystem — on the same pipelines and security gates as the payment systems.
- Founded the SRE practice from nothing and ran it as embedded SRE-as-a-Service for **20+ stream-aligned teams across 4 regions**: SLIs, SLOs, error budgets, incident command, blameless review, **99.999% uptime** on critical systems and **MTTR down 60%**.
- Took the platform from inception to enterprise scale: **300+ applications**, **700+ repositories**, **6 GitHub organisations**, **99% IaC coverage** across AWS, GCP and EKS, **SLA from 99% to 99.99%**. Kubernetes on GitOps for 20+ production workloads; reusable pipeline libraries across 10+ languages that **cut build times 40%** and **cost 30%+**.
- Observability end to end plus chaos engineering; automated backup and DR for 5 mission-critical systems, and ran the restores that proved they worked. Hired and grew engineers from trainee to senior; at peak **37 engineers reported to me** across DevOps, security and QA, including a **security team of 6**.

Security:

- Built the AppSec programme: threat modelling (STRIDE, VAST) with data-flow diagrams mandatory for every new service, CVSS and EPSS risk scoring that **cut exposure windows 70%**, and a **Security Champions Program** that upskilled **100+ developers** and pushed ownership into product teams.
- Zero-trust access: secrets in Vault with dynamic issuance and rotation, MFA with chat-ops confirmation for production, VMs and clusters hardened to CIS with Wazuh for FIM and intrusion detection.
- Led internal audits, ran bug bounties, and wrote the **Incident Response, DR and Business Continuity** programmes, all three of which I have since run in anger. Benchmarked against BSIMM, OWASP SAMM and DSOMM.
- Brought **AI into the operations loop**: model-assisted incident triage, postmortem drafting and infrastructure review, with an engineer signing off every time. An unverified suggestion is not a control.

Earlier: Security Research, Systems & Network Engineering

Telecom, healthcare retail and public sector

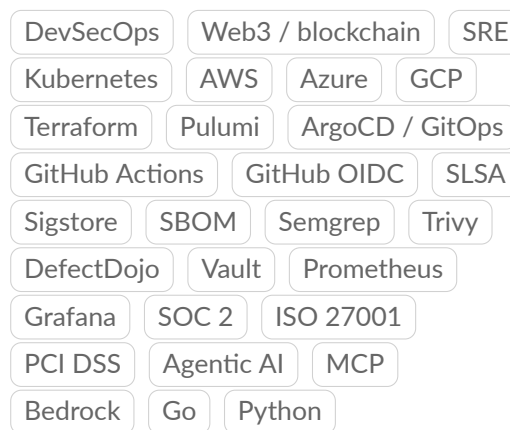
📅 2013 – 2019

Container-escape research on a Kubernetes lab I built; infrastructure for **500+ workstations**, **150+ pharmacies** and a **2,000-user campus**.

caught real residual bugs, and taught the discipline that model-reported critical findings get verified before they are believed.

- **Reusable agent skills and delivery flow.** An internal library of agent skills for recurring DevSecOps work (dependency-remediation waves, DAST runs, findings triage, stack provisioning), plus AI-driven roadmap and ticket workflows with one tracked task per change — so the same fix runs the same way for anyone, and the audit trail is a by-product of shipping.

TECHNICAL



- **Security:** cloud and zero-trust architecture, IAM/PAM, key management (HSM, PKI), AppSec, **supply-chain security**, vulnerability management, incident response and forensics.
- **Compliance:** **SOC 2 Type II**, **ISO 27001**, PCI DSS, NIST CSF, CIS, SWIFT CSCF, evidence automation, auditor engagement.
- **Languages:** Go, Python, Rust, Java, JavaScript. English and Russian, both fluent.

EDUCATION

M.Sc. Secure Systems and Networks Engineering

Innopolis University, 2018 – 2020
Full-tuition scholarship with stipend

B.Sc. Applied Informatics, with honours
2014 – 2018