



Lead Security Engineer, Purple Team

Malachi Randall

(913) 555-0148
malachi.randall@example.com
<https://linkedin.com/example/malachirandall>
Overland Park, Kansas 66212

Contact

Address

Overland Park, Kansas 66212

Phone

(913) 555-0148

Email

malachi.randall@example.com

LinkedIn

<https://linkedin.com/example/malachirandall>

Website

malachirandall.com

September 08, 2026

Hiring Team
Sentinel Arc Security
Kansas City
Missouri

Dear Hiring Team at Sentinel Arc Security,

I am applying for the Lead Security Engineer, Purple Team role at Sentinel Arc Security. Your work connecting adversary research, detection engineering, and the SOC is a close match for the work I have led across MDR customer environments. I am drawn to the chance to test real attacks and turn the results into better defensive coverage.

In my current role, I own a purple-team program that uses current actor, malware, and tooling research to recreate intrusion paths against crown-jewel systems. I build emulation plans with Caldera, Atomic Red Team, Prelude, and custom tradecraft, then measure prevention, visibility, alerting, and response outcomes. This work has given engineers and customers clear priorities for closing coverage gaps.

My blue-side work includes writing and tuning Sigma, KQL, and Splunk detections from endpoint, network, identity, cloud, SIEM, and EDR telemetry. I have tested command-and-control, credential access, lateral movement, persistence, and evasion scenarios, using CrowdStrike Falcon and Microsoft Sentinel data to check alert quality and investigation context. I enjoy the practical loop between realistic attack behavior and detection improvements.

I bring 13+ years across offensive security, detection engineering, threat hunting, and MDR operations, supported by OSCP, CRT0, GCFA, and CISSP credentials. I have presented technical findings to engineers, SOC analysts, customers, and executives, and I would bring that same clear reporting and hands-on ownership to Sentinel Arc Security.

Thank you for considering my application. I look forward to discussing how I can help Sentinel Arc Security prove and improve detection of real attacks.

Sincerely,

Malachi Randal

Malachi Randall