Malachi Randall

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

SUMMARY

Lead Security Engineer with 13+ years connecting **offensive security**, **adversary emulation**, **detection engineering**, **threat hunting**, and MDR operations. Builds realistic attack plans, recreates intrusion paths, and translates endpoint, network, identity, cloud, SIEM, and EDR telemetry into durable detection content. Researches actors, malware, tooling, command-and-control methods, evasion, and behaviors affecting high-risk environments and crown-jewel systems. Measures defensive coverage through repeatable validation, then communicates findings clearly across engineers, SOC analysts, customers, and executive stakeholders. Hands-on work includes Caldera, Atomic Red Team, Prelude, Scythe, Sigma, KQL, Splunk, Microsoft Sentinel, CrowdStrike Falcon, Python, and PowerShell. Ready to help Sentinel Arc Security close gaps between adversary research, detection engineering, and SOC response.

EXPERIENCE

Lead Security Engineer, Purple Team

September 2021 - Present

Northstar Defense Analytics

Denver, Colorado

Owns purple-team operations across MDR customer environments, combining **adversary research**, attack emulation, detection validation, customer reporting, and mentoring. Connects offensive tradecraft with endpoint, network, identity, and cloud telemetry so engineering and SOC teams can prioritize practical coverage improvements.

- Mapped actor tradecraft into Caldera **emulation plans** for **crown-jewel systems** and customer environments.
- Converted attack findings into Sigma, KQL, and Splunk detections using Falcon and Sentinel telemetry.
- Validated command-and-control, **credential access**, **lateral movement**, persistence, and evasion with repeatable scenarios.
- Built coverage reports separating prevention, visibility, alerting, and response outcomes for executive decisions.
- Mentored detection engineers through case reviews, workshops, and peer checks across research and handoffs.
- Presented customer findings with prioritized remediation steps, measurable **coverage gaps**, and response recommendations.

Senior Detection Engineer

June 2018 - August 2021

Redwood Signalworks

Austin, Texas

Led detection content development for an MDR service supporting technology, financial services, and healthcare customers across hybrid cloud environments. Turned threat research and controlled emulation into analytic content, telemetry improvements, customer findings, and stronger SOC response practices.

- Mapped adversary behaviors to **MITRE ATT&CK** and translated research into **Sigma** and Sentinel analytics.
- Ran **Atomic Red Team** and Scythe scenarios against PowerShell, credential theft, **remote services**, and cloud abuse.
- Correlated Windows, Linux, DNS, proxy, identity, and cloud records to expose high-risk blind spots.
- Measured alert precision, investigation context, and response handoffs through controlled validation exercises.
- Presented customer remediation priorities to architects and technical leaders using sequenced **detection** improvements.
- Built Falcon prevention policies and **Splunk** searches from current malware and actor research.

Offensive Security Consultant

July 2016 - May 2018

Ironclad Cyber Group

Raleigh, North Carolina

Delivered authorized **penetration testing** and **adversary emulation** for mid-market organizations, shaping realistic attack paths, evidence collection, and blue-team improvements. Adapted command-and-control infrastructure, tradecraft, and reporting for external, internal, and hybrid-cloud engagements.

- Built command-and-control infrastructure for external, internal, and hybrid-cloud emulation engagements.
- Used **Caldera**, Python, PowerShell, and **Atomic Red Team** to reproduce attacker behaviors safely.
- Assessed endpoint and **network telemetry** for **evasion**, logging, and alert-routing weaknesses.
- Created detection recommendations with analytic logic, data sources, validation steps, and escalation context.
- Produced leadership briefings connecting observed attack chains with prioritized control changes and retest criteria.
- Adjusted emulation plans around customer scope, rules of engagement, and defensive objectives.

Security Operations Analyst

August 2014 - June 2016

Blue Meridian Systems

Columbus, Ohio

Monitored and investigated endpoint, network, identity, and cloud events within a 24/7 **SOC**. Improved **SIEM** and EDR content through threat hunts, isolated lab exercises, investigation guides, and concise leadership reporting.

- Tuned SIEM correlation rules and **EDR** policies after reviewing recurring false positives.
- Hunted **Windows**, DNS, proxy, and authentication data for command-and-control and lateral movement.
- Reproduced adversary behaviors with **Atomic Red Team** before production alert validation.
- Created triage guides and evidence checklists for consistent escalation and containment.

- Summarized incident trends and logging limitations for targeted monitoring investments.
- Correlated endpoint, network, **identity**, and cloud events during distributed business operations.

Junior Security Analyst

June 2013 - July 2014

Lakeview Technology Services

Cleveland, Ohio

Supported managed customer monitoring and incident triage under senior analyst supervision. Built foundational skills in SIEM investigation, endpoint analysis, threat hunting, lab validation, case documentation, and customer communication.

- Reviewed SIEM alerts and endpoint activity during managed customer monitoring operations.
- Correlated host, network, and identity records for **PowerShell**, **malware**, and authentication events.
- Documented triage steps and escalation criteria for smoother responder and customer handoffs.
- Built threat-hunting queries and dashboards for Windows, **DNS**, **proxy**, and endpoint data.
- Assisted isolated lab exercises covering command-and-control, **persistence**, and evasion behaviors.
- Prepared case notes preserving timelines, affected assets, evidence, and follow-up actions.

PROJECTS

Crown-Jewel Detection Validation Program 2026

Created repeatable purple-team scenarios for high-blast-radius systems, combining Caldera, Atomic Red Team, Sigma, KQL, and customer telemetry to measure prevention, visibility, alerting, and response coverage.

Cloud Identity Abuse Emulation 2024

Recreated cloud identity attack paths with Scythe and Sentinel analytics, giving SOC teams practical evidence for tuning detections, improving investigations, and prioritizing control changes.

LEADERSHIP & AWARDS

- MDR Detection Innovation Award, Northstar Defense Analytics, 2024
- Client Defense Partnership Award, Redwood Signalworks, 2020
- SOC Excellence Recognition, Blue Meridian Systems, 2015

EDUCATION

Bachelor's Degree in Cybersecurity

2013

Kent State University GPA: 3.8

Kent, Ohio

Coursework: *Network Security, Digital Forensics, Secure Systems, Incident Response*

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP) 2024
- GIAC Certified Forensic Analyst (GCFA) 2022
- Certified Red Team Operator (CRTO) 2020
- Offensive Security Certified Professional (OSCP) 2017

TECHNICAL SKILLS

- **Purple Team Tools:** Caldera, Atomic Red Team, Prelude
- **Emulation Platforms:** Scythe, Caldera, Atomic Red Team
- **SIEM Platforms:** Splunk, Microsoft Sentinel, SIEM
- **EDR Platforms:** CrowdStrike Falcon, EDR, endpoint telemetry
- **Detection Languages:** Sigma, KQL, Splunk searches
- **Scripting Languages:** Python, PowerShell, Bash
- **Threat Frameworks:** MITRE ATT&CK, adversary tradecraft, attack paths
- **Telemetry Sources:** Endpoint telemetry, network telemetry, cloud telemetry
- **Security Operations:** MDR, MSSP, SOC operations
- **Offensive Techniques:** Command and control, evasion, credential access
- **Detection Practices:** Threat hunting, detection validation, content development
- **Reporting Methods:** Executive reporting, customer reporting, coverage assessment

SKILLS

- Adversary Emulation
- Threat Hunting
- Evasion
- CrowdStrike Falcon

- Purple Team Operations
- Offensive Security
- Detection Engineering
- Incident Response
- MITRE ATT&CK
- Command and Control
- SIEM and EDR
- Splunk
- Microsoft Sentinel
- Detection Validation
- Customer Reporting

PROFESSIONAL AFFILIATIONS

- Purple Team Community Mentor, Kansas City Cybersecurity Meetup, September 2023 - Present
- Adversary Emulation Workshop Facilitator, Midwest Security Collective, January 2021 - Present
- University Cyber Defense Competition Coach, Kent State University, September 2018 - May 2020

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST