Saoirse Kelly Junior Incident Response Engineer

San Francisco, CA · saoirse.kelly@gmail.com · +1 415-555-0137 · linkedin.com/in/saoirsekelly

PROFILE SUMMARY

- **Junior Incident Response Engineer** with **3 years** in SOC and DFIR work, now handling **BEC and ransomware cases** for a **cyber insurer's small business policyholders**, after a year at an **MSSP**.
- Works daily in **Microsoft 365** and Entra ID logs, collects evidence with **KAPE** and Velociraptor, contains hosts with **SentinelOne**, parses artifacts with Eric Zimmerman's tools, and writes basic **Python** and PowerShell.
- Building depth in **Windows artifact analysis**, **Unified Audit Log searches** and **timeline building**, following the team's NIST 800-61 case steps so every finding ties back to **hashed, logged evidence**.
- Works with **senior responders**, the **claims team** and **breach coach counsel** on every case, and walks **policyholder IT contacts** through evidence collection when the business has no security staff.
- Keeps the **BEC playbook** and the team's **UAL query library** up to date, shows new SOC hires how to read **Windows event logs**, holds **GCIH**, and is studying for **GCFA**.

TECHNICAL SKILLS

Frameworks & Certifications:	NIST 800-61, SANS PICERL, MITRE ATT&CK (basics), GCIH
EDR & SIEM:	SentinelOne Singularity, Microsoft Defender for Endpoint, Splunk (SPL), KQL (basics)
Forensic Collection & Timelines:	KAPE, Velociraptor (collections), FTK Imager, Eric Zimmerman's Tools, chain of custody
Memory & Malware Analysis:	ANY.RUN, Joe Sandbox, Volatility 3 (basics), YARA (basics)
Network & Packet Analysis:	Wireshark, Zeek logs, Suricata alerts, firewall and VPN logs
Cloud & SaaS Logs:	Microsoft 365 Unified Audit Log, Microsoft Entra ID sign-in logs, Google Workspace audit logs
Scripting, SOAR & Threat Intel:	PowerShell, Python (basics), MISP, VirusTotal, Jira

EDUCATION

San José State University — **B.S. in Forensic Science, Digital Evidence** — San Jose, CA · Aug 2019 to May 2023

GIAC — **GCIH certification** — San Francisco, CA · Mar 2025

WORK EXPERIENCE

Coalition Inc. — **Junior Incident Response Engineer** — San Francisco, CA · Oct 2024 to Present

- Ran the first call with policyholders after each claim, setting severity and the evidence plan under **SANS PICERL**, and started collection the same day on **91%** of cases.
- Scoped **68 business email compromise** cases in **Microsoft 365** tenants, tracing attacker sign-ins, inbox rules and MailItemsAccessed events through the **Unified Audit Log** and **Entra ID** sign-in logs.
- Collected **KAPE** triage from Windows servers on ransomware cases and parsed event logs, Prefetch and Amcache with **Eric Zimmerman's tools**, finding the attacker's first logon on **19 of 22** cases.
- Deployed **SentinelOne** across policyholder networks at the start of ransomware cases, isolating infected hosts and blocking AnyDesk and Rclone on **2,140 endpoints** before the attacker could get back in.
- Wrote the team's **BEC investigation playbook** with ready-made Unified Audit Log searches, cutting the time a new analyst needs to scope a mailbox case from 2 days to **6 hours**.

NTT DATA — **SOC Analyst** — Omaha, NE · Jul 2023 to Sep 2024

- Triaged **Suricata** and firewall alerts for managed security clients, checking **Zeek** connection and DNS logs for beaconing, and escalated **37 confirmed compromises** to the incident response team.
- Detonated suspicious attachments and downloads in **ANY.RUN**, pulling C2 domains, hashes and dropped files from each report, and added **412 indicators** to the team's **MISP** instance.
- Ran weekly **Splunk** hunts for scheduled task and Run key persistence mapped to MITRE ATT&CK, which found **6 infected hosts** that no existing alert had caught.