Dahlia Stein Principal Incident Response Engineer

Boca Raton, FL · dahlia.stein@gmail.com · +1 561-555-0182 · linkedin.com/in/dahliastein

PROFILE SUMMARY

- **Principal Incident Response Engineer** with **13 years** of **DFIR consulting** at 2 response firms, leading **ransomware, extortion and cloud intrusion cases** for clients sent by **cyber insurers and breach counsel**.
- Sets the team's tooling across collection (**Velociraptor**, KAPE), forensics (**Magnet AXIOM**, X-Ways), timelines (**Timesketch**), reversing (**IDA Pro**, Ghidra), EDR (**SentinelOne**, CrowdStrike) and **Python**.
- Expert in **ransomware recovery planning**, **Microsoft 365 token theft** and **data theft scoping**, and writes final reports that **counsel, insurers and regulators** can rely on when they decide who gets notified.
- Works with **breach coach counsel**, carrier claims teams, **threat actor negotiators** and client **IT and executive teams**, runs the daily bridge on major cases, and joins board briefings alongside counsel.
- Leads the firm's **DFIR methods group**, trains new responders on **Velociraptor** and **memory forensics**, has coached **6 analysts** into senior roles, and holds **GCFA**, **GNFA** and **GREM**.

TECHNICAL SKILLS

Frameworks & Certifications:	NIST 800-61, SANS PICERL, MITRE ATT&CK, Cyber Kill Chain, GCFA, GNFA, GREM
EDR & SIEM:	SentinelOne Singularity, CrowdStrike Falcon, Microsoft Defender for Endpoint, Splunk, Microsoft Sentinel (KQL)
Forensic Collection & Timelines:	Velociraptor (server and hunts), KAPE, Magnet AXIOM, X-Ways Forensics, FTK Imager, Plaso, Timesketch
Memory & Malware Analysis:	Volatility 3, MemProcFS, IDA Pro, Ghidra, x64dbg, YARA, CAPA
Network & Packet Analysis:	Zeek, Arkime, Wireshark, NetFlow, RITA
Cloud & SaaS Logs:	Microsoft Entra ID, Microsoft 365 Unified Audit Log, AWS CloudTrail, Azure Activity Logs, Okta System Log
Scripting, SOAR & Threat Intel:	Python, PowerShell, Sigma, Cortex XSOAR, MISP, VirusTotal

EDUCATION

George Mason University — **M.S. in Computer Forensics** — Fairfax, VA · Aug 2011 to May 2013

GIAC — **GCFA, GNFA and GREM certifications** — Washington, DC · 2015, 2017 and 2019

WORK EXPERIENCE

Arete — **Principal Incident Response Engineer** — Boca Raton, FL · Mar 2020 to Present

- Led the response on **58 ransomware and extortion cases**, running the daily bridge with breach coach counsel, the insurer and client IT from first call to closure under NIST 800-61.
- Planned containment and rebuild for a manufacturer whose whole **VMware ESXi** estate was encrypted, resetting every privileged account and krbtgt twice, and got core ERP back online in **6 days**.
- Wrote the firm's method for **Entra ID** and **Microsoft 365** token theft, including OAuth app abuse and device code phishing, cutting median cloud scoping time from 5 days to **2**.
- Built the **Velociraptor** collection kit every engagement starts with, hashing and logging each artifact for chain of custody, and cut time to first triage data from 2 days to **9 hours**.
- Reversed encryptors and exfiltration tools from new ransomware groups in **IDA Pro** and Ghidra, writing **YARA** rules and IOC packs the team has since run on **212 cases**.

Kroll Cyber Risk — **Senior DFIR Consultant** — Washington, DC · Jul 2013 to Feb 2020

- Rebuilt the exfiltration path in a law firm breach from firewall logs, NetFlow and **Zeek**, proving to counsel that **38 GB** left over WinSCP, which set the notification scope.
- Ran compromise assessments for private equity buyers before acquisitions, hunting across **CrowdStrike** and **Splunk** data mapped to MITRE ATT&CK, and found active intruders at **7 of 41** targets.
- Ran ransomware tabletop exercises for client executives and IT teams, then rewrote their IR plans around the gaps, growing the readiness retainer list from 8 clients to **35**.