Jamin Becker

Engineering Manager · Detection Platform · Cybersecurity

Charlotte, NC
linkedin.com/in/jaminbecker
github.com/JaminB

SUMMARY

Grounded in security operations, with hands-on experience across incident response, malware analysis, and threat detection, before transitioning into software engineering and technical leadership. Spent several years as a staff engineer in FireEye's R&D group, co-founded two security companies, and now manage the Detection Platform at Huntress, protecting over 5 million endpoints and 11 million identities. Technically engaged and comfortable going deep, with a security practitioner's perspective on building and leading effective teams.

EXPERIENCE

Huntress

Apr 2022 – Present · 4 yrs

Senior Software Engineering Manager · Detection Platform

May 2025 – Present · Remote

- Manage the Detection Platform engineering org, responsible for the systems and pipelines powering threat detection across over 5 million endpoints and 11 million identities.
- Support R&D of novel detection techniques operating at over 2 million events per second.
- Own hiring, performance management, and career development for a team ranging from entry-level to principal engineers.
- Lead development of a SOAR orchestration layer and its integration with our agentic systems.
- Work with product, threat research, and SOC leadership to define and maintain the multi-year detection infrastructure roadmap.

Developer Tech Lead · Manager · R&D

Jul 2022 – May 2025 · 2 yrs 11 mos · Remote

- Led detection tooling development that improved the SOC's ability to triage and respond to incidents at scale.
- Built integrations across TIP, malware analysis pipelines, and EDR/M365 enrichment for real-time alert context.
- Migrated critical workflows to Apache Airflow and AWS Lambda, improving reliability and reducing manual operations.
- Shipped a detection rule builder and search engine used daily by detection engineers and SOC analysts.
- Built core APIs and interfaces that underpin Huntress's detection platform.

Senior Threat Operations Developer · R&D

Apr 2022 – Jul 2022 · 4 mos

- Built tooling for the Threat Operations team to accelerate threat research and expand detection coverage.

Dynamite Analytics

Feb 2019 – Jun 2023 · 4 yrs 5 mos

Co-Founder · Advisor

Apr 2022 – Jun 2023 · Remote

- Moved into an advisory role after hiring full-time leadership; continued providing technical and strategic input.

CTO & Co-Founder

Apr 2019 – Apr 2022 · 3 yrs 1 mo · Remote

- Co-founded a cyber threat intelligence company (formerly Vlabs) focused on giving security operators better tooling for detecting complex attacks.

- Set technical direction, hired the engineering team, and led product R&D across network analysis and threat intelligence.
- Shipped DynamiteNSM, an open-source NSM platform built on Zeek and Elasticsearch (171 GitHub stars).
- Maintained integrations with threat feeds and SIEMs; active contributor to the open-source security community.

Senior Software Engineer Feb 2019 – Apr 2019 · 3 mos · Atlanta Metropolitan Area

PacketTotal LLC · Acquired June 2021

Feb 2019 – Jun 2021 · 2 yrs 5 mos

Creator & Founder Remote

- Built PacketTotal from scratch: a free PCAP analysis engine for network traffic visualization, timeline reconstruction, and artifact extraction.
- Grew to wide adoption across the security community; acquired June 2021.
- Designed and built the full stack solo: backend pipeline, analysis engine, and frontend.

FireEye, Inc.

Apr 2017 – Feb 2019 · 1 yr 11 mos

Staff Software Engineer · Innovation & Custom Engineering (R&D) Remote

- Built forensic tooling within FireEye's Innovation and Custom Engineering (ICE) R&D group, used directly by Mandiant consultants on engagements.
- Built a Python application that simplified O365 forensic investigations for IR teams, replacing complex manual tooling.
- Worked with the data science team to automate ML model deployments into production.
- Contributed to a bootkit detection capability running on AWS Lambda.

SPX Corporation

Sep 2015 – Apr 2017 · 1 yr 8 mos

Senior Information Security Engineer Ballantyne, NC

- Reported directly to the CISO, covering vuln management, incident response, software development, and remediation.
- Wrote an event forwarder daemon to integrate the endpoint solution with the enterprise SIEM.
- Built a multi-threaded share scanner to identify PII and sensitive IP on open Windows shares.
- Consolidated security tools into a centralized ELK-based log management and alerting stack.
- Led deployment of security controls across corporate infrastructure.

Bank of America

Sep 2014 – Sep 2015 · 1 yr 1 mo

VP, Security Engineer · Specialist Charlotte Metro

- Built BI tooling for Global Information Security's recovery group, consolidating security data into board-level metrics and reports.
- Wrote root-cause analysis and risk quantification algorithms operating across enterprise-scale security datasets.
- Built an automated phishing email evaluation engine deployed enterprise-wide.
- Developed a SQL-like query language for automatic security report generation.
- Built custom reporting and data collection platforms for Global Information Security teams. (Patent: Information Management and Notification System)
- Managed the GRC platform transition, automating workflows to reduce manual overhead.

TIAA-CREF

Sep 2013 – Sep 2014 · 1 yr 1 mo

Incident Response · Information Security Analyst — Charlotte Metro

- Monitored and responded to threats using ArcSight, Splunk, and Security Onion in a large financial institution.
- Built custom ArcSight plugins integrating with multiple network infrastructure APIs.
- Built a custom API and analyst UI to automate triage tasks and support team collaboration.
- Performed malware analysis with IDA Pro and Cuckoo Sandbox, and PCAP analysis with Wireshark and custom Python scripts.
- Helped deploy and configure multiple IDS platforms.

SKILLS & TECHNOLOGIES

MANAGEMENT

`Eng Management` `Hiring` `Roadmapping` `Mentorship` `Technical Leadership` `Shape Up`

SECURITY

`Detection Engineering` `Threat Intelligence` `DFIR` `Malware Analysis` `PCAP Analysis` `Zeek` `Suricata`

ENGINEERING

`Python` `JavaScript` `AWS` `Apache Airflow` `Elasticsearch` `Django` `Linux` `Claude Code` `AI Dev Workflows`

OPEN SOURCE & NOTABLE PROJECTS

PacketTotal

Acquired · 2021

Free PCAP analysis engine for network traffic visualization, timeline reconstruction, and artifact extraction. Built solo from scratch; acquired June 2021. Featured in *Help Net Security*.

`Python` `PCAP` `Network Analysis` `Threat Intel`

DynamiteNSM

github.com/DynamiteAI/dynamite-nsm

Open-source Network Security Monitor built on Zeek and Elasticsearch. **171 GitHub stars, 23 forks.**

`Python` `Zeek` `Elasticsearch` `NSM`

HoneyBot

Scripts and libraries for capturing and correlating packet captures alongside PacketTotal, enabling automated honeypot data collection.

`Python` `Honeypot` `PCAP`

FileProxy

github.com/JaminB/FileProxy

Unified REST API that abstracts access to cloud storage backends (S3, Google Drive, Dropbox, Azure Blob) with encrypted credential management.

`Python` `Django` `AWS` `REST API`

PRESS, PUBLICATIONS & TALKS

HUNTRESS BLOG	Time Travelers Busted: How to Detect Impossible Travel	2023
DYNAMITE ANALYTICS	PacketTotal Community Service — Webcast Presenter	2020
TRELLIX (FIREEYE)	BIOS Boots What? Finding Evil in Boot Code at Scale!	Aug 2018
LINKEDIN PULSE · AUTHOR	Deriving Threat Intelligence from Packet Captures	2018
LINKEDIN PULSE · AUTHOR	What I Learned from Building a Network Analysis Service from Scratch	2017
BLEEPINGCOMPUTER	PacketTotal: A Useful Site for Analyzing PCAP Files	Feb 2017
HELP NET SECURITY	PacketTotal: A free, online tool for analyzing packet captures	Feb 2017

EDUCATION

University of North Carolina at Charlotte Sep 2011 – Aug 2016

Bachelor of Science, Computer Science