Jim Saveker

Detection and Response

Austin, TX

james@saveker.org

(212) 960-8469

www.saveker.org

linkedin.saveker.org

@jim@toot.saveker.org

jsaveker

SKILLS

Cyber Risk Assessment

Threat Modelling

Incident Response

Threat Intelligence

Technical Management

Management Reporting

CERTIFICATIONS

Certified Ethical Hacker (February 01, 2005)

EC | Council

ECC36182073212

Architecting with Google Cloud Platform (November 12, 2018)

Coursera

S73L5GAZFB3G

Elastic Google Cloud Infrastructure: Scaling and Automation (November 12, 2018)

Coursera

H98E32XVLJRK

Elastic Cloud Infrastructure: Containers and Services (November 12, 2018)

Coursera

WE9JSRQD93PR

PUBLICATIONS

Embracing Threat Informed Defense (February 01, 2023)

Blog

Embracing Threat Informed Defense helps defenders sharpen their focus and improve cybersecurity risk posture.

Jim is an experienced cyber risk professional with over 17 years of experience. His key focus areas include regulatory compliance, forensic investigations, and cyber incident detection and response.

WORK EXPERIENCE

Google

(March 01, 2019 - Present)

Security Engineering - Detection and Response

Senior TPgM in the Security Surveillance Team, which is responsible for addressing state-sponsored and other malicious activity targeting Google's networks and users.

Threat Informed Defense (TID) – Program Lead

Built and led a team tasked with measuring cyber threat detection coverage and effectiveness across Google and Alphabet companies. Informed engineering priority for gaps relating to highest severity threats. Standardized nomenclature for describing badness across Alphabet.

Crown Jewels Program – Infrastructure Pillar Lead

Established an infrastructure Crown Jewels category to highlight infrastructure that supports mission-critical business processes that have a material impact on Alphabet and its users if compromised. Populate detection engineering backlog with Crown Jewel threat scenarios to prioritize mitigations alongside all other enumerated threat sources.

End Point Security - Vendor Assessment, Selection, and Engagement

Implement best-in-class endpoint telemetry by building in-house or buying vendor solutions.

www.google.com

PwC

(April 01, 2005 - March 01, 2019)

Director - Security Privacy and Risk

Information Security Consultant with specialist knowledge of Digital Forensics, Incident Response, Regulatory Compliance, and Cybersecurity Strategy.

Examples of client engagements

- Cyber Breach – Remediation at a Global Financial Services Organization
- Cyber Incident Response Planning – Hedge Fund
- Threat & Vulnerability Management (TVM) at a Global Financial Services Organization
- Global PCI DSS Assessment at an Insurance Organization
- Forensic Investigations (Fraud and Corruption) – Investment Banking
- Data Governance - Investment Banking

www.pwc.com