JIM **SAVEKER**

Austin, TX · cell (212) 960-8469
james@saveker.org · linkedin.com/in/jamessaveker

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.

EXPERIENCE

03/2019 – PRESENT

TPM – DETECTION & RESPONSE, GOOGLE LLC (AUSTIN, TX)

Threat Informed Defense (TID) – Program Lead

Built and led 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.

- Designed and led the development of a threat data pipeline enumerating business risks, associated threat scenarios, and attack chains of atomic behaviors, otherwise known as Tactics, Techniques, and Procedures (TTPs).
- Led the development of supporting tooling integrated into the detection pipeline (controls as code) to support the measurement of detection coverage, posture, and effectiveness as it relates to specific threat actors, nation-states, or specific campaigns.
- Engaged with teams responsible for preventative controls, supporting a single pane of glass view of the preventive and detective controls surface.
- Led reporting and review forum to provide transparency to tech lead managers and support business decision-making to allocate engineering resources to counter threats relating to Alphabets' most severe risks.
- Built custom reports for leadership measuring defensive posture against multiple dimensions such as target actors, geographic locations, attack techniques, and motivation.
- Enriched incidents with context based on observed threat intelligence to support security engineers conducting investigations.
- Created, implemented, and managed processes to perform detailed detection analysis of Red Team exercises. Recorded observations as threat scenarios and resulting attack chains (groups of TTPs) processed by the threat data pipeline to populate control gap analysis and feed a prioritized backlog of detection engineering work.

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.

- Interview product area leadership to understand what keeps them up at night and what are the most important mission-critical business processes.
- Conduct a Threat model for each mission-critical business process, risk rank based on probability and impact criteria, and derive Threat Scenarios with the highest risk.

- For each Threat Scenario, count related infrastructure components that may be logically affected.
- Feed results into the TID pipeline to prioritize remedial work alongside other threat sources.

End Point Security - Vendor Assessment, Selection, and Engagement

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

- Conducted Endpoint Detection & Response (EDR) market analysis and created a model to asses vendors against business requirements.
- Evaluated the performance of shortlisted vendors and produced reports of findings for business with recommendations and rationale.
- Negotiated terms, secured funding and executed contract with selected vendor.

12/2012 – 03/2019

DIRECTOR – SECURITY, PRIVACY & RISK, PWC LLP (NEW YORK, NY)

Cyber Breach – Remediation at a Global Financial Services Organization

- Operated as “two in a box” with CIO of an organization that underwent a significant breach. Supplied executive leverage and support in designing global remediation programs.
- Designed and led key workstreams in a $150M remediation program focused on E2E vulnerability management, threat-informed defense, and supply chain risk.

Cyber Incident Response Planning – Hedge Fund

- Developed and socialized incident response plan for CISO and helped set up a Cyber Incident Response Team (CIRT), including representation from the business.
- Developed and conducted cyber threat war gaming/tabletop exercises to help the client to evaluate their cyber threat response and organizational preparedness, stress testing the newly implemented incident response plan.
- Evaluated the performance of various teams during the scenario, analyzed gaps, and provided the client with details of their areas of improvement and potential vulnerabilities.

End to End Threat & Vulnerability Management (TVM) at a Global Financial Services Organization

- Developed End to End TVM Target Operating Model based on industry-leading practice and developed a roadmap for implementation.
- Aided in implementing technology such as RiskSense and integrated with the organizations' asset management system (ServiceNow) and governance, risks, and control (GRC) system Archer.
- Integrated tools such as Rapid7 and Tanium in support of program compliance.
- Defined internal threat and vulnerability risk rating framework.
- Created Policies and Standards to enforce program governance.
- Developed program metrics and dashboards for management reporting.

Global PCI DSS Assessment at an Insurance Organization

- Led a global PCI-DSS v3 assessment on a client’s operations across the Middle East and Western Europe.
- Worked closely with local IT representatives in each country to produce a detailed Data Flow Diagram (DFD) detailing the flow of card data through the client’s environment.
- Reviewed the current policies, processes, working practices, and technologies against the PCI Data Security Standard (PCI DSS) for in-scope systems.

- Produced detailed gap assessment reports and recommended remedial actions to pursue compliance.

04/2005 – 12/2012

MANAGER – FORENSIC TECHNOLOGY SOLUTIONS, PWC LLP (LONDON, ENGLAND)

Forensic Investigations (Fraud and Corruption) – Investment Banking

- Mapped the client's data to decide which information sources could be relevant, capture the relevant information in a forensically sound manner, and make it available to the investigators and lawyers to recover assets (IP) and funds involved in a significant identified fraud event.
- Led an internal investigation into a rogue trader involving the capture and analysis of email, telephone conversation recordings, call records, Reuters, and Bloomberg chat transcripts, reports from bespoke trading systems, and analysis of the trader's desktop PC. Wrote witness statement in support of the criminal prosecution.

Data Governance - Investment Banking

- Established a Data Governance Program and Long-Term Data Management Strategy, including associated policies, processes, and procedures to assess risk, improve quality, and control the dissemination of data between the business, affiliate entities, regulators, and third-party vendors.
- Conducted discovery, inventory, and classification of data held by the business across more than 8,000 applications hosted within multiple data centers and circa 100,000 data archive tapes across Europe.
- Triaged information systems of strategic value to the business and documented 80 critical bespoke systems, confirming data, and developing a reporting framework.
- Created an application rationalization program to reduce operating costs whilst continuing to supply data to the business and external parties.
- Preserved existing data controlled by the business, including review of data retention policies in line with regulatory requirements.
- Established strategic relationships and negotiated contractual terms with vendors to supply essential services to enable the business to meet its legal and regulatory responsibilities.

FRAMEWORKS & REGULATORY REQUIREMENTS

- Office of the Comptroller of the Currency (OCC) - Heightened Standards for Large Financial Institutions
- Federal Financial Institutions Examination Council (FFIEC) - Cybersecurity Assessment Tool
- Center for Internet Security (CIS) - Critical Security Controls
- Payment Card Industry Data Security Standard (PCI-DSS)
- New York State Department of Financial Services (NYDFS) - Part 500 and 504
- EU General Data Protection Regulation (GDPR)
- National Institute of Standards and Technology (NIST) 800-53 - Cyber Security Framework
- SWIFT Customer Security Program (SWIFT CSP)
- Mitre Att&ck Framework