

David J. Tortora

Security Program Leadership · Incident Command · Insider Threat & Investigations

Build the program, develop the people, leave a function that runs without me.

Remote, or New York City metro

[LinkedIn](#) | [tortora.dev](#) | [stateofthethreat.com](#) | [stateoftheattack.com](#) | [stateofthedefense.com](#)

Last updated September 2026

SUMMARY

Security leader with 25+ years across security program development, incident command, and team leadership, who builds programs that outlast any one person. Built Thrive's Incident Commander function from zero, methodology through knowledge base, and directed the full P1 and P2 incident load through it for an international MSSP serving 2,000+ clients globally, from declaration through restoration and across time zones from the West Coast to Hong Kong.

Background spans the U.S. Marines (three tours in Iraq, squad to platoon-scale leadership) and a decade as a senior detective in financial crime, cybercrime, and digital forensics, bringing an investigator's lens to enterprise risk. Coordinated with FBI, CISA, and the UK NCSC on multi-jurisdictional matters.

Author of State of the Threat, State of the Attack, and State of the Defense. One intelligence shop, three perspectives: the threat brief tells your board what's coming, the attack analysis shows your SOC what it looks like, and the defense case study shows your team why the controls that should have been there weren't.

LEADERSHIP HIGHLIGHTS

- **Built a function from zero.** Stood up Thrive's Incident Commander capability: methodology, playbooks, escalation model, and knowledge base. Directed the full P1 and P2 incident load through it, from routine outages through full-scale ransomware, coordinating teams of up to 20 on sustained incidents. Led every major engagement through to the end of the role.
- **Designed the IR program architecture.** Authored the CRU (Containment & Remediation Unit) business proposal. Designed the Deputy IC role to scale CIRT capacity. Built the CIRT Readiness program with executive tabletop exercises that put client leadership through an incident before a real one arrives.
- **Turned incident patterns into prevention.** Ran monthly IC Office Hours across regions, taking what was going wrong on live incidents back to internal stakeholders so they could advise their own clients on the same gaps before it happened to them.
- **Led the ransomware recovery that converted a \$500K contract.** Led the response for a non-client prospect during an active ransomware event. The trust earned converted the relationship into a \$500K contract.
- **Compressed industry-standard recovery timelines.** Led ransomware recovery on a 10-server encryption event: containment through restoration in 24 hours against a 5-to-7-day industry standard.
- **Applies AI operationally, not theoretically.** Built an AI-assisted analysis workflow that turns first-party observation and open-source collection into documented threat-actor TTPs and published intelligence, sustaining a daily executive brief with long-form analysis on Sunday. AI accelerates collection and first-pass synthesis. The analysis and the call stay human.
- **Initiated Thrive's NCSC partnership.** Built standing relationships across the FBI, CISA, and the UK NCSC, and enrolled clients in the NCSC program so UK notifications route through Thrive ahead of NCSC direct outreach.

CORE COMPETENCIES

Security Strategy & Program Design · CSIRT / CIRT Design & Buildout · Incident Command & Major Incident Management · Executive Risk Communication · Breach Counsel & Cyber Insurance Coordination · Federal Agency Coordination (FBI, CISA, NCSC) · Tabletop Exercise Design & Facilitation · Financial Crime & Fraud Risk · Digital Forensics Program Leadership · Methodology, Playbook & Policy Development · Regulated Environments (Financial Services, Healthcare, CJIS) · AI-Assisted Workflow Design · Threat Intelligence Strategy & Publication · Team Development & Mentorship

Frameworks. MITRE ATT&CK · NIST CSF · CMMC · PCI-DSS · CIS Controls

Technical environment. Elastic/ELK · FortiSIEM · SentinelOne · Binalyze · AWS · Google Cloud · Cloudflare · Endpoint, network, cloud, and forensic-image analysis · OSINT · Blockchain and crypto tracing

EXPERIENCE

SECURITY INCIDENT COMMANDER

Thrive · International MSSP, headquartered in Foxborough, MA

06/2025 to 07/2026

Sole Incident Commander for a global client base. Directed every P1 and P2 incident from the West Coast to Hong Kong, from declaration through restoration, coordinating teams of up to 20 on sustained incidents. Set the direction of the investigation, tasked the technical teams, and translated findings into business risk. Built the function alongside the casework: playbooks, automation, supporting roles, and partnerships.

- **Program build.** Shipped processes, playbooks, and knowledge base articles for the Incident Commander function. Tested playbooks. Post-incident reviews that changed behavior. Included the CRU business proposal, Deputy IC role design, and CIRT Readiness program with executive TTX.
- **Executive advisory during incidents.** Translated threat data into business impact for C-suite leadership during active incidents. Delivered facts, options, and pathways forward in real time.
- **Breach response coordination.** On a breach there are a lot of parties at the table: in-house and external breach counsel, third-party forensic firms, and the cyber insurance carrier. Pulled it together so each of them got what they needed and the client had one person to deal with while they got back up and running. Read early where the matter was heading (litigation, regulator, or claim) and preserved the evidence, chain of custody, and privilege before anyone asked, so nobody had to rebuild it later.
- **Federal and international coordination.** Worked with the FBI, CISA, and the UK NCSC when a matter crossed borders. Initiated Thrive's NCSC partnership, establishing the channel through which UK client notifications reach Thrive ahead of NCSC's direct outreach.
- **Cross-region program leadership.** Stood up IC Office Hours as a recurring engagement for internal stakeholders and Service Delivery UK, aligning incident response practices across regions.

DETECTIVE, CYBERCRIME & FINANCIAL CRIMES

Bergenfield Police Department

09/2015 to 09/2025

Hundreds of cases over a decade, from graffiti to homicide, with specialization in financial crime, cybercrime, and digital forensics. Worked million-dollar fraud cases using digital forensics, OSINT, and blockchain analysis. Coordinated with FBI and federal partners on complex matters.

- **Built the department's digital forensics program from zero.** Established procedures, acquired tooling, and trained detectives to handle digital evidence independently. No prior capability or budget.
- **Secured a grant for cryptocurrency-tracing tooling.** Identified the capability gap, secured the grant, integrated the tooling into investigative workflows, and trained the team. Zero cost to the department.
- **Designed and ran a fraud awareness program for local businesses.** Deployed detection tooling and ran workshops that measurably reduced fraud vulnerability across the community.
- **Closed a cold case missing persons case dating to the 1970s.** Maintained continued engagement with the family over years; coordinated with NamUs to secure a DNA match that closed the case.
- **Designed and delivered an active-shooter response program for 40+ personnel.** Scenario design, facilitated drills, and readiness measurement.
- **Applied for subpoenas, authored and executed search warrants, held chain of custody, and testified in court** across financial crime, cybercrime, and digital forensics cases. Court-qualified expert witness. Full detail at tortora.dev/investigations.

PRINCIPAL

ADS Risk Solutions LLC

03/2025 to Present

- Independent security risk assessment practice (adsrisk.com): structured controls review against recognized standards, cyber insurance application and customer security questionnaire verification, CMMC position analysis, and executive incident-readiness tabletops. No products, no resold licenses, no commissions.

EARLIER ROLES

PATROL OFFICER

Bergenfield Police Department

07/2010 to 09/2015

- Made scene-level decisions during criminal incidents, domestic violence, and mental health crises. Ran preliminary investigations, directed scene preservation, and coordinated handoffs to detectives.
- Drove patrol operations compliance that contributed to the department's successful CALEA national accreditation.
- MADD Enforcement Award recipient for DUI enforcement results.

CORRECTIONS OFFICER

Bergen County Sheriff's Department

06/2009 to 07/2010

- Designed and launched a cross-training program across housing units that reduced overtime costs and improved shift coverage facility-wide.
- Responsible for security and regulatory compliance across a 1,000+ inmate population.

LABORER

East Rutherford Department of Public Works

2007 to 2009

STAFF SERGEANT, U.S. MARINE CORPS

U.S. Marine Corps, Twentynine Palms, CA

2003 to 2007

- **Three tours in Iraq.** Led teams scaling from a squad to a full platoon, with accelerated promotion each deployment cycle.
- **Developed 50+ junior Marines and Naval officers** through cross-branch mentorship; 10 promoted under supervision.

COMPUTER & NETWORK ADMINISTRATOR

Rutherford Board of Education

1998 to 2003

- Supported systems, networks, and servers across six schools.
- Contributed to district-wide upgrades including hardware refresh, software, and security tool deployments.

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP)

ISC2

Certified CMMC Professional (CCP)

Cyber AB, ISACA-administered

Certified Financial Crimes Investigator (CFCI)

IAFCI

Certified Cyber Crimes Investigator (CCCI)

IAFCI

TEEX PER-371: Cybersecurity Incident Response and Management

Texas A&M TEEX, DHS/FEMA

TEEX Infrastructure Protection

Texas A&M TEEX, DHS/FEMA

SPECIALIZED TRAINING

- Threat Modeling: Embracing Worst-Case Scenarios
- Critical Infrastructure Resilience and Community Lifelines
- Critical Asset Risk Management
- Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness
- Critical Infrastructure Security and Resilience Awareness
- Cryptocurrency Investigations; Intermediate Cyber Investigations: Virtual Currency
- Advanced Digital Forensic Analysis: iOS & Android; Windows Acquisition; Digital Forensic Triage with EZ Tools
- Open Source Intelligence; Deep Web Searching; Dark Web Investigations
- Forensic Accounting and Fraud Examination; The Bank Secrecy Act; Suspicious Activity Reporting
- FBI Basic Historical Cell Site Analysis
- Court-qualified expert witness (Drug Recognition Expert certification); Basic Trial Testimony
- Proactive Police Supervision; First-Line Supervisor: Characteristics, Training, and Challenges

The complete training inventory, roughly 150 courses across financial crime, cryptocurrency, OSINT, digital forensics, legal process, critical infrastructure, and leadership, is published at tortora.dev/certs.

COMMUNITY @ INDUSTRY LEADERSHIP

ISC2 NJ Chapter (CISSP Study Group Lead)

InfraGard NJ

IAFCI

ISACA

ASIS International

PBA Local 309 (Former President, VP, Secretary)

Elected President of PBA Local 309, and previously Vice President and Secretary. Led the local's executive board, represented the membership, and handled contract negotiation and grievance resolution. Named Local of the Year during tenure.

PUBLISHING

One intelligence shop, three audiences: the board, the responders, and the teams closing the gaps. Built on first-party observation rather than aggregated vendor reporting. Detection rules and IOCs are shared on the sites and pushed to third-party registries including URLhaus and the other abuse.ch trackers, AlienVault OTX, and Open Source Malware.

- **State of the Threat** (stateofthethreat.com). Daily board-level brief translating geopolitical and regulatory risk into business impact for executives who have to answer to a board, with the long-form analysis on Sunday.
- **State of the Attack** (stateoftheattack.com). Full kill-chain analysis of single intrusions, from initial access to objective, written from first-party observation and shipped with detection rules and IOCs.
- **State of the Defense** (stateofthedefense.com). Case studies rebuilding real attack patterns through fictional companies to show where people, process, and technology each failed.

AWARDS

- MADD Enforcement Award
- PBA Local 309, Local of the Year
- Additional medals and commendations across U.S. Marine Corps and Bergenfield Police Department service