CYBER

THREATBOARD™

Data-Centric Platform for Threat Management

THREATBOARD: STATE-OF-THE-ART CYBER THREAT MANAGEMENT

ThreatBoard is Peraton's distributed, data-centric platform for cyber threat intelligence (CTI), threat management, and threat hunting. ThreatBoard provides autonomous capability to ingest all cyber threat data—from diverse sources, with different controls, forms, and formats—and to perform data aggregation, tagging, validation, enrichment, correlation, sharing, and analysis. Because ThreatBoard automates the correlation and contextualization of threat data and shows connections in graphical displays, it significantly accelerates the speed at which analysts can identify campaigns, detect advanced persistent threats (APTs), analyze incidents, deter attacks, and share threat intelligence.

ThreatBoard closes:

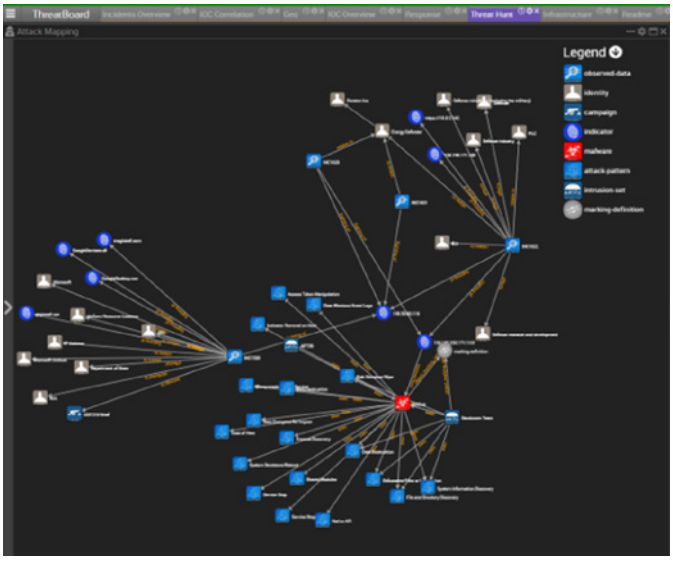
- Information gaps, by combining all cyber related data in one platform and breaking down data silos
- Knowledge gaps, by autonomously correlating and contextualizing data (indicators of compromise (IoCs), events, reports, email, etc.)
- Visibility gaps, by producing customizable and user-friendly graphical displays of CTI and relationships
- Time gaps, by accelerating attack detection
- Action gaps, by enabling both rapid attack mitigation and sharing of CTI to protect connected infrastructure

As cyberattacks increase in frequency, severity, and sophistication, so does the need for agile, actionable CTI and rapid threat detection and mitigation. Peraton's ThreatBoard meets this growing need. Built on a flexible and extensible data fabric architecture, ThreatBoard's "single pane of glass" offers a one stop integration point and state-of-the-art artificial intelligence (AI) and machine learning (ML) capabilities to identify and counter attacks that are stealthy, persistent, novel, widely dispersed, or dynamically changing.

ThreatBoard automatically ingests and synthesizes all cyber information, creating a cohesive, correlated, and operational picture of the complete threat landscape. ThreatBoard's visualizations depict relationships and connections among IoCs and incidents, so analysts can quickly see and identify patterns, threat actors, campaigns, malware, and more.

BENEFITS

- **Provides complete situational awareness** via comprehensive integration of threat data from diverse sources, forms, and formats across the enterprise, plus numerous 3rd party CTI data feeds
- **Reduces time, effort, and cognitive load on analysts** via automated, AI-driven correlation and contextualization of events and graphical display of the full threat picture and relationships
- **Shortens time frame to detect and deter attacks and resolve incidents**, including APTs, malware campaigns, and dispersed and multi-modal attacks
- **Supports wide collaboration and sharing** of CTI in conjunction with strong data governance
- **Automates analysis of cyber events**, increasing the knowledge base quicker and at lower cost
- **Flexible**, **extensible system** easily incorporates new sources of CTI, new format versions, emerging products, and extends to other threats (electronic warfare (EW), information warfare threats, etc.)



ThreatBoard graphic display depicting diverse IoCs, and events and their relationships in an attack map

KEY FEATURES

- Automatic data ingest with natural language processing (NLP) ingests, parses, and synthesizes all data from
  - disparate sources (on-premise sensors; cloud; IT, OT, and IoT networks; ICS and SCADA systems; edge devices, etc.),
  - diverse security domains, products, and feeds, and
  - in varying forms and formats (structured and unstructured data, text, email, code, metadata signatures, forensic reports, etc.)
- Automatic data markings identify and enforce terms of use, privacy laws, policy controls, and data storage / access rules for different types and sensitivities of data
- Multi-conditional correlation detects, tags, scores, and flags events based on mission parameters and user-defined criteria for confidence, severity, and priority
- AI-driven data enrichment and contextualization automatically builds a full picture of a potential threat
  - autonomously pre-fetches relevant CTI from 3rd party sources (Virus Total, Alien Vault, RiskIQ, Hybrid Analysis, Anomali, and more)
  - maps to multiple threat and attack matrices (MITRE, Vectra.AI, AM!TT, etc.).
  - uses ML to identify modified and novel threats
- Graphical displays depict the full threat picture, with correlated events and integrated views so analysts can quickly discover and investigate unusual patterns, stealthy attacks, and sophisticated campaigns.
- Flexible, extensible architecture and use of standard formats (STIX, MISP, etc.)
  - integrates with SIEM, SOAR, and systems for incident reporting and trouble ticketing
  - easily accommodates new format versions, new products, and new types of data and threats
- State-of-the-art data management supports intra- and inter-organization collaboration and CTI sharing, including governance and compliance with data restrictions, regulations, and policies
- AI-based analyst support provides intelligent search, efficient information retrieval, and access to ThreatBoard's expanding store of CTI, with automated question answering (QA) and natural language interfaces coming soon

STATUS AND PROOF POINTS

ThreatBoard is currently deployed in multiple federal agency teams responsible for cyber threat protection, management of CTI, and cyber threat analysis. ThreatBoard has proven capability to:

- Rapidly identify campaigns that were difficult, if not impossible, for analysts to uncover without its automated correlation and graphical displays
- Automate malware analysis—correlating, contextualizing, and detecting email phishing campaigns much faster and with significantly less cognitive load on analysts
- Deliver substantial speed-ups—from days to minutes—in de-duping and processing backlogged IoCs, correlating the IoCs to CTI data feeds, prior incidents, and remediations, and preparing structured reports for incident response teams
- Streamline workflows and standardize processes and procedures across activities and teams responsible for cyber threat hunting, cyber incident management, and threat reporting, yielding improvements in efficiency and responsiveness

ThreatBoard is Peraton's deployment-ready platform for CTI and cyber threat management. For more information on ThreatBoard, cyber managed services, and Peraton's full suite of mission capabilities for cyber defense, cyber resiliency, and integrated threat protection, contact:

threatboard@peraton.com

or Steve Relitz,

Cyber Systems Engineering

stephan.relitz@peraton.com

peraton.com/capabilities/cyber/