Arbitr Security

GIBSEN Threat Matrix™

The Arbitr ThreatOps Platform is a new way to visually present cyber incidents over time, providing a better understanding and context to respond to, remediate, and report attacks. We created a new visual language to display and report incidents named GIBSEN™ (Graphical Information Base for Security Event Notation) visual language. With GIBSEN, Arbitr enables you to observe each incident across multiple planes-of-attack, understand how the attack behaves, visualize the methodology used, and see the assets created or leveraged by the attack.

Threat Matrix Overview

The Arbitr Threat Matrix is a time drive map of the actions and behaviors of an adversary's attack. It is a visual map that sequences an incident from inception to completion across four major domains:

- **Cloud** (Hyperscalers/SaaS)
- **Networks** (Internal and External)
- **Hosts** (Servers, Endpoints, Appliances, Memory, Registry, Storage)
- **Operational Technology** (OT, IoT, Primary Logic Controllers)

Framework Alignment

The Arbitr Threat Matrix will also help you map to popular incident framework, including:

- MITRE ATT&CK Tactics®
- Mandiant Targeted Attack Lifecycle®
- Lockheed Martin Cyber Kill Chain®

Arbitr ThreatOps: The Defender's Advantage

In our popular media, vendor and analyst reports, and social media channels, the CISOs and defenders never win in the battle against threat actors. For every breach that makes the news and is ambulance chased by vendors (which we strive not to do), we are willing to bet that cyber defenders have thwarted thousands of attacks. While we know the battle against threat actors will never end, one of our primary objectives at Arbitr is to tip the fight in favor of the defenders. One of the profound insights that a matrix will demonstrate for you and your executive audience is that defenders only have to be right once; threat actors have to be right dozens of times to complete a successful breach.

Once you try Arbitr's ThreatOps platform (free to try), you will see new ways to create TTP (tools, techniques, and processes) rules using tools like Sigma—we help move the advantage to the defenders. We hope that Arbitr can make cyber incidents simple to consume, create recovery plans, and make both easily reportable for business, governance, cyber insurance, and technical audiences.

Cyber From The Incident Perspective

Arbitr takes the investigator's perspective, focusing on creating a simple, visible, focused, consumable, clean incident response storyline. We enable blue teams and threat hunters to create a shareable and collaborative cyber incident platform that is not a discussion forum but a consolidated visual timeline that builds a single end-to-end incident report that is specific, targeted, actionable, and reportable. This is the fundamental premise of the Arbitr ThreatOps platform. We help you deliver the actionable specifics required to respond to, remediate, and report to meet your organization's requirements. Arbitr provides the underlying data and understanding to map to leading cyber frameworks from MITRE ATT&CK, NIST, Google Mandiant, and others.

The GIBSEN Visual Language

The Arbitr Threat Matrix is based on our GIBSEN visual language. We use simple descriptive iconology to build an intuitive, time-driven representation of each cyber incident's processes, artifacts, and behaviors. GIBSEN accelerates understanding of cyber incidents, provides a basis for team training, and builds institutional knowledge that will often otherwise leave your organization. Each node in a GIBSEN diagram is a database structure that contains the artifact category, the technical details, forensic logs, and analyst commentary on the specific node. This allows you to create top-level executive views and drill down to forensics-level evidence for the most detailed analysis. GIBSEN diagrams enable you to quickly identify and remediate causal events or patterns to create TTPs to prevent entire families of attacks, not just individual IOCs.

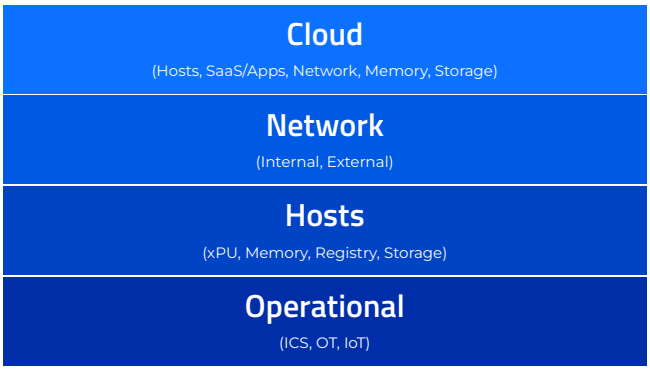
Arbitr GIBSEN Framework

Threat Matrix Planes based on the GIBSEN Framework

The core security planes in the GIBSEN framework are cloud, network, host, and operational technology. These planes represent the core active layers present within modern enterprises. Some items can live in multiple planes; a firewall is an excellent example. In one case, it can live in the network plane between internal and external networks. In another case, it could be used as a host when it acts as the platform for malware. This type of example can be true for many devices within the enterprise, and we will classify them based on their role in a given cyber incident.

Unlike topic-down network diagrams, GIBSEN produces threat matrix views driven by the incident's essential artifacts in a standardized and consistent format.

Arbitr GIBSEN Artifact Planes



Inside each GIBSEN plane lives the detailed analysis that accelerates understanding, provides actionable insights, and serves as a training tool for the entire security and risk management teams.

Cloud (Networks, Storage, SaaS/Apps, Websites)

- Hyperscalers
- Internet

Network

- Internal
- External

Host (xPU, Memory, Registry, Storage)

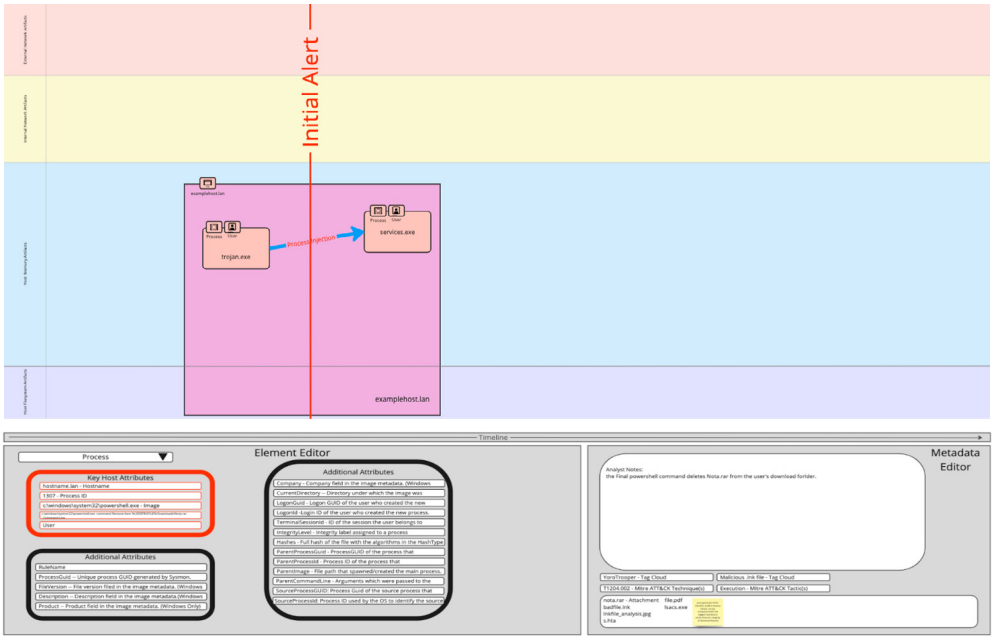
- Any discrete computing platform
- Any server
- Any endpoint/edge device
- Any appliance

Operation

- Industrial Control Systems
- Operational Technology
- Internet of Things
- Primary Logic Controller

The Arbitr Threat Matrix - The Visual Cyber Incident Experience

The Arbitr Threat Matrix is a new way to visually present cyber incidents over time, providing a better understanding and context to respond, remediate, and report attacks. We enable you to observe each incident across multiple planes of attack, understand how the attack behaves, visualize the methodology used, and see the assets created or leveraged by the attack. Arbitr created a new visual language to display and report incidents named GIBSEN (Graphical Information Base for Security Event Notation). The GIBSEN model changes the user experience for conducting and reporting cyber incidents and threat hunts. It enables you to see into the mind of a threat actor and create a detailed time-driven map that tracks every deception, step, process, artifact, and malicious action they take to build a complete understanding of how to respond to, remediate, and report on critical cyber incidents.



Arbitr wants to change how blue teamers and threat hunters investigate, remediate, and report on cyber incidents. We are trying to do this with a simple tool, “the right click” vs “the cut and paste.” When you get an alert, it can be easily added to the Arbitr Threat Matrix, and a collaborative GIBSEN diagram will be created to create an automated incident report. You can right-click on the initial artifact in the GIBSEN launch queries and follow the kill chain to build a complete end-to-end Threat Matrix. Each new artifact added to the Threat Matrix will record the technical details from the source tools, and each member of the investigation team can directly enter their analysis, map to popular frameworks like MITRE, and build the content required for governance and executive reporting.

Tiers of Cyber Incident Reporting

The Arbitr Threat Matrix is designed to enable incident reporting on multiple levels. Most incidents that warrant report development will also have various audiences. You can select the reporting levels and technical details included to address the different needs of business, governance, and security operations. We enable you to choose the level of reporting required for each audience:

Governance and Business

- BoD and C-Suite
- Auditor and Regulators
- Cyber Insurance Providers

Operational and Preventions

- CIO/CTO/CISO
- SecOps

Detection Engineering

- Threat Hunters
- Cyber Forensics

Training and Institutional Knowledge

The time your cyber teams invest not only serves the operation needs of developing incident reports, but it can also provide training for other cyber professionals with their professional development. Often, cyber training can be more conceptual or theoretical. Artbitr's Threat Matrix provides real-world pragmatic education that builds the institutional knowledge required to combat families of APTs (Advanced Persistent Threats) that are often relaunched in multiple variants by known threat actors.

Summary

Arbitr's Threat Matrix and GIBSEN visual language provide a new perspective on conducting, collaborating, and reporting on cyber incidents. We aim to enable GIBSEN as an open standard for the cyber community, government organizations, and educational organizations.

Arbitr Security

www.arbitrsecurity.com