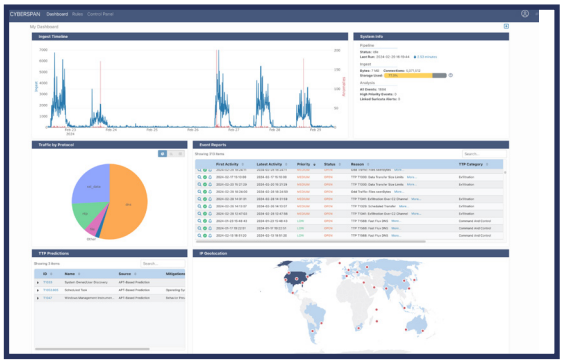
IntelliGenesis
WHERE INTELLIGENCE BEGINS

CYBERSPAN®

Feel Secure. Defend Together!



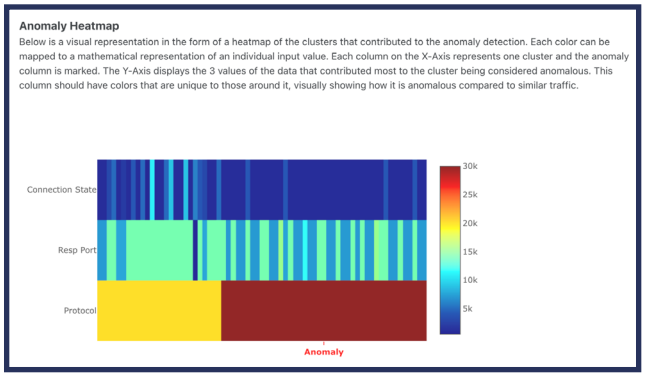
ANOMALY DETECTION ACROSS THE CYBER INFRASTRUCTURE

- Provides fundamental cyber protection for small and medium sized Defense Industrial Base (DIB) businesses.
- Utitlizes information collected at the network boundary to detect changes in network behavior in the one arena an attacker cannot change, raw packets. Packets do not lie!
- Secures traditional IT devices, as well as IoT devices, like Smart TVs, Alexa, Google Home, etc., increasing privacy and security.

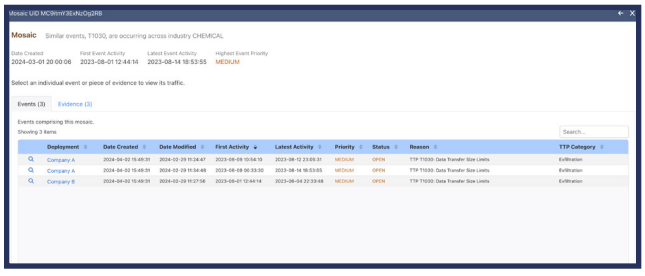
WHY CHOOSE CYBERSPAN?

- Easy, Secure Client Onboarding with Dedicated Support
- Seamless Deployment to Your Network - No Agents to Install
- On-Premise AI Analysis Prevents Sensitive Data Exposure
- Fortify Against Threats Hidden in Your Network
- Bolster Network Tools & Maximize Your Cybersecurity Investments

Explainability



Community Insights



DETECTION CAPABILITIES:

- Data Exfiltration
- Denial-of-Service Attacks
- Ransomware
- Port Knocking
- Non-Standard Port Use
- Proxy Misuse

UNSUPERVISED LEARNING MODELS:

Packet: Analyzes all network traffic to detect and identify anomalous activity across the entire network

Device: Detects anomalous activity in the context of a single device

Time: Identifies time periods which contained anomalous activity on the network

SUPERVISED LEARNING MODELS:

- Maps malicious network traffic to known MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs)
- Performs predictive analysis of traffic sizes to identify anomalous volume of data transfer
- Incorporates output of other intrusion detection systems (IDS) to enhance detection and analysis
- Analyzes the user agent string in HTTP traffic for consistency and accuracy across connections

FEATURES

Category	Capability
Universal Features	• Agentless Network Monitoring • Analyzes Network Traffic • API Access to All Data in JSON and STIX Formats • Maintains Privacy of Users • Maintains Privacy of User Activity • Monthly Updates
Deployment Types	• Physical On-Premise • Virtual On-Premise • Cloud Hosted
Management Console	• Defend together with CYBERSPAN™ Management Console, anonymized data from across the sensor install base. See what kinds of attacks are on the horizon, centralize management of sensor deployments.
Detection Capabilities	• Data Exfiltration • Denial-of-Service Attacks • Ransomware • Port Knocking • Non-Standard Port Use • Proxy Misuse
Data Collections and Buildup	• **Evidence:** The result of an individual model or analytic that, by itself, only indicates unusual or potentially notable activity. It, alone, does not warrant display to a user • **Event:** An object composed of one or more pieces of evidence, often matching a known attack pattern or model, that tell a holistic story about activity that the user should be aware of • **Mosaic:** A combination of Events from multiple sensors that indicate a pattern or trend across a community
Dashboards	• ATT&CK Mitigations for Detected TTPs • Data Volume Metrics • Protocol Type Distribution • Anomalous and Malicious Activity
Learning Models	• Packet: Analyzes all network traffic to detect and identify anomalous activity across the entire network • Device: Detects anomalous activity in the context of a single device by clustering only the traffic through that device • Time: Identifies time periods which contained anomalous activity on the network by grouping all traffic into one-minute blocks and clustering the metadata of those groups • Using the features such as IPs, ports, protocols, and durations, the model estimates an expected number of bytes transferred. This is compared to the actual quantity to identify unusually sized data transfers • Using Natural Language Processing (NLP) and decision tree classification models to examine the user agent string for each HyperText Transfer Protocol (HTTP)
Customizations Available	• On-site Installation and Troubleshooting Support • Other Data Processing • Other Analytics • Other Data Models