The Security Problem for VSDNs. Virtual software-defined networks (VSDNs) for connected cars, planes, tanks, drones, remote work environments, disaster and construction sites etc. can be quantum-encrypted to protect them from external attackers getting in. But there is is presently only poor protection, monitoring and control of what accredited users do on the network. If someone comes by a username and password either legitimately or by force, fraud or guesswork, then that person can do many potentially malign things on a virtual network before anyone notices and considers stopping them. This includes software updates sent to vehicles by an auto manufacturer. This security gap in detecting and neutralizing the insider threat is one reason we do not see as many self-driving cars on the road as many had predicted by now.

The Conatix Omniskia Solution. The Conatix Omniskia insider threat detector for virtual software defined networks (See All, Know All, Detect All) has got you covered. Our insider threat detector spots suspicious activity by network users and can kick someone off the network and/or alert the sysadmin as needed.

AI-Powered Anomaly Detection. Conatix delivers cutting-edge real-time analytics for packet, network, and security logs using advanced Deep Learning and Machine Learning models. Conatix Omniskia is built on a robust ecosystem of open-source tools, enterprise integrations, and trusted technology partners. Our platform leverages **Grafana**, **Docker**, **Kafka**, and **Elasticsearch** to process and visualize massive streams of log data, enabling instant anomaly detection and proactive threat response. Whether for enterprise security, network performance, or compliance, Conatix empowers analysts with precision insights to safeguard digital infrastructure.

Real-Time Processing. Ingest and analyze terabytes of network and security logs in real-time, with millisecond-latency insights.
AI-Driven Anomaly Detection. Deep Learning and Machine Learning models trained to detect unusual patterns and potential threats before they escalate.
Unified Visual Analytics. Seamless integration with Grafana dashboards for intuitive, customizable real-time visualizations.
Scalable Architecture. Built with Docker and Kafka for distributed, fault-tolerant analytics across any infrastructure.

NETWORK LOG ANALYTICS. Network logs are the lifeblood of modern IT infrastructure monitoring. They capture detailed records of network activity, including connections, traffic patterns, errors, security events, and performance metrics. Without analyzing these logs, organizations operate in the dark—unable to spot security breaches, performance bottlenecks, or misconfigurations in time to take action. **Omniskia** specializes in processing these massive log streams in real-time, using machine learning and deep learning to detect anomalies automatically. Our platform empowers network and security teams to respond to incidents faster, maintain compliance, and optimize system performance.

What We Monitor. Conatix ingests network, packet, and security logs in real time using **Kafka** for streaming, processes them with **machine learning models** to detect unusual patterns, and visualizes findings in **Grafana** dashboards. This combination allows proactive detection of threats, compliance violations, and operational inefficiencies.

What We Measure. By leveraging AI-driven analysis of network logs, Conatix helps organizations:

- Detect intrusions and anomalies before they cause damage
- Optimize network performance and reduce downtime
- Maintain compliance with industry regulations
- Improve the efficiency of IT and security teams

PACKET LOG ANALYTICS. Packet logs provide a wire-level view of network activity. Each packet captures source/destination addresses, ports, protocol, timing, sizes and flags—enough detail to reconstruct conversations, baseline normal traffic, and catch abnormalities in real time. **Conatix** uses deep-learning models to learn those baselines and surface anomalies such as scans, floods, unusual protocol mixes, and lateral movement—without relying on brittle rule sets.

What We Monitor

- Packet volumes and burst patterns across time windows.
- Protocol distribution shifts (e.g., UDP spikes vs. TCP data/connect events).
- TCP flag irregularities (*SYN, ACK, RST, FIN*) that indicate scans or resets.
- 5-tuple flow behaviors (source/destination IP/port + protocol) and deviations from baselines.
- Latency/throughput outliers, fragmentation, and retransmission indicators.

What We Measure

- **Count:** Total number of anomalies or events in the selected window.
- **Heatmap of Anomalies by Day:** Calendar-style density view for spotting recurring hotspots by date/hour.
- **Top Anomaly Reasons:** Ranked breakdown (e.g., *Port Scan*, *UDP Burst*, *Auth Failures*) to prioritize response.
- **Packet Volume Over Time:** Time-series of packets; spikes indicate scans, floods, workload surges.
- **UDPv4 / TCP_DATAv4 / TCP_CONNECTv4:** Example protocol/event classes commonly tracked; values like *468 / 211 / 50* indicate counts within the time range.

SECURITY LOG ANALYTICS. Security logs capture events related to authentication, firewall decisions, intrusion attempts, and abnormal traffic patterns. They are one of the most critical data sources for defending against cyber threats. **Conatix** ingests and analyzes these logs in real time, using machine learning to detect patterns that indicate attacks, reconnaissance, or policy violations.

What We Monitor

- Source and destination IP activity to identify attackers or compromised hosts.
- TCP flag combinations to detect suspicious connection patterns.
- High-volume or unusual event types such as repeated login failures or DNS floods.
- Security event trends over time, segmented by protocol and severity.
- Targeted destination ports that could indicate exploitation attempts

What We Measure

- **Top Source IPs (All):** Shows external and internal IP addresses generating the highest event counts.
- **TCP Flag / Event Breakdown:** Helps identify abnormal handshake patterns or aggressive connection resets.
- **Top Event Types:** Shows event types dominating logs (e.g., SYN floods, suspicious DNS activity).
- **Security Events Over Time:** Charted to reveal when attacks occur, useful for correlating with incident timelines.
- **Top Destination IPs & Ports:** Highlights which systems or services are being targeted.

What's Next. Integration of user and device-level data analytics while respecting all relevant privacy laws.

This is a 5-minute demo of Conatix Omniskia: https://vimeo.com/manage/videos/1114314444
And this is a 1-minute video overview of Conatix: https://vimeo.com/734117465