riverbed®

Cybersecurity Threat Hunting

NetOps & SecOps teams need to proactively find and eliminate threats.

Cyber threat hunting is the practice of proactively and iteratively seeking out, identifying, isolating, and disabling threats that may have penetrated an organization's network. The threat hunting process aligns NetOps and SecOps teams and challenges them to think like their adversaries based on recognized tactics, techniques, and procedures

(TTPs). Instead of waiting for an intrusion detection system to issue alerts and then react, the most successful threat hunters leverage visibility across the entire network – from the endpoint to data access – to eliminate threats that have evaded traditional defenses and controls.

The Art of Proactively Identifying Threats

Form a hypothesis

Collect & Analyze all Data

Hunt for Additional Insights

Identify Threats

Neutralize Adversaries
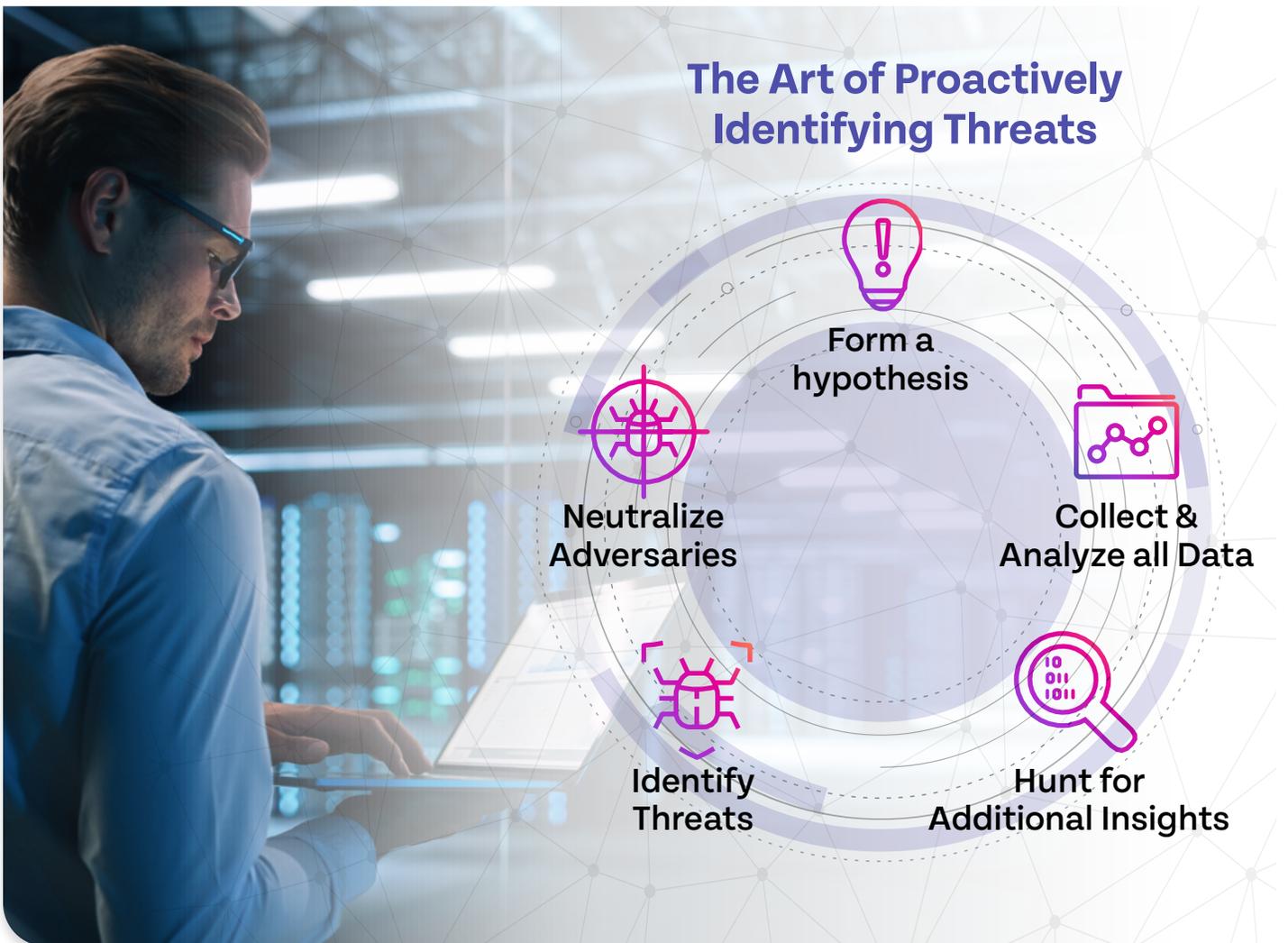
A Threat Hunter's Arsenal

The tools needed to proactively hunt threats help to achieve end-to-end visibility across the entire network environment and offer actionable insights.

Riverbed's Alluvio Unified Observability solutions allow threat hunters to see across their entire network environment. By integrating data from every user, device, application, and network, across a common dashboard, threat hunters have a single source of security truth from unified insights.

Armed with this data, threat hunters can fundamentally transform their approach to seek out and eliminate threats before serious damage occurs.

Resolve
security threats & performance issues up to **90% faster**

- **Full-Fidelity Flow Monitoring** with port and dependency mapping as well as long-term data retention offers broad visibility into all network traffic.

- **Packet Capture with Deep Packet Inspection** (DPI) examines protocol details and offers abundant packet storage for data-level forensic analysis.

- **Infrastructure Monitoring** provides details into change management, and detects unusual activity on network devices, such as saturation of an interface by an attack.

- **Endpoint Detection** monitors desktops, laptops, and other end user devices to detect and investigate suspicious activities.

- **Log Analysis** extracts data from log files for trend and pattern analysis.

- **Anomaly Detection** recognizes changes in volume and velocity of traffic between IPs.

Learn more at
https://visibility.riverbed.com/

riverbed®

Riverbed — Empower the Experience

Riverbed is the only company with the collective richness of telemetry from network to app to end user that illuminates and then accelerates every interaction so that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed offers two industry-leading solution areas – Alluvio by Riverbed, an innovative and differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users, whether mobile, remote, or on-prem. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com.