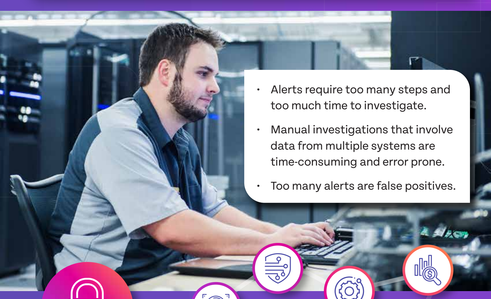
riverbed

The Importance of Automating Security Forensics

Manual Forensic Analysis Is Time Consuming

Without automated integrations between traditional security tools and network performance monitoring solutions, security investigations suffer.



- Alerts require too many steps and too much time to investigate.
- Manual investigations that involve data from multiple systems are time-consuming and error prone.
- Too many alerts are false positives.

67% of organizations feel the attack surface is growing, driven by:

- **Third-party IT Connections**
- **Support for Remote Workers**
- **Increased Public Cloud Usage**
- **Adoption of SaaS Applications**[1]

Benefits of Automating Security Investigations

Automating security investigations create consistency in security processes and improve threat detection and response by providing context enrichment and improving prioritization.

91% of organizations believe network automation is important to NetSecOps collaboration.[2]

46% of SOC teams are automating security operations processes "extensively."

44% are automating security operations processes "somewhat." [3]

Top 3 benefits experienced by organizations when the network team and security team successfully collaborate:

- **58%** Faster Resolution of Security Issues
- **52%** Reduced Security Risk
- **46%** Operational Efficiency[4]

Alluvio IQ Automates Security Forensics Investigations

Alluvio IQ, Riverbed's SaaS-delivered unified observability service, provides SecOps teams with easy and automated access to Alluvio network performance data for fast, consistent threat investigations. Traditional security tools, like SIEM and SOAR, send event data to Alluvio IQ so the investigative runbooks can gather supporting network data and send it back – all without human intervention.

Using Alluvio IQ to investigate network threats improves collaboration between NetOps and SecOps teams, plus:

- Provides more consistent investigations – the same steps, every time no matter which analyst is investigating.
- Delivers reliable, repeatable, and efficient investification processes with fewer errors.
- Enables more in-depth investigations to reduce risks
- Increases perception that incidents are being handled quickly.
- Improves SOC team morale – less turnover, greater job satisfaction.

1. https://www.esg-global.com/research/esg-research-report-security-hygiene-and-posture-management
2. https://info.enterprisemanagement.com/netsecops-webinar-netcraftsmen
3. https://www.esg-global.com/research/esg-research-soc-modernization-and-the-role-of-xdr-technology.html
4. https://info.enterprisemanagement.com/netsecops-webinar-netcraftsmen

For more information on Alluvio by Riverbed, visit:
https://www.riverbed.com/products/unified-observability.

ALLUVIO by riverbed