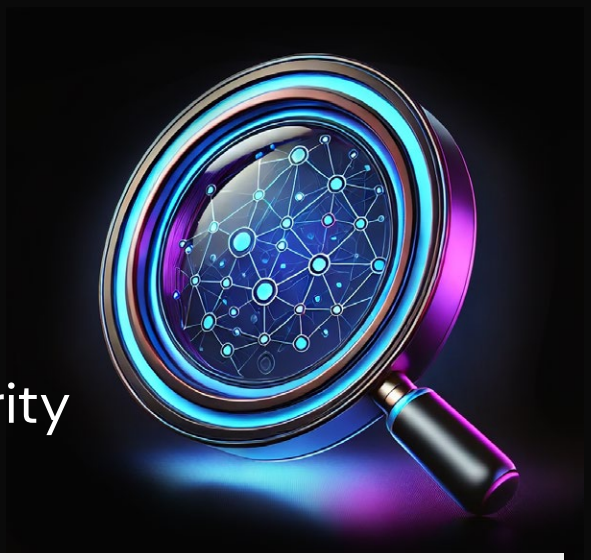
LiveAction + EXTRAHOP



WHITE PAPER

Using ExtraHop and LiveWire Together for Efficient Network Security Identification and Investigation

EXECUTIVE SUMMARY

Efficient network security incident response requires both swift identification of security incidents and in-depth analysis of the relevant data. This whitepaper demonstrates how organizations can use ExtraHop as the primary tool to identify security incidents, and then pivot to LiveWire for Security for a comprehensive forensic investigation on the affected packets. By integrating these two complementary solutions, organizations can streamline their incident response process and improve overall network security.

Introduction

In the rapidly evolving digital landscape, organizations must develop an efficient and effective network security incident response strategy. ExtraHop and LiveWire for Security are two powerful network security solutions that, when used in tandem, provide a seamless and comprehensive approach to incident response. This whitepaper will discuss how organizations can leverage ExtraHop for the initial identification of security incidents and then pivot to LiveWire for Security for a detailed forensic investigation on the affected packets.

EXTRAHOP

Identifying Security Incidents with Real-time Network Analytics

ExtraHop is a real-time network analytics platform that focuses on providing full visibility into network traffic, detecting anomalies, and helping organizations respond to security incidents more effectively. Its advanced machine learning capabilities enable ExtraHop to rapidly identify potential security risks and provide valuable insights for mitigating them. By using ExtraHop as the primary tool for detecting security incidents, organizations can quickly identify and respond to potential threats.

LiveWire

Comprehensive Forensic Investigation on Packets

LiveWire for Security is a versatile packet forensics solution that caters to networks of various sizes, from small-scale operations to expansive data centers and cloud environments. Its primary focus is on deep packet inspection and analysis, offering features like Intelligent Capture, a user-friendly Web UI, and seamless integrations with other solutions. By pivoting to LiveWire for Security following the identification of a security incident by ExtraHop, organizations can conduct thorough forensic investigations on the affected packets, ensuring a comprehensive and accurate understanding of the incident.

Streamlined Incident Response with ExtraHop and LiveWire for Security

- Integrating ExtraHop and LiveWire for Security enables organizations to streamline their incident response process, with ExtraHop identifying security incidents and LiveWire for Security providing the necessary forensic investigation on the affected packets.

Efficient Incident Identification and Response

- ExtraHop's real-time network analytics capabilities allow for the swift identification of security incidents. By starting with ExtraHop as the primary tool for detecting potential threats, organizations can quickly initiate their incident response process.

  Example: A manufacturing company can use ExtraHop to monitor its industrial control systems for signs of unauthorized access or malicious activity. If ExtraHop detects an anomaly, the company can quickly initiate an incident response process to minimize potential damage.

In-depth Forensic Investigation with LiveWire for Security

- Following the identification of a security incident by ExtraHop, organizations can pivot to LiveWire for Security for a comprehensive forensic investigation on the affected packets. This enables security teams to gain a deeper understanding of the incident and formulate effective mitigation strategies.

  Example: If ExtraHop detects a data breach at a retail organization, security teams can use LiveWire for Security to analyze the affected packets and determine the source of the breach, the extent of the data compromised, and the appropriate steps to remediate the issue.

Conclusion

ExtraHop and LiveWire for Security, when used together, provide organizations with an efficient and comprehensive approach to network security incident response. By starting with ExtraHop to identify security incidents and pivoting to LiveWire for Security for detailed packet forensics, organizations can streamline their incident response process and improve overall network security. This integrated approach enables organizations to proactively respond to evolving cyber threats and maintain a robust security posture in the digital world.

Appendix

What is ExtraHop?

ExtraHop is a network detection and response (NDR) company that focuses on providing cybersecurity and performance management solutions. Their platform uses real-time analytics, machine learning, and artificial intelligence to analyze network traffic, detect anomalies, and provide insights for both security and performance optimization.

ExtraHop's core product, the ExtraHop Reveal(x), is designed to help organizations monitor, detect, and respond to threats within their network environment. It works by passively analyzing network traffic, identifying patterns and behaviors that may indicate potential threats or performance issues, and providing alerts and recommendations to IT and security teams. By offering visibility into network activity and potential threats, ExtraHop aims to help organizations proactively manage their cybersecurity posture and improve network performance.

Some key features of ExtraHop's solutions include:

1. **Real-time analytics:** The platform processes and analyzes network data in real-time, allowing organizations to identify and respond to potential threats and performance issues quickly.
2. **Machine learning and AI:** ExtraHop's technology leverages machine learning and artificial intelligence to identify patterns and detect anomalies in network traffic, which can indicate potential threats or areas for performance improvement.
3. **Full visibility:** ExtraHop provides visibility into all network traffic, including encrypted traffic, enabling organizations to monitor their entire network environment and gain insights into potential vulnerabilities and performance bottlenecks.
4. **Integration with other security tools:** ExtraHop's platform can integrate with other security solutions, such as Security Information and Event Management (SIEM) systems, to provide a more comprehensive and effective cybersecurity strategy.

Overall, ExtraHop focuses on delivering advanced network detection and response capabilities to help organizations protect their network environments, optimize performance, and maintain compliance with industry regulations.

Appendix

Once a security event is generated using ExtraHop how are the packets acquired used for a network forensic security investigation?

ExtraHop's network detection and response (NDR) platform focuses on real-time analysis of network traffic to identify and alert on potential security threats. However, it does not store the full packet data by default. To conduct a network forensic investigation using packet data, you will need to integrate ExtraHop with a packet capture (PCAP) solution to collect, store, and analyze the raw packets.

Here are the general steps for conducting a network forensic security investigation using ExtraHop combined with a packet capture solution:

1. **Configure packet capture:** Set up a packet capture solution to store the raw packet data. This can be a standalone appliance, a virtual machine, or a cloud-based solution. Make sure that the packet capture solution is configured to capture traffic from the relevant network segments.
2. **Integrate ExtraHop with packet capture solution:** Configure ExtraHop to send relevant event data, alerts, or triggers to the packet capture solution. This integration will enable the packet capture solution to correlate the detected security events with the corresponding packet data.
3. **Investigate security events:** When ExtraHop generates a security event or alert, use the event details to identify the associated packets in the packet capture solution. This may involve searching for specific IP addresses, port numbers, protocols, or other attributes related to the event.
4. **Analyze packet data:** Once you have located the relevant packet data, use network forensic analysis tools to examine the packets in detail. This may involve looking for signs of malicious activity, such as unauthorized connections, data exfiltration, or command and control traffic. Network forensic tools can help you reconstruct sessions, extract files, and visualize data flows.
5. **Generate a report:** Document your findings from the network forensic investigation, including the security event details from ExtraHop and the packet analysis results. This report can be used to support incident response efforts, remediation actions, or compliance reporting.

By integrating ExtraHop with a packet capture solution, you can leverage the real-time analytics and detection capabilities of ExtraHop while having access to the raw packet data necessary for a detailed network forensic security investigation.

Appendix

Why is LiveWire and Omnipeek a better tool for packet level security forensics investigations the ExtraHop?

LiveWire (from LiveAction) and Omnipeek (from Savvius, now a part of LiveAction) are designed specifically for packet-level analysis and deep packet inspection (DPI), which makes them better suited for security forensics investigations at the packet level compared to ExtraHop, whose primary focus is network detection and response (NDR) based on real-time analytics and machine learning. Here's a comparison of the capabilities of these tools:

1. **Packet capture and storage:** Both LiveWire and Omnipeek have built-in functionality for capturing and storing raw packet data, allowing security analysts to perform in-depth forensic investigations. ExtraHop, on the other hand, is primarily focused on real-time analysis and does not store full packet data by default. To conduct packet-level forensics with ExtraHop, you would need to integrate it with a separate packet capture solution.

2. **Deep packet inspection:** LiveWire and Omnipeek offer deep packet inspection capabilities, which enable security analysts to analyze packet payloads and extract detailed information about network traffic. This is useful for identifying malicious activities, such as data exfiltration, command and control traffic, or unauthorized access. While ExtraHop can analyze network traffic to some extent, its primary focus is on detecting anomalies and potential threats based on traffic patterns, rather than deep packet inspection.

3. **Advanced analysis tools:** Both LiveWire and Omnipeek provide advanced packet analysis tools, such as protocol decoders, filters, and visualization options, which allow security analysts to quickly identify and investigate security incidents at the packet level. ExtraHop's focus is on real-time analytics and machine learning for anomaly detection, so it does not offer the same level of packet analysis tools as LiveWire and Omnipeek.

4. **Network forensics focus:** LiveWire and Omnipeek are specifically designed for network forensics and troubleshooting, with features that enable security analysts to reconstruct network sessions, visualize data flows, and correlate events across multiple data sources. ExtraHop, on the other hand, is primarily focused on network detection and response, making it better suited for proactive threat detection and response rather than in-depth forensic investigations.

While ExtraHop excels in providing real-time analytics and anomaly detection for network security, LiveWire and Omnipeek are better suited for packet-level security forensics investigations due to their focus on deep packet inspection, packet capture and storage, and advanced analysis tools specifically designed for network forensics.

901 Campisi Way, Suite 222
Campbell, CA 95008
USA +1 (888) 881-1116

LiveAction provides end-to-end visibility for network security and performance. By relying on a single source of truth – the packets – LiveAction gives modern enterprises the confidence needed to ensure the network is securely meeting business objectives, providing full network visibility to better inform NetOps and SecOps, and reducing the overall cost of network and security operations. By unifying and simplifying the source of collection, inspection, presentation, and analysis of network traffic, LiveAction empowers network and security professionals to proactively and quickly identify, troubleshoot, and resolve issues across increasingly large and complex networks.

To learn more about LiveAction, visit www.liveaction.com