JOINT SOLUTION BRIEF

Analyst-Level Security Intelligence from InQuest and Gigamon Fights Cyberattacks in Real Time

The Challenge

SOC analysists need all the help they can get in facing an onslaught of threats. There are numerous tools on the market, both commercial and open source, but most can't handle the variety of attacks or even process the firehose of data generated by carrier-class networks. If you can't peek inside a multitude of file formats and harness a wide range of security tools, you can't be sure your network is secure.

Integrated Solution

Integrated with the Gigamon Visibility Platform, InQuest automates mundane SOC tasks to free up analyst brainpower for where it's needed most. InQuest can perform Deep File Inspection (DFI) and apply updated intel feeds from InQuest Labs to raise alarms as needed while avoiding false positives. Gigamon provides the reliable hardware base and traffic carving power to unleash InQuest's capabilities.

Joint Solution Benefits

- Strategic orchestration from InQuest harnesses multiple security tools to deliver easy-to digest security assessments
- InQuest's Deep File Inspection (DFI) unravels nested malware other tools miss
- InQuest Labs' extensive knowledge of real-world malware campaigns inform threat hunting signatures and intelligence
- Enhanced visibility and easy access to traffic from physical, virtual, and public cloud networks through the Gigamon Visibility Platform
- The Gigamon platform filters and deduplicates traffic so InQuest can put its focus where it's needed most

Introduction

Security operations center (SOC) teams need tools that help identify and quash threats. Unfortunately, too many commercial and open-source tools can't rise to the challenges faced by SOCs. These tools lack reliable throughput support, can be easily bypassed by attackers using common evasion techniques, and can't dissect objects stored in some of the most common malware file formats typically leveraged by malicious actors.

In contrast, InQuest, an all-encompassing network-based threat eradication platform, leverages machine learning and intelligent orchestration to streamline your analytic workflow and provides a variety of tools to assist with collaboration, investigation and reporting.

InQuest: Built by SOC Analysts for SOC Analysts

InQuest empowers your SOC with the ability to prevent, detect and hunt intruders and insider threats across your enterprise. With InQuest, you can identify, process and inspect data — both in motion and at rest — to prevent malicious code from exploiting your assets. The platform leverages the InQuest Labs research team's extensive knowledge of real-world malware campaigns in tandem with their proprietary Deep File Inspection (DFI) engine to unravel and expose content that bypasses traditional defense platforms.

InQuest appliances are contained within a 1U chassis and are tailored for throughput rates ranging from 100Mbps to 20Gbps with clustered deployments capable of handling 100Gb+. The Deep File Inspection engine dives into the recursive nature of today's threats, decompressing, decoding, deobfuscating and decompiling files at wire speed rates of ingestion. Plus, InQuest sends data to — and digests data from — complementary vendor solutions, helping produce a single digestible threat score with a detailed threat receipt highlighting the indicators responsible for reaching that conclusion.

How the Gigamon Visibility Platform Helps

Thanks to the Gigamon Visibility Platform's hardware reliability coupled with its unparalleled support for throughput rates and feature-rich traffic carving and distribution, InQuest can focus its attention where it's needed most. Together, InQuest and Gigamon deliver analyst-level scrutiny at multigigabit speeds, all the while reducing alert fatigue and allowing precious human time to be spent where it matters.

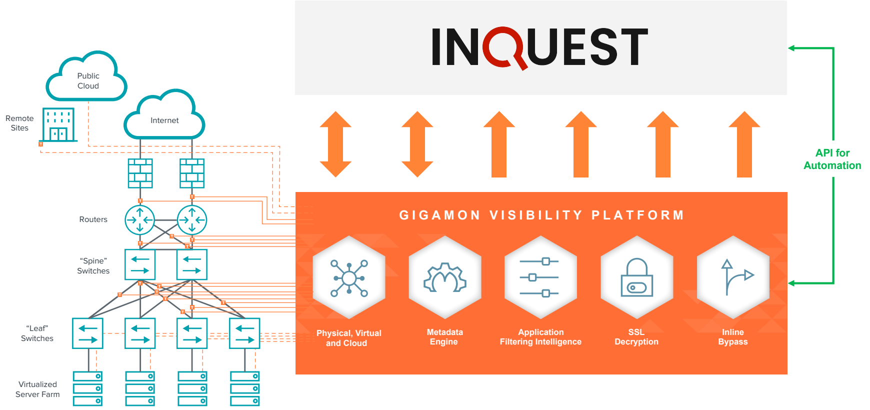

Figure 1: The Gigamon and InQuest Collector Joint Solution

Gigamon tools and InQuest have been deployed as a joint solution in the field in a number of enterprises, including across multiple environments within the United States Department of Defense. Key Gigamon Visibility Platform features that enhance the value of InQuest deployments to hunt and eliminate threats, include:

- **Easy access to traffic from physical, virtual, and cloud networks:** The Gigamon Visibility Platform manages and delivers all network traffic — including east-west data center traffic and private and public cloud workloads — to InQuest, efficiently and in the correct format, to eliminate blind spots and help ensure collective monitoring and analysis of all traffic.
- **Filtering out irrelevant traffic:** There's no point loading a tool with traffic it will only drop after identifying it. The Gigamon Visibility Platform sends InQuest only the traffic and sessions it needs to hunt down intruders and malware.
- **Load balancing to spread traffic across multiple devices:** When traffic flows are larger, the Gigamon Visibility Platform can split the flow across multiple InQuest appliances.
- **SSL decryption:** The Visibility Platform can be used to decrypt SSL encrypted traffic, where threats can lurk, so that InQuest can inspect it out of band.
- **Deduplication:** Pervasive visibility requires tapping or copying traffic from multiple points in the network, which in turn means tools may see the same packet more than once. To avoid unnecessary packet-processing overhead on InQuest, the Visibility Platform removes duplicates before they consume resources and helps balance monitoring coverage.
- **Aggregation to minimize number of tool ports used:** Where links have low traffic volumes, the Gigamon Visibility Platform can aggregate these together before sending them to InQuest to minimize the number of ports needed. By tagging the traffic, the Gigamon Visibility Platform can also identify the traffic source.
- **Easier control of asymmetric routing to ensure session information is kept together:** Most security devices require that all the packets in a session be inspected by the same device, since incomplete sessions risk being blocked. The Gigamon Visibility Platform provides an intelligent and efficient way to help ensure this inspection happens in most architectures.

For more information on Gigamon and InQuest solutions, visit:
www.gigamon.com and www.inquest.net.