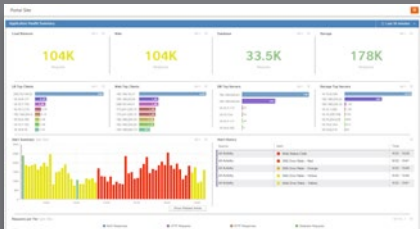




Detect Advanced Persistent Threats by Examining Activity on the Wire



ExtraHop's Open Data Stream enriches the FireEye Threat Analytics Platform (TAP) so that IT security teams can more effectively detect advanced persistent threats.

JOINT SOLUTION HIGHLIGHTS

- Persistent visibility of all activity between machines
- Enrich the FireEye TAP with critical security events and metrics
- Detect reconnaissance and data exfiltration activity immediately
- Deep visibility without having to deploy agents

CONTINUOUS MONITORING OF ACTIVITY ON THE WIRE

The ExtraHop wire data analytics platform equips IT organizations to analyze all their wire data—all L2-L7 communications between systems, including full bi-directional transaction payloads. Deployment is simple, only requiring a copy of network traffic from a port mirror or network tap. The ExtraHop platform features industry-leading scalability with up to a sustained 20Gbps throughput and 20Gbps bulk decryption so you do not miss anything.

ExtraHop provides persistent visibility into all activity between machines, which is the missing piece in security architectures. With ExtraHop, IT organizations have the essential information needed to detect reconnaissance and data exfiltration performed by the threat actor.

ENRICH FIREEYE'S THREAT ANALYTICS PLATFORM

With the ExtraHop Open Data Stream, IT security teams can now enrich their existing security dataset in the FireEye Threat Analytics Platform (TAP) with critical wire data, including the events and metrics needed to detect advanced persistent threats.

The integration sends the following crucial events and metrics to the FireEye TAP:

- DNS activity including domain lookups and possible command-and-control communications
- HTTP payload data, including MD5 sums and threat signatures
- Session tracking, such as unexpected SSH connections from external clients
- Reconnaissance activity as attackers probe networks

TRY EXTRAHOP FREE

Download the ExtraHop Discovery Edition, a free-forever virtual appliance that lets you start exploring what is possible with wire data analytics.

www.extrahop.com/discovery

