

Typhon Accelerated Threat Detection

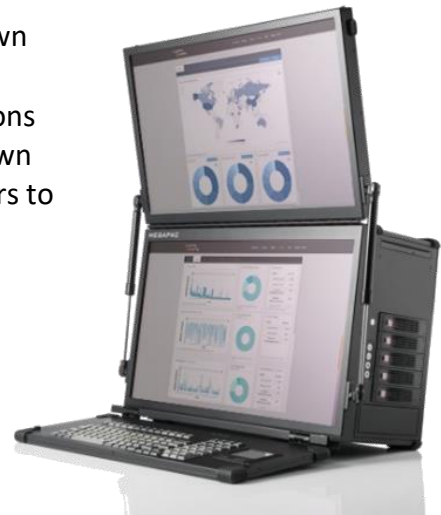
Pinpointing cyber security vulnerabilities on your network...in record time

Xanadata's Typhon vulnerability and threat detection platform enables companies to rapidly identify internal systems that are attempting to connect to external high risk sites, both inbound and outbound, and how the current network defences are reacting to these connection attempts. It gives customers a rapid insight into their security posture: organisational threat vector diversity, threat reaction time, attacker dwell time and security estate performance.

Typhon uses hardware based High Performance Compute (HPC) acceleration to enable massive brute force analytics of large amounts of log data, providing hard evidence for bad actor activity, and combines this with back-end artificial intelligence and machine learning techniques to then expand the search beyond known bad hosts to identify new attack vectors.

Key end-user benefits

- Rapidly scans network history, matching millions of known threat vectors by analysing terabytes of data per hour
- Gives clear and rapid insight of high-risk traffic connections
 - Powerful interface enables users to drill down to known bad traffic connections and quickly enables responders to home in on the most serious breaches
 - Simple view back in time to observe patient zero and identify attacker primary ingress
 - Offers automatic report generation providing instant actionable remediation information
- Advanced machine learning techniques go beyond static threat intelligence to detect previously unknown threat vectors
- Fully customisable to specific customer requirements



The Typhon platform is a high performance analytics platform capable of analysing billions of log lines, scanning for millions of potential threats in parallel, reducing a task that would have previously been impractically long and expensive, to a few minutes.

This vast performance increase in throughput is achieved through the use of custom designed HPC acceleration silicon that packs in compute performance equivalent to a 2000 node Hadoop cluster into a single node, delivered as either a single 2U appliance aimed at continuous in house analytics or a mobile solution aimed at incident response.

Typhon delivers a conclusive, verifiable and proven view of corporate cyber security posture at an unprecedented speed. For more information contact us at info@xanadata.com