BLUSAPPHIRE

INTELLIGENT CYBER DEFENSE

BLUNAF

NETWORK BASED BEHAVIOR ANOMALY DETECTION AND TRAFFIC ANALYTICS

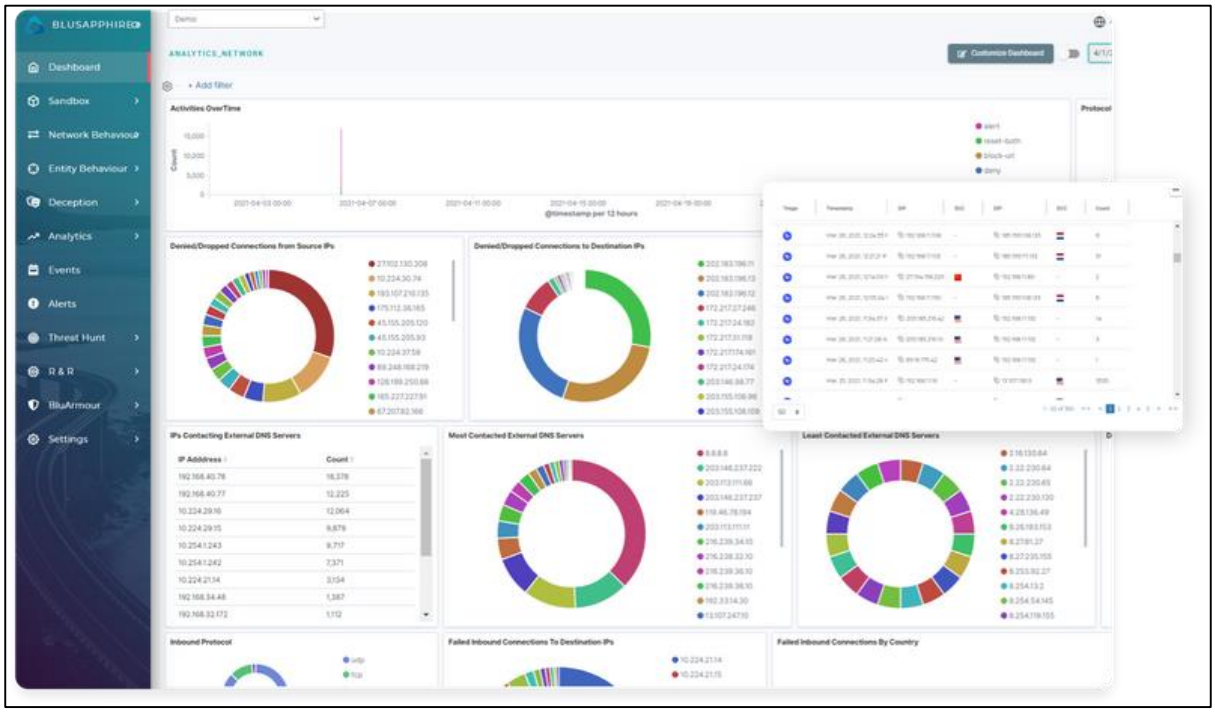
Network Traffic Analysis & Network Behaviour Anomaly Detection

Network Traffic Analysis (NTA) and Network Behaviour Anomaly Detection (NBAD) are utilized to detect suspicious traffic by looking at Behaviour based patterns via traffic analysis is carried out real time. This can complement and in many cases can replace traditional signature-based network solutions.

BluSapphire supports most of industry standard protocols. It does not rely on SSL Decryption and hence easier to deploy and scale, while offering higher detection and response capabilities. BluSapphire while relying on network behaviour-based techniques also employs signal intelligence techniques to understand and detect malicious traffic.

The data point for Real time NTA/ NBAD for North & South traffic shall be to have a network sensor deployed and having SPAN/ Port Mirror traffic passed onto the same.

For East and West traffic: SPAN/ Port Mirror can be consumed and analysed.



Detection and analysis

Deep Packet Inspection (DPI)

Deep packet Inspection means different things to different vendors. BluSapphire uses DPI to detect C&C activity and pick up botnet activity without relying on Threat Intelligence. This helps detect threat actors C&C even if they use valid sites like Google or Amazon. Detection relies heavily on Signal Intelligence techniques to pick patterns of activity.

Static analysis

BluSapphire performs real time static analysis on the packets, which includes IDS, signature matching, looking for indicators of compromise, command and control network traffic and environment traffic.

Behaviour analytics module

BluSapphire platform comprises of advance behaviour analysis module, which is similar to sandbox, but built-in house from the scratch. Behaviour analytics module focus on understanding attacker activity to revile the payload.

Looking at the behaviour really helps us understand the attacker techniques e.g.:

- Memory for credentials
- Stealing tokens
- Becoming admin
- Escalating its privileges
- Process Injection
- Disk Persistence
- Download stage 2, 3 etc.,
- Command control traffic – maintain control
- Registry Hiding and Persistence
- DLL injections
- Anomalous traffic
- Misused protocols
- File system changes
- Abnormal data transfers
- Abnormal account activity
- Irregularities in the processes

Please check out the MITRE ATT&CK Whitepaper for full list of detections.

AI and ML based detection

By Utilising Multiple machine learning models BluSapphire to identify malicious activity; our machine learning models go beyond conventional models enabling Threat detection at faster rate.

Our model has high detection rate of 99.8% of detection rate which is highest in the industry till date. Currently we monitor over 40 different file types looking for malicious activity and this results in organizations to detect with accuracy and, hence reduce false positives.

Static Binary Analysis

Akin to Reverse Malware Engineering on the fly at wire speed, BluSapphire enables rapid detection of malicious zero-day malwares or Ransomwares even without ever executing them. What usually takes days and weeks can now be achieved at wire-speed.

Network Behaviour Anomalies

Whether its data exfiltration over DNS, SSH or HTTP(S) or an attacker looking for vulnerabilities, BluSapphire's advanced machine learning models can detect these network anomalies immediately and contain the threat using native response and remediation. BluSapphire can also immediately enquire the endpoint that is causing the behaviour and gather context around the suspicious activity in seconds. Armed with activity and context, BluSapphire can quickly identify and remediate these threats in real-time.