TELEMETRI

Use-Case

Threat Detection Efficiency

An explosion of data, combined with a shortage of analysts, means that legitimate online threats get lost in the noise.

Growth in global IP traffic outpaces most organizations' ability to react to threats. They are often so flooded by data they are rarely able to identify which network addresses are a priority to isolate for further investigation. Industry surveys have found that the typical organization can only investigate 29% to 56% of the security alerts that arise. Fully 74% of security analysts admit to ignoring security events and alerts because there are just too many to consume.

This issue will compound over time. Annual global internet traffic is expected to reach 3.3 ZB per year by 2021 (278 EB per month) according to Cisco. Network security is foundational to organizational security, and all organizations struggle with the volume, variety, and velocity of data. Quick identification of the most important issues is a vital step towards effective allocation of scarce analyst capacity.

Telemetri has shown a 90% reduction in non-actionables and false positives.

By using network-enriched data, **Telemetri** improves the signal-to-noise ratio, reduces false positives, and provides visibility into previously obscured activity of interest and potential problems. When **Telemetri** collects information from the Internet, it is "mapping" not only the networks themselves but the "transportation systems" that connect them to each other. This allows users to understand how organizations on the Internet are interacting with them. Specifically, **Telemetri** adds contextual, network-centric data to the organization's already available log data regarding all traffic coming into their network. They can then use this enriched data to filter out all the non-actionable information that is irrelevant to their concerns or needs.

With Telemetri, users can create a high-resolution map of the internet that allows users to pinpoint indicators of compromise.

Key Indicators of Compromise (IOC) can thus be found within cloud telemetry data, user activity, system events, firewall activity, and more. In fact, specific sequences and combinations of events and specific patterns can also signal an incident, threat, or risk that requires attention. By removing "non-actionables," the organizations looking for those needles in the haystack – genuine threats – can cut the haystack into a fraction of its former volume. In turn, that enables analysts to focus on true threats instead of having to go through *everything* and risk missing genuine issues or threats because they got lost in the noise.

Telemetri thus allows analysts to more effectively allocate their time, streamline their analytical processes and attention.

Point-based approaches like blacklists and reputation services cannot identify and characterize threats across the entire Internet. If the only level of resolution is network addresses, organizations are in trouble. **Telemetri** moves beyond point-based approaches to characterize networks across the entire Internet to quickly get "out of the weeds" and focus on targeted portions of network traffic, both inbound and outbound.

An example of the enriched data is the country code (out of approximately 200), as well as a third-party index of 'trust' for the associated country (International Transparency International's Corruption Perception Index or TICPI) that ranges from 0 (low trust) to 99 (high trust).

This is the mechanism by which **Telemetri** saves analysts so much time. If the network address comes from a Content Delivery Network (CDN), they might set that information aside or filter it – there's nothing they need to do but point and click. But if they see network activity coming out of a Commercial Cloud Provider from Eastern Europe known for supporting ransomware, they can isolate and flag the information as suspect and worth further investigation.

Telemetri can help identify most attacks against your network by identifying indications of compromise (IOC) as well as help the Tier Two or Three analyst identify where in the Kill Chain the attacker (human or malware).

Analysts have a common set of questions when a threat or incident is identified. **Telemetri** is designed to answer many of those quickly, and accurately - enabling a quicker response, more accurate and reducing closure time. Importantly, **Telemetri** also helps move "non-incidents" off the table quickly, allowing more time to focus on real threats, getting the most bang for the buck out of the analyst team

There is no need to "rip and replace" your existing infrastructure or tools to implement **Telemetri**, and our adaptive and dynamic datasets make everything else coordinate more productively.

- More effective security: less time spent on fewer problems
  Less exposure to legal liability for data loss and more confidence "we got the important things done"
  Faster threat detection, before an intrusion can last long enough to do serious damage
  Decreased margin of error on detection and resolution of real threats
  Lower cost for more effective security