Security Analytics & Logging

Problem

The need to handle an increasing volume and variety of millions of security information points (assuming you have the ability to capture those). The overall level of security intelligence required today goes well beyond the capabilities of yesterday's infrastructure.

Solution

By implementing the preceding steps in this blueprint and the foundational Network Blueprint* layer, you are able to scale analytical capabilities with the help of the security ecosystem (and SaaS), control and move large volumes of data across low-latency direct connections, and observe all localized interactions between all parties in a distributed and scalable manner. You can incrementally improve your inspection capabilities through all levels of the OSI stack while applying evolving models and analytical intelligence. More importantly, you have the control to act on, or respond to, the delivered insights. Improve your policies (enforced globally at all intersection points – therefore, across all clouds and partners) and further compartmentalize risk over time. Adapt to changes in business processes and technology from a position of governance. Provide real-time risk positions and trend analysis as decision support for the security roadmap, backed by data to prove the return on security posture. Likewise, stop investing in ineffective practices.

Constraints

1. Low visibility into activity at the edge limits the security data collected.
2. Building infrastructure required to conduct large scale and deep analytics on the data can surpass skillsets.
3. Building out analytics inside a single cloud is like locking a single room in the house. The larger picture across mobile and business ecosystems is not being accounted for.
4. Centralizing analytics means reduced reaction times to geographically dispersed threats.
5. Each region has different threat vectors, regulations and profiles that can require different analysis and response. It's not one size fits all.
6. Defense in depth requires analytics at all levels of the environment, which can be siloed and therefore ineffective.

Steps

1. Plan where data will be aggregated and how it will be accessed (Data Blueprint*).
2. Inventory real-time event processing and data sources/logs that are planned or currently available (e.g., boundary, inspection, end-point).
3. For each of the network segmentation classes of traffic, plan the initial behavioral analytics models and process for tuning them.
4. Apply hybrid infrastructure services in the isolated, closed-circuit environment. Logging repositories should be immutable, but false logs should not be possible either.
5. Observe the known good state to learn normal behavior for anomaly detection.
6. Run your own penetration, vulnerability and behavioral tests to tune the models.
7. Integrate policy enforcement for real-time response to attacks.

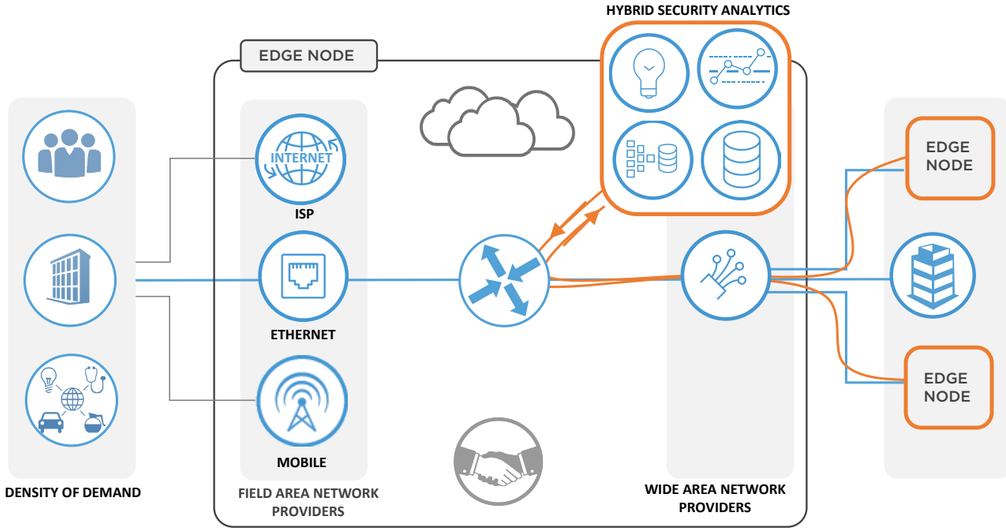
Forces

- Cybercrime is growing at the same pace and sophistication as digital business.
- Zero-day vulnerabilities are increasing as the pace of technology change increases and maturity and understanding decrease.
- Recent advice from authorities and industry experts is to assume your environment is already compromised and has been for quite some time. You just don't know it yet.
- Infiltration is driving the need to observe all kinds of behavior in order to detect subtle patterns, not just the obvious threats.
- In the rapidly changing world of digital business, it will become increasingly difficult to understand risk profiles without established analytical models.

Results

- The security position for the firm is not only well understood, but is observable and policy controlled—with machine learning.
- Capacity issues are buffered by expansion into cloud services, and can in the future can be mitigated in real time as models and policies learn that behavior.
- Achieve an optimal mix of real-time event processing and situational analysis.
- Skillsets and innovation can be easily sourced from an ecosystem of security services.
- New business models and cloud services can be activated seamlessly with full protection.
- Security and risk management are now enablers of digital business, not barriers or detractors.

Reference View



* Network and Data Blueprints — IOAKB.com