Security as a Digital Business Enabler

Problem

Security teams are seeing exponential change and increasing complexity, and have less time to balance the risk. Attacks, across more technologies, are getting more sophisticated, and the impact is now significantly higher (loss of trust can put you out of business). Security has to slow things down to protect the firm, but the business needs growth at speed to survive.

Solution

For many industries, the shift to digital business already happened. IOA has been developed (over years) from studying that shift and capturing architecturally what others did and are doing. Innovation is not invention, but more the application of an existing solution in a new context. With that in mind, take algorithmic (algo) trading as a precedent. It exhibits many of the same challenges as those facing IT security. There are very large volumes of data that must be captured, analyzed and then acted upon in real time. The market shifts continuously, and machines are programmed to act autonomously based on that change. The impact of failure is business threatening, and the compliance and legislative requirements are extremely fine-grained, strict and uncompromising. To solve, many companies needed to re-architect, starting with IOA and controlling all digital communications (pattern 1). Instead of clouds, in this case, they integrated with market exchanges and counterparties (pattern 2), and to scale they applied autonomous machines and artificial intelligence. AI is not that new in the security space;however, there is a difference. They didn't apply AI to their existing architecture to help them manage the "things" which leads to having too much data and unhelpful 'business intelligence'. AI was incorporated into the new architecture to deeply analyze the "communication between the things" and understand and control what was happening in real time. To expand on that analogy, it's the use of CEP that presents real-time data (state) to a series of models (AI), which triggers bots (autonomous engines) to go take action. This informs a master monitor that updates, adapts and improves the system. Self-aware means self documenting. Self-adapting means at the speed of the attack. Security is a digital business enabler, with guardrails.

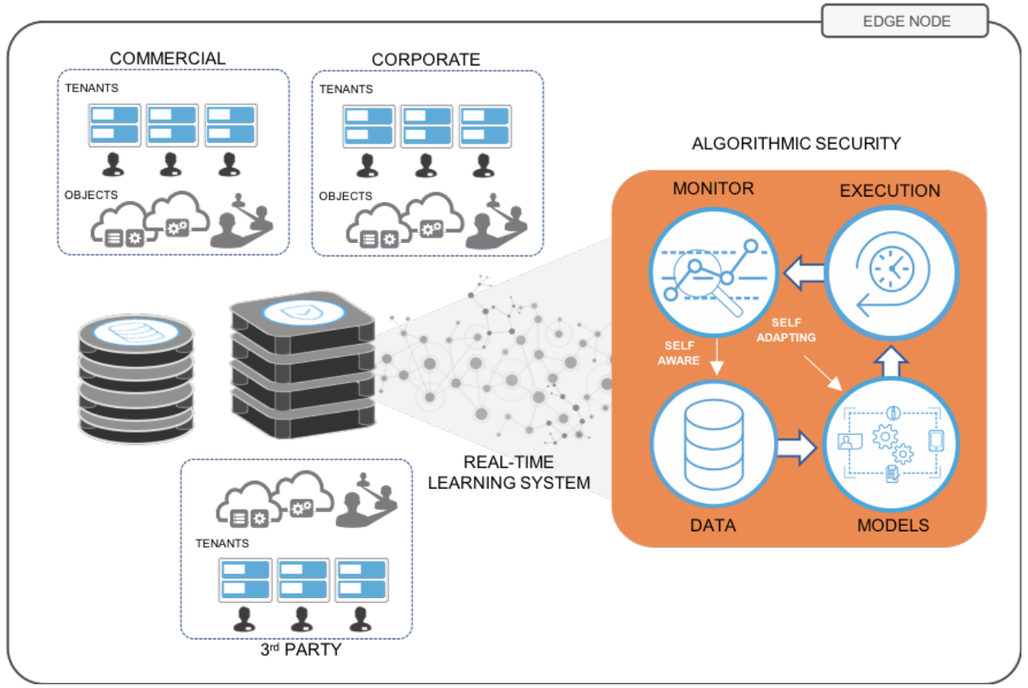
Constraints

1. IT security teams are unable to effectively transform at the same pace at which the threat they face is evolving. This leaves them trying to deal with the threat using the technology that they already know and have installed — which was not designed for the challenges of digital.
2. Segmentation has not necessarily been used as a corporate means to compartmentalize problems, and as such, all activities feel like boiling the ocean.
3. If a human is involved, the time to respond goes up by at least an hour. An automated autonomous attack can laterally compromise more than a thousand machines in a fraction of that time (in a large-scale flat network).
4. Teams are overwhelmed by multiple data sources that do not contain the relevant context and correlations to quickly detect, hunt and react to attack. This means data has to be constantly transformed, compared and verified.

Steps

1. Aggregate events with complex event processing: Analyze all cross-tenant communication to inform CEP models for each isolated network. All other incidents and alerts should be handled at security zone/tenant level.
2. Share intelligence with partners and customers: The cornerstone of digital business is multiparty business engagement, so reach out socially to your counterparts and share your architecture. Exchange incident data directly with real-time feeds. Security data equates to experience; your models become exponentially smarter.
3. Apply end-to-end behavioral analytics: UEBA (user and entity behavioral analytics) can educate your models on what normal looks like (self-aware and self-updating). Use CEP (step 1) to simplify UEBA and avoid the multisystem mashup of disparate data. With CEP feeding UEBA, this can be automated.
4. Develop algorithmic models: Start simple, have the system record a month of activity, learn from that history and deploy models in shadow mode. Set to being live when false alarms, or necessary interventions, reach near zero.
5. Pre-emptively respond: Define independent automated workflows for each response type. Multiple workflows can be triggered to scale the real-time (parallel) response.

Reference View



Forces

- Technology life cycles are shrinking, toward being throwaway. Managing the "things" is becoming pointless.
- The number of devices (IoT) and endpoints (with micro services) is headed toward millions.
- The average time for a breached company to perform a forensic assessment (on what happened) is six weeks and getting longer.
- The need to understand critical relationships (on the network) is becoming paramount.

Results

- Complexity is reduced (abstracted). Security is not about chasing patches on endpoints, but rather securing tenants (zones). Thus tenants can be on different clouds and handle changes locally. Security can focus on CEP.
- Attacks or incidents can be isolated and targeted at scale.
- Security is constantly learning, not just from direct experience, but from information shared with partners and customers.
- Sharing this architecture builds trust and can improve your counterparties' security – which further reduces you own risk as well.
- In this architecture you can approve non-sensitive and low-risk changes/activities automatically (get out of the way), with guardrails.
- IT security is no longer a detractor, but a strategic advantage.

Controls

- Unify security and risk metrics across ecosystem.
- Develop user and entity behavior analytics.
- Complex event processing.
- Predictive analytics and automated response.
- Service chaining and workflow optimization.
- Leverage algorithmic modeling.
- Autonomous security bots (SecBots).