Milton Security and the Argos Platform

Threat Hunting, Detection, and Response as a Service

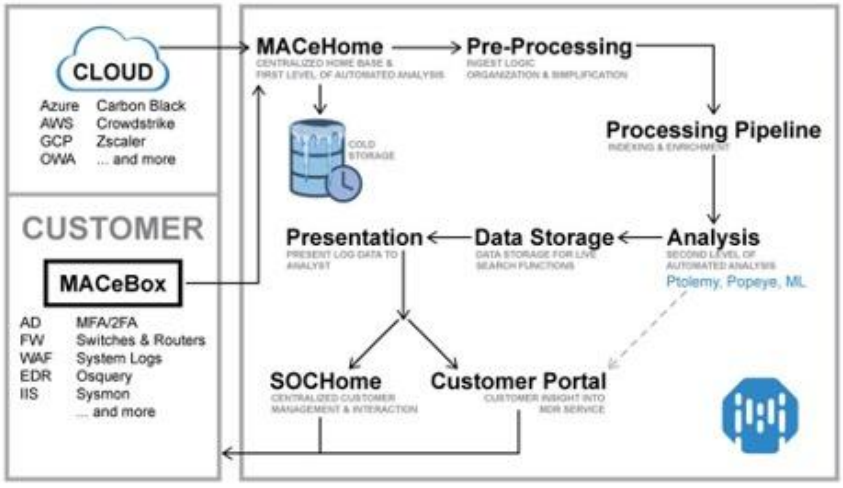
What is Argos?

Argos has been developed by Milton Security from the ground up as a Managed Detection and Response platform. Why did we do that rather than buying a SIEM off the shelf? Because security event detection is incredibly difficult, like trying to find a needle in a haystack. Actually, even worse than that, because the hay and the needles look very similar and are hard to distinguish. Legacy solutions create frameworks that generate alerts based on predetermined activity in order to solve the haystack problem. Unfortunately, this leads to alert storms for the SOC and alert fatigue for the security and technology teams.

Purchasing these security products is only a beginning. Without someone to review, analyze, and take action, the product never provides its real value. Many organizations don't have the budgets to maintain enough qualified staff to monitor events 24 hours a day. Malicious actors, however, are operating 24x7x365 globally. Trying to keep up with them requires a highly skilled and experienced team operating every minute of the day. Milton Security has just such a team in our Operations division, and they are using our world class Argos Platform to deliver those services.

How it works

Argos tackles this challenge with AI and ML methodology, threat intelligence, data enrichment, and human analysis. Essentially, the goal is to remove the haystack of data and leave behind the needles. This is done by applying Threat Intelligence and AI/ML tools and techniques to remove the hay and then sift through what

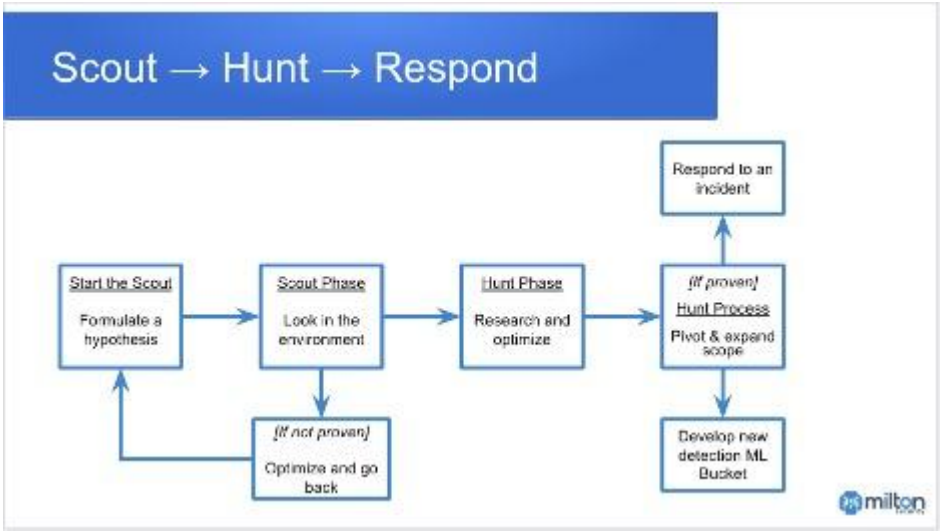


remains with a “magnet” to find the needles. Once the mass of good data is removed, the remaining data is where our human analysts operate, scouting for malicious activity. Scouting turns into active hunting by skilled SOC analysts.

Threat Hunting

The Milton Argos Platform is designed to allow our analysts to correlate data between various sources to paint larger pictures than any single endpoint agent can provide. With the addition of endpoint malware, CASB, and network access agents, we are able to analyze sources of data we see traversing the network. Beyond the endpoint data, Argos is designed to ingest everything and allow us to correlate across all endpoints and systems. We will want all cloud systems and on premise systems to have their data ingested into Argos. This typically offers us additional data that products like Netskope, ZScaler, etc may obfuscate.

In order to do this, all the security and technology data available in a client’s environment needs to be loaded into Argos. Once loaded into Argos, data ingestion logic is applied to align all the data into a single haystack. Then machine learning, threat intelligence, data enrichment, and a further round of machine learning are applied. Automated alerts and notifications are created for things that we know are bad and need to be remediated in some fashion (known bad actor operating from a specific IP address that should just be blocked, for example). Before these alerts are delivered, they must have a human analyst review and agreement that the alert is not a false positive. What remains is where our human analysts operate to scout, then actively hunt, and then trap/kill and mitigate the threat.



Remediation

In a client environment where we are actively involved in remediation, not just the analysis, scouting, hunting and alerting, Milton will need access to client systems. For example, the client may use a CASB and an EDR product for the endpoint. If we have accounts on those products, we can take action based upon a defined set of rules and procedures in a playbook. The CASB could be used to prevent an infected endpoint from touching any client systems. And the malware or EDR systems can be used to identify and isolate payloads on the system in question. Our staff will have accounts on your consoles so that they can correlate what they are seeing within Argos with real time event data in these systems.

All the Components

Milton Security consists of 3 main divisions: Operations, Platform Engineering, and 1MC-Labs. Each of these divisions interacts with the others to create a single virtuous cycle delivering a virtual SOC, Threat Hunting, and Response services to the client. Operations is where the deployment engineers, security analysts, threat hunters, and Argos Platform reside and deliver to the client. 1MC-Labs does threat research, malware analysis, and supports incident response. Everything that 1MC-Labs knows becomes a feed into Argos to enhance the platform, enabling it to learn and get smarter every day. Platform Engineering is responsible to develop the systems that form the Argos Platform and to build the integration with data sources and tools.

How We Integrate Our Clients

Integration & Deployment (I&D) is the set of processes which bring our new client into Argos and then maintain the integration over time. This is a relatively straightforward onboarding process run by our dedicated I&D team and follows these standard steps:

1. Scope, location, and method of access for data
2. Deploy MACeBox (virtual machine containing collection tools) into client networks
3. Configure systems (cloud and local) for data collection
4. Begin ingestion and forward process
5. Normalize data
6. Quality Assurance
7. Build playbooks
8. Go Live

Once live, we monitor and tune on a monthly basis. All clients have access to a portal with data on their service. In addition, every client has real time, live interaction with the security analysts and threat hunters in the SOC via communication platforms such as Slack and Microsoft Teams. Clients will receive End of Shift, End of Day, End of Week, and End of Month reports as developed in the playbook phase of I&D.

Protecting The Data

All client data is encrypted, both at rest and in transit. No access to data or Argos systems is allowed from clients external to the Milton data centers and SOC's. All client data is isolated from all other clients in private storage and computing segments. Milton's data centers are monitored 24x7 for inappropriate internal and external activity.

Put It All Together

Milton Security is truly a one stop shop for Security Operations, providing full featured monitoring, analysis, threat hunting, detection, and response services. This means that we become an extension of your security team, integrated into your program, and providing you with a world class SOC.