ALERT LOGIC™

QUICK FACTS BATTLECARD

Battlecard: AT&T MTDR (AlienVault)

Overview Summary

AT&T Managed Threat Detection and Response is built on the AT&T Unified Security Management (USM) platform, which combines the essential security capabilities needed for effective threat detection and response in a single pane of glass. Key capabilities include asset discovery, vulnerability assessment, Network Intrusion Detection (NIDS), Endpoint Detection and Response (EDR), and SIEM event correlation and log management. In addition, through the platform's AlienApps integration framework, the security monitoring and orchestration capabilities can extend to a wealth of 3rd party security technologies, giving their customers broad threat coverage for effective, early detection and rapid response.

QUICK FACTS BATTLECARD

AT&T MTDR (AlienVault)

	SOC Capabilities	Cloud Services	Price Analysis
Characteristics:	• 2 US Based SOCs, Primary in Austin, TX. 2nd in VA. • Financially backed SLA on all level of alarms. • Platform built on NIST Framework.	• Support, On-Prem, AWS, Azure, GCP, and Hybrid. • Zero focus on Containers in Docker (control plane and API). • All instances are logically segregated **(No Multi-tenant)**	• Offer a 14-day trial (tool only) • Packaged as a microservice to any current AT&T customer • Price is based on (hot) short term log storage
Weakness:	• Heavy remote PS and SSH use. • Limited visibility to devices using agent only. Very limited response actions with the agent. • Seldom recommend agent use.	• Unable to collect true network traffic in the cloud (flow logs) • Reliant on cloud microservices for cloud log visibility	• Storage costs include log enrichment at customer's expense because of larger ingestion sizes and larger instances. • Heavily dependent on third party products
Considerations:	• MTDR service built on USM Anywhere toolset. • Analysts can take response actions via Response Action Rules. • Integration with all edge and network products for monitoring. • AlienApp integration with all other security services offered by AT&T. • Platform does not compress logs and enriches them causing a higher storage volume than other competitors.	• Log data is forwarded and enriched prior to processing and storage, which increases transmission size and storage costs. • Data is stored in AWS Elastic Search for short term and AWS Glacier for long term storage • API integrations for collection and response into SaaS platforms via AlienApps.	**Tool** (for MSSP + Tool) • Essentials - 15-day storage $1075 p/m • Standard - 30-day storage $1696 p/m • Premium - 90-day storage $2595 p/m **Service** • $6,695 per month min (based on log consumption). • Note – AT&T uses the Trial (POC) as a deal closer often. POCs are led by SE's not the SOC team.

AT&T MTDR (AlienVault)

QUICK FACTS BATTLECARD

WHAT THEY DO:

- Maintain the (OTX) Open Threat Exchange, one of the largest crowd sourced threat intel feeds, with curated threat intelligence developed into a “correlation rules” or security use cases.
- AT&T touts deep threat intelligence with collaboration between the Alien Labs (threat intelligence team), the AT&T CSO and info collected from network of sensors feeding data to the AL team for evaluation.
- Integrated into multiple SaaS applications and 3rd party tools with “AlienApps” to collect and facilitate response. (Currently 450+ AA)
- Deployment team does a TMW with every deployment as a detailed source of discovery, pre-deployment. (Additional Upfront Cost)
- Offers a dynamic set of security services as part of their MSSP model.
- Offers a well-versed and dynamic set of consulting services.

QUESTIONS TO ASK:

- Do you need data stored for longer than 90 days?
- Is visibility into true network traffic in the cloud important to you?
- How quickly do you require your SOC to respond to any incidents?
- Are you using SentinelOne as your EDR?
- Are you looking for a full service or on a path to self-sufficiency?
- Is container-based coverage important to you?
- Do you need a consolidated view of both internal and external vulnerabilities?

AT&T MTDR DISADVANTAGES:

- Mid-market and enterprise have the choice to buy the platform only or MTDR as a service. This causes them to act as a tool vendor about 50% of the time.
- Cannot pull network-based traffic directly from cloud servers
- No agent-based scanning.
- Sensors limited to 600 MB IDS scan capability, no ability to scan 1GB or above without multiple sensors engaged.
- UEBA handling is non-existent.
- UBA works fairly-well but is still in an immature phase..
- No on-premise netflow or j-flow support.
- No investigation reporting.
- They store larger log files because they enrich logs and then store them without compression in hot storage.
- They charge on a per GB basis with Tiers of hot storage. TMW is part of deployment with a significant upfront charge to perform.
- Sensor are under-powered for the job they must do. Requires multiple sensors per deployment.

AT&T MTDR ADVANTAGES:

- Able to bundle services as an offer to anyone in their network i.e Internet circuit, DDoS, MTDR, MEPS, Managed Vuln. Program, etc…
- Integrates well with other AT&T services.
- DDOS protection is bar none, we don’t compete with DDoS
- There are 2 types of AlienApps – Advanced and Basic.
- Advanced AlienApps are API integrated applications. Currently 34.
- Basic AlienApps are log ingestion plug-ins only. Currently 350+.
- Easy deployment with remote services to assist with deployment.
- Threat modeling exercises done for all MTDR customers as a part of the pre-deployment planning.