AT&T Managed Threat Detection and Response

Deployment Plan for:

Tulane University

Presented by:
Todd Waskelis | AVP, AT&T Cybersecurity Consulting
Tony DeGonia | TSC 4, Public Sector, SLED/LED East

Saturday, March 11, 2023

AT&T

Today's Agenda:

1: Purpose

2: Current MTDR Service Tier

3: Deployment Timeline (Current)

4: Initial Scoping of the Environment

5: Current Efforts

6: Current Efforts - Threat Model Workshop

7: Current Efforts – Palo Alto PA7050 Firewall

8: New Deployment Plan

9: New Deployment Timeline (After TMW)

Purpose

The purpose of this presentation is to provide an update for the deployment of the AT&T Managed Threat Detection and Response (MTDR) Service. The service is currently being deployed within the information technology environment at Tulane University.

Outline of issues

There have been several issues that have plagued the MTDR deployment over the last 3 months. Below is an outline of the issues.

i. Sensor issues ingesting logs from the Palo Alto PA7050 Firewall. The overall volume of logs created and passed to the sensor is causing the sensor to overload, peak its resources and then crash.

ii. With the overload of the PA 7050 Firewall associated sensor, the number of logs that are passing through the sensor to the control node are causing an overutilization of resources which in turn causes the Cloud Based Control Node to falter. This is causing slow processing of the data as it is sent up to the cloud from the premise-based sensor.

iii. Threat Model Workshop was not conducted at the onset of the deployment because of an issue with the signing of the contract. The TMW has since been initiated and is almost a completed step in the deployment process.

Current MTDR Service Tier

6

6 TB Service Tier

6TB of Hot Storage, 90 days of indexed searchable events.

24x7 proactive security monitoring and investigation from the AT&T SOC

Built on Unified Security Management (USM)

Powered by AT&T Alien Labs threat intelligence

18

Sensors included

Purpose-built USM Anywhere Sensors deploy natively into each environment and help you gain visibility into all of your on-premises and cloud environments. These sensors collect and normalize logs, monitor networks, and collect information about the environments and assets deployed in your hybrid environments.

1

Threat Model Workshop

At AT&T Cybersecurity, we take the time to get to know our customers and their business. Every AT&T Managed Threat Detection and Response service begins with an on-site or remote threat model workshop led by AT&T Cybersecurity Consulting.

P

Perpetual Raw Log Storage

MTDR allows customers to store ingested raw logs in the USM Anywhere Cold Storage perpetually for the life of the customers service.

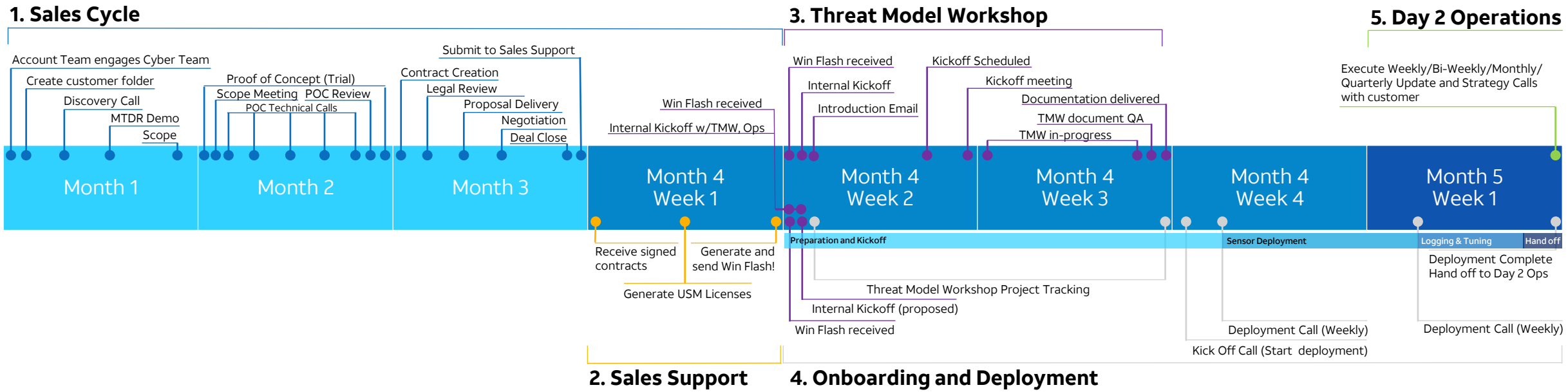
1

Security Analyst Training Session

The AlienVault USM Anywhere: Security Analysis 2-day course provides security analysts with the knowledge and tools to fully leverage AlienVault USM Anywhere to perform analyst duties

AT&T

Deployment Timeline (Current)



*Note: This is an approximate timeline of events for the sales and onboarding process. Deviations from the exact process occur often and timeline are extended and retracted based on customer requests and requirements.

**Note: This process represents a macro view of the service. More detailed processes and procedures are managed and documented by the various teams represented in this process.

AT&T

Initial Scoping of the Environment

Tulane University

Amazon Web Services
AWS Sensors: 2
24.494 GiB/Month with EPS: 3.1
Accounts: 2
Cloudtrails: Yes
EC2s: 3
S3 Buckets: 0
Umbrella: 0

Microsoft Azure
Azure Sensors: 2
20.814 GiB/Month with EPS: 3.6
Subscriptions: 2
Webapps: 4
Virtual Machines: 45
alienapp Sensors: 1 373.864 GiB/Month with EPS: 65.6

Office 365

On Premise
On-Premises Sensors: 4 12.242 TiB/Month 1842.7 average EPS
Locations: 3
Concurrent Users: 5000
Working Hours: 12x7
UTMs/NGFW/dedicated active Firewalls (enterprise): 3
Small low activity firewalls (SMB): 20
AlienVault NIDS(sensors): 3
Other Network Devices: 17
User workstations: 7500
Other Windows/Linux Servers: 553
Other NGFW EPS: 146
Other SFW EPS: 54
Other AVIPS EPS:4.2
Other DIPS EPS: 2.52
Other SPAM EPS: 3.15
Other WebProxy EPS: 2.52
Other NetDev EPS: 0.5
Endpoints: 0.025
Other webservers EPS: 0.63
Other servers: 0.21
Total Estimated Data Consumption: **12.661 TiB/Month**
Total Estimated EPS: **1915.0** with average log size: **2551 bytes**

Minimum Tier: 10 TB with filtering assumption at: 25%

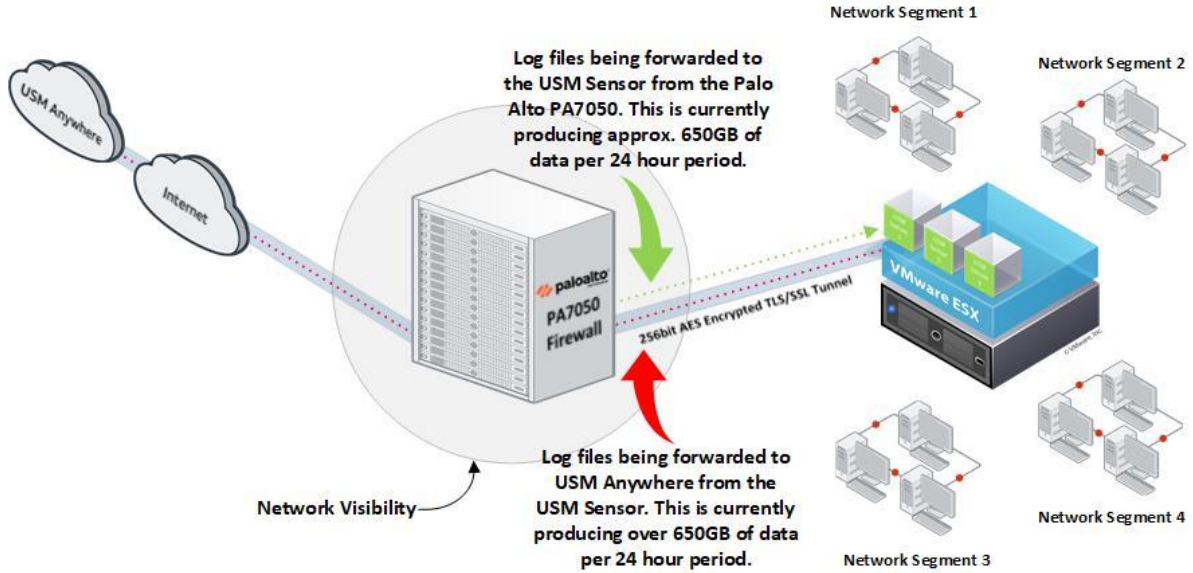
Recommended Tier: 15 TB

Current Efforts

Deployment Highlights

Initial Deployment of USM Sensors have occurred in the Datacenter and with an Azure Deployment

- **Itusmsensor1p01** – sensor dedicated to NxLog and Syslog ingested from the environment.
- **Itusmsensor1p02** - sensor dedicated to Palo Alto PA 7050 Firewall Pair.
- **Itusmsensor1p01** – had an issue flapping until the PA7050 stopped sending logs to p02.
- **Itusmsensor1p02** – had an issue flapping also because of the log volume coming from the PA7050 Firewalls.
- The cause of the flapping was determined to be because the USM Control Node was overwhelmed with the volume of logs coming from the **p02** sensor.



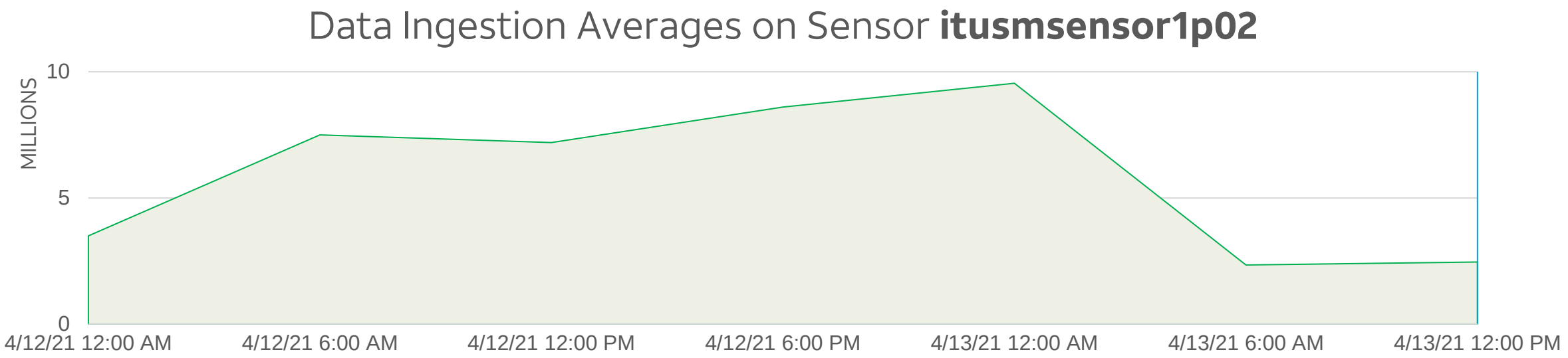
AT&T

Current Efforts

Deployment Highlights

Initial Deployment of USM Sensors have occurred in the Datacenter and with an Azure Deployment

- **Itusmsensor1p01** – sensor dedicated to NxLog and Syslog ingested from the environment.
- **Itusmsensor1p02** - sensor dedicated to Palo Alto PA 7050 Firewall Pair.
- **Itusmsensor1p01** – had an issue flapping until the PA7050 stopped sending logs to p02.
- **Itusmsensor1p02** – had an issue flapping also because of the log volume coming from the PA7050 Firewalls.
- The cause of the flapping was determined to be because the USM Control Node was overwhelmed with the volume of logs coming from the p02.



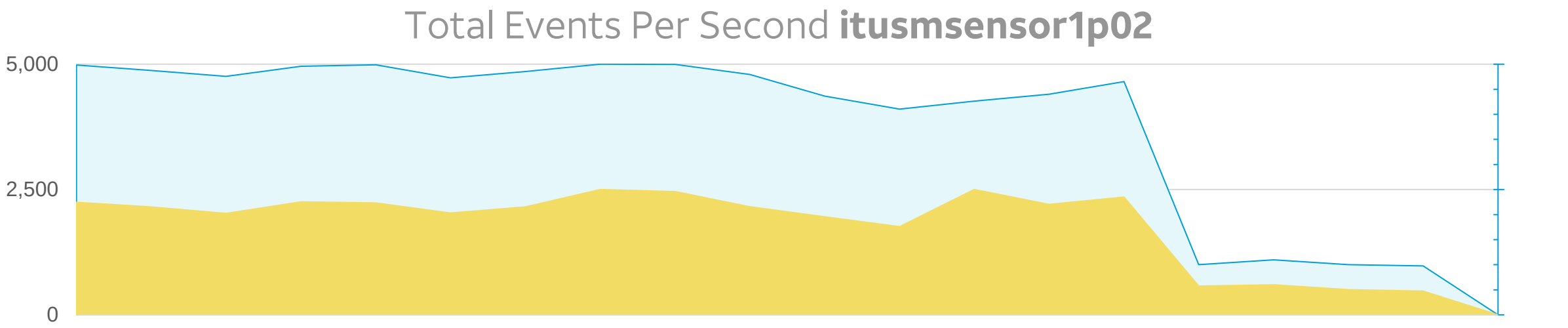
AT&T

Current Efforts

Deployment Highlights

Initial Deployment of USM Sensors have occurred in the Datacenter and with an Azure Deployment

- **Itusmsensor1p01** – sensor dedicated to NxLog and Syslog ingested from the environment.
- **Itusmsensor1p02** - sensor dedicated to Palo Alto PA 7050 Firewall Pair.
- **Itusmsensor1p01** – had an issue flapping until the PA7050 stopped sending logs to p02.
- **Itusmsensor1p02** – had an issue flapping also because of the log volume coming from the PA7050 Firewalls.
- The cause of the flapping was determined to be because the USM Control Node was overwhelmed with the volume of logs coming from the p02.



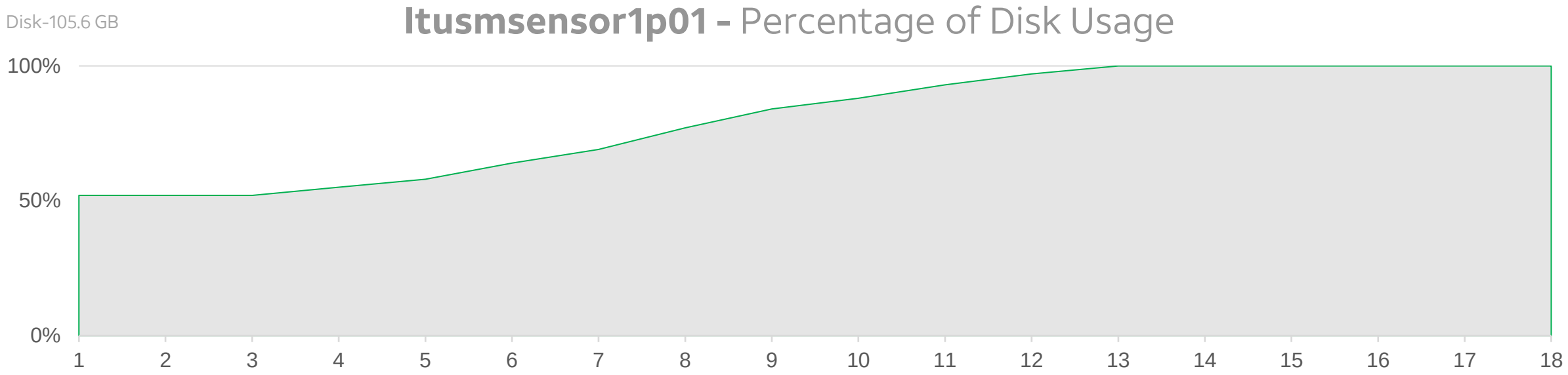
AT&T

Current Efforts

Deployment Highlights

Initial Deployment of USM Sensors have occurred in the Datacenter and with a sensor Azure Deployment.

- **Itusmsensor1p01** – sensor dedicated to NxLog and Syslog ingested from the environment.
- **Itusmsensor1p01** – had an issue flapping until the PA7050 stopped sending logs to p02.
- Most likely the reason for this 100% utilization of HDD on itusmsensor1p01 is because the sensor has been unable to pass data efficiently to the control node and has therefore cached the data awaiting stable connectivity.
- The cause of the flapping was determined to be because the USM Control Node was overwhelmed with the volume of logs coming from the **p02** sensor.

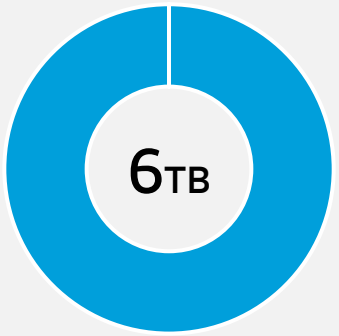


AT&T

Current Efforts – Palo Alto PA7050 Firewall

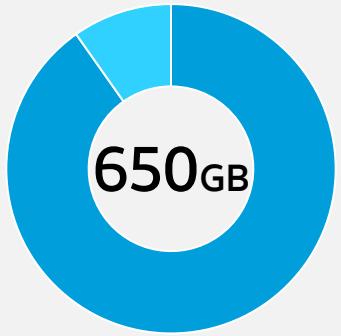
Tier Storage

Total monthly storage allocation in USM Control Node.



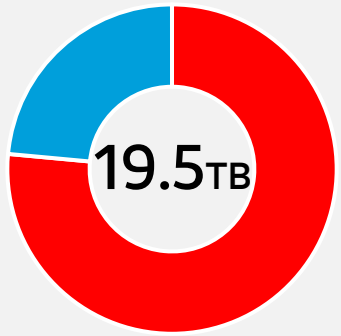
Daily Ingest

Estimated ingestion of logs into the **ltusmsensor1p02** sensor from the PA7050 Firewall on a 24-hr. basis.



Total Util.

Estimated total storage utilization with ingesting ONLY logs from the PA7050 Firewall over a 30-day period at the current rate of ingestion.

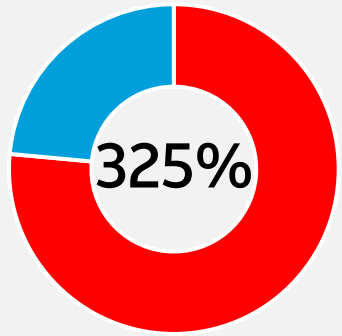


Sensor MTTC

Mean Time To Capacity for the **ltusmsensor1p02** sensor in the event it loses connectivity to the USM Control Node but continues to ingest logs from the PA7050 Firewall.

Tier Utilization

Estimated total storage capacity utilization overage for the USM Control Node in the event the PA7050 Firewall continues to send logs at its current rate and volume.

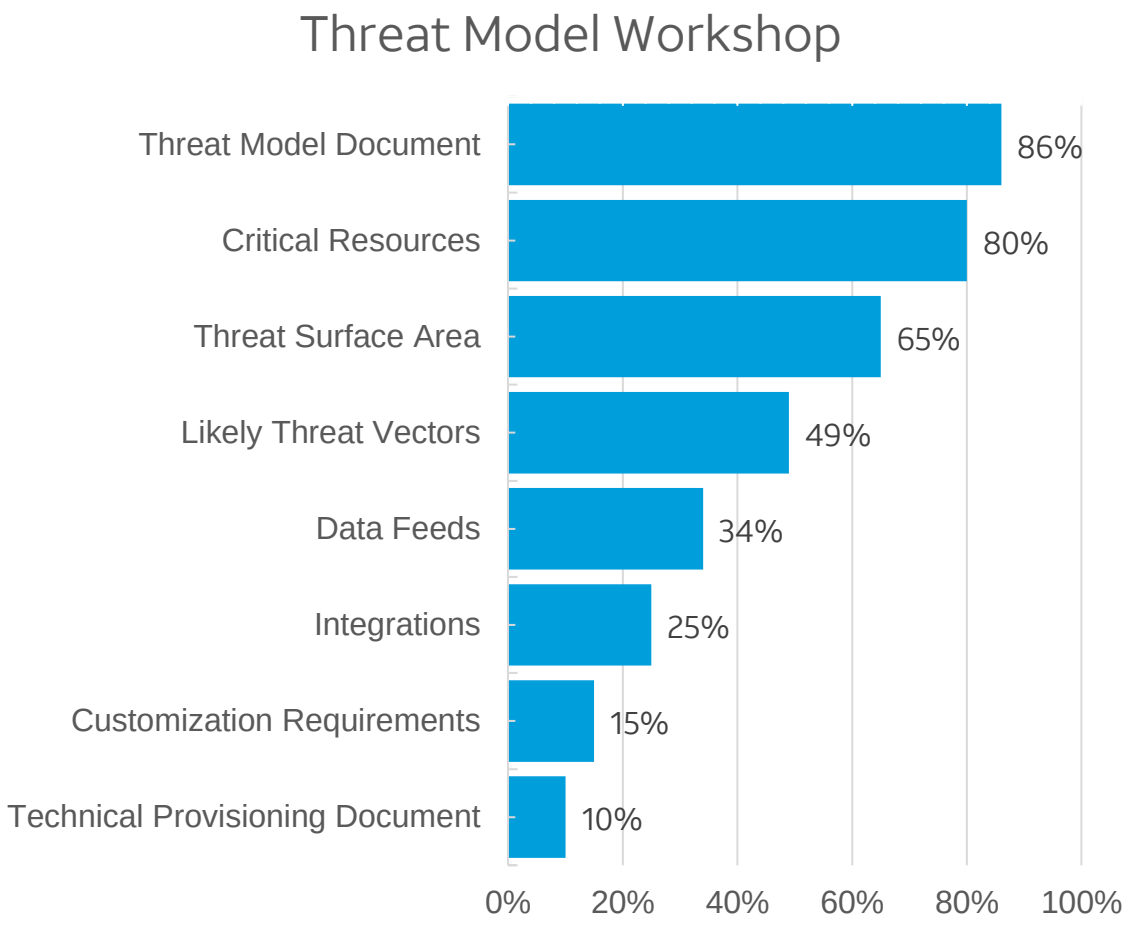


AT&T

Current Effort - Threat Model Workshop

Potential benefits:

- Meet the AT&T Cybersecurity team that will be working to help protect your enterprise
- Dedicated workshop time spent with the AT&T team
- Threat Model Document outlining your:
  - Critical Resources
  - Threat Surface Area
  - Any Identified Likely Threat Vectors
- Technical Provisioning Document outlining the following for your key business functions:
  - Integrations
  - Data Feed
  - Customizations Required For Deployment
- Enables the AT&T team to gain an understanding of the customer's environment and more effectively deploy the USM platform



AT&T

New Deployment Plan

AT&T

New Deployment Plan (After TMW)

A New Deployment Plan

- A New Deployment Plan with the initiation and execution of the Threat Model Workshop, there is a new deployment plan that will take shape to carry out the remainder of the onboarding. The new deployment plan provides the following efforts toward the deployment:

Phase 1

- Upon completion of the Threat Model Workshop and the TMW Quality & Assurance checks AT&T Cybersecurity Consulting will deliver documentation derived from the collection of information during the TMW. **(*Threat Model Document* (TMD) and *Technical Provisioning Document* (TPD))**
- Upon delivery of the TMD and TPD, the operations team will hold a series of calls to develop the ***Technical Deployment Document*.**
- At the delivery of the Technical Deployment Document, Operations will schedule a series of calls with the customer to begin the ***New Service Delivery Process*.**
- The initial call will be a review of all previously deployed sensors, a review of previously deployed data feed and integrations. As well as a discussion of existing log sources and how they fit into the new deployment plan. **(Initial Weekly Deployment Call)**
- The series will occur on an agreed upon day every week until the conclusion of the deployment project. **(Deployment Calls – Weekly)**
- In addition, there will be a second weekly ***"Check-in"*** call to ensure that everything is proceeding as planned for both the customer and AT&T. **(Weekly Check-in Call)**
- There will be a third call scheduled bi-weekly for Operations Management, Sales Management, Customer Management to discuss the advancement of the project from a senior level and discuss the USM Tier and how it is performing. ***(USM Control Node Utilization Review & Tier Review Discussion)***
- It is expected that sometime around the conclusion of Phase 1 of the project, AT&T and the Customer will need to discuss next steps to provide coverage of the entire environment, as phase 1 will only cover those most critical assets to be monitored. We do not anticipate having a sizing discussion during the execution of Phase 1 of the deployment project.
- Once Phase 1 of the deployment project is complete, There will be a handoff meeting to take Phase 1 to ***Day 2 Operations,*** where your Incident Response Plan will go into effect. Once that occurs, the customer security team will be fully engaged with the ***MTDR SOC Operations Team*** with 24x7 monitoring and collaboration via the **Incident Response Plan Document**. This will also include a ***Weekly/Monthly/Quarterly Meeting*** with your assigned **Threat Hunter** who will provide reporting into the condition of the services rendered and be able to discuss any changes the customer might want to see from the service.

Note***

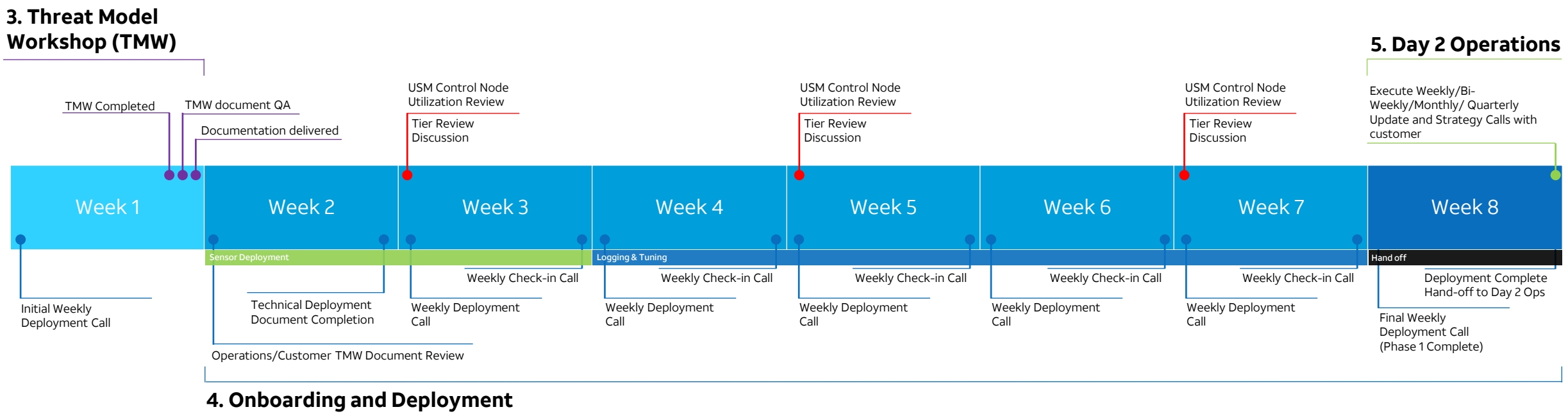
- This deployment was scoped originally at a **15TB Tier** and in order to accommodate the whole of the environment, all parties involved will need to collaborate to discover when, where, and how the second and third phases of the deployment project will take place. We will also need to discover when the customer can budget and request the upgrades to accommodate the second and third phases of the project.

Phase 2

- Once the upgrade to accommodate Phase 2 of the project is complete, we will then initiate the deployment team to re-engage for a phase 2 plan similar-to the one covered above

AT&T

Deployment Timeline (New)



*Note: This is an approximate timeline of events for the sales and onboarding process. Deviations from the exact process occur often and timeline are extended and retracted based on customer requests and requirements.

**Note: This process represents a macro view of the service. More detailed processes and procedures are managed and documented by the various teams represented in this process.

AT&T


AT&T