DESC – Technical Proposal – DNS, Internet Security, and Observability Project

Submitted To:	**Dubai Electronic Security Center (DESC)**
Submission Date:	**08.12.2025**
Reference No:	**PCS/DESC/762640**

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

Table of Contents

Proprietary and Confidential

This proposal contains information from Paramount Computer Systems LLC that is confidential and privileged. The information is intended for the private use of Dubai Electronic Security Center (DESC). By accepting this proposal, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from Paramount Computer Systems LLC. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Information

Company	Dubai Electronic Security Center (DESC)				
Document Title	DESC - Technical Proposal - DNS, Internet Security, and Observability Project				
Due Date	08.12.2025				
Ref.	PCS/DESC/762640				
Classification	Public	For Internal Use Only	Confidential	Strictly Confidential	Secret
Location	Dubai, UAE				
No. pages	89				
Document Type	Proposal		Deliverable		General – Approach

Recipient
Organization
Dubai Electronic Security Center (DESC)

Document History			
Version	**Date**	**Name**	**Notes**
1.0	26.11.25	Mohammad Khaled	Technical proposal

Cover Letter

To,

Dubai Electronic Security Center (DESC)

Date: 08.12.2025 **Reference No: PCS/DESC/762640**

Sub: DESC - Technical Proposal - DNS, Internet Security, and Observability Project

Dear Sir,

On behalf of Paramount, I am pleased to submit the enclosed proposal in response to the above referenced solicitation. I believe our proposal offers you an exceptional combination of innovative technology, real-world experience and unrivalled subject matter expertise that will help ensure the success of this initiative.

We understand the requirements and propose the following services:

- DNS Security – Security Domain – 1 Year license, Implementation Services
- Threat Intel -

We are delighted at the prospect of being evaluated by Dubai Electronic Security Center (DESC) as a potential vendor to collaborate with the company to offer our expertise that meets your requirements. We value the trust you place in a business relationship with us.

In summary, we believe that our proposed Solution will provide an excellent fit to your stated requirements. If you require any further information or clarification of any elements of our proposal, please contact me in the details mentioned below.

Yours Sincerely,

Amit Sharma
Solution Architect
Email – amit.sharma@paramountassure.com
Mobile - +971 564041683
Paramount Computer Systems LLC

Cyber Security is Paramount.

1. Executive Summary

Dubai Electronic Security Center (DESC), established in 2014 under Law No. 11 issued by His Highness Sheikh Mohammed Bin Rashid Al Maktoum, was created to position Dubai at the forefront of cyber resilience and digital protection. The Center plays a central role in strengthening the emirate's digital ecosystem by advancing security, enabling trusted information exchange, and supporting Dubai's ambition to be a global benchmark for innovation, safety, and technological leadership.

Guided by the principles of reliability, innovation, and collaboration, Dubai Electronic Security Center (DESC) drives the execution of the Dubai Cyber Security Strategy across its core domains—maintaining a secure digital environment, safeguarding the continuity of critical information systems, enabling secure and flexible information flow, and fostering research, innovation, and community awareness. The Center remains committed to supporting all government entities in achieving strong cyber maturity through effective governance, proactive threat mitigation, and continuous improvement.

As Dubai's digital footprint expands, Dubai Electronic Security Center (DESC) continues to play a strategic role in protecting the emirate's information assets, telecommunications infrastructure, and mission-critical systems. Through the development and adoption of advanced cybersecurity capabilities, the Center ensures that government entities operate in alignment with established information security standards and are equipped to navigate an evolving threat landscape.

In this context, Dubai Electronic Security Center (DESC) is inviting qualified partners to submit proposals for the design, deployment, and implementation of a comprehensive Archiving Solution under a Build, Operate, and Transfer (BOT) model. The solution is expected to integrate seamlessly with existing DNS and observability platforms while meeting stringent requirements for scalability, resilience, data governance, and cybersecurity compliance.

2. Bill of Quantities

	DNS Security - 1 Year		
S.No	Part No	Description	QTY
1	SD-DNSA-ENT-ADV - 1YR	DNS Armor Advanced Enterprise License- Includes DNS Firewall, Threat Intelligence, AI/ML Module for Advanced Protection, Web Filter, Application Access Control for On Premise and Off Premise Users and Assets - Unlimited QPS; Unlimited DNS Local Resolver/ DNS Forward Proxy	1
2	SD-DNSA-CP- 10T- 1YR	DNS Armor Control Plane - Up to 10 x Active Tenants	1
3	Premium Support - 1YR	Secure Domains Premium Support (24x7)	1
4	SD-PS-Scope	Secure Domains Professional Services Per Scope (Installation, Configuration and Knowledge Transfer)	1
5	SD-TAM- D	Technical Account Manager - Dedicated	1
	Anomali Security and AI Platform: 1 Year		
	Anomali - Threat Stream - **Enterprise SaaS Edition - Anomali's CTI - Threat Intelligence Platform**		
6	TS-100-SAAS- ENT	Anomali Threat Stream Enterprise SaaS - Threat Intelligence Platform: - Unlimited Users. - Unlimited Integrations.	1
		Anomali University: Unlimited Access Continuous Online E-learning includes courses and certifications	
		Anomali TAM: Dedicated TAM During the Subscription Period for Onboarding, Adoption, Integrations, Quarterly Success Review, Regular Calls	
	Anomali ThreatStream **ONPREM Hosted License**		
7	TS-103-ONPM-ENT	Anomali Threat Stream - Enterprise - ONPREMISE Hosted License for ONPREMISE Deployment	1
	Anomali ThreatStream **DR Hosted License**		
8	TS-103-ONPM-ENT	Anomali Threat Stream - Enterprise - DR Hosted License	1
	Anomali **ThreatStream HA Hosted License**		
9	TS-103-ONPM-ENT	Anomali Threat Stream - Enterprise - HA Hosted License	1

3. DNS Security Solution - DNS Armor

3.1. Solution Architecture

The proposed **DNS Armor™** platform is architected as a **Sovereign Private Cloud** solution, purpose-built to transform DESC into a centralized provider of cyber-defense for the Dubai Government.

Unlike traditional solutions, this architecture offers a **flexible Multi-Tenant framework**. It empowers DESC to dictate the governance model ranging from fully managed security for smaller entities to delegated self-service for mature organizations while maintaining absolute data sovereignty within the UAE.

The architecture is designed with the expectation that all **DNS query analytics, statistics, reporting, log search, and security intelligence** will be performed through DESC's enterprise **Data Lake solution**. This approach enables comprehensive cross-domain security analytics, advanced correlation with other telemetry sources, and centralized business intelligence capabilities.

However, the platform **fully supports direct access to DNS logs, analytics, and search operations through DNS Armor™** native interface as an optional add-on for teams requiring DNS-specific operational visibility. This capability is optional and subject to additional storage infrastructure requirements as detailed in the Infrastructure Requirements section of this document.

3.2. High Level Design

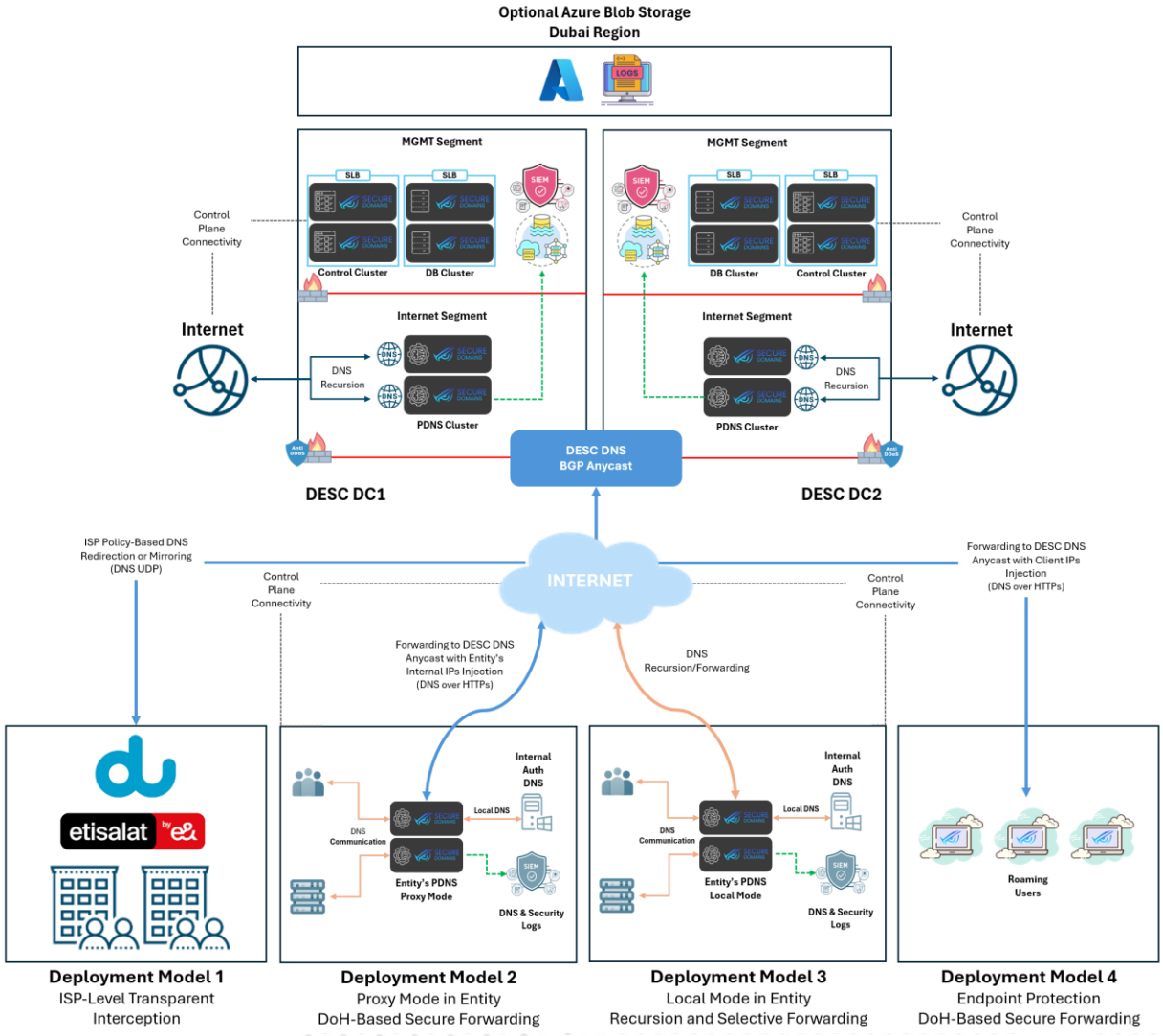


Figure 1 - High level architecture diagram

3.3. Core Architecture Layers

Control Plane (Management Segment)

- Redundant control clusters across both datacenters
- Multi-tenant policy management with per-entity isolation
- Centralized DESC oversight dashboard

- Secure connection to Secure Domains threat intelligence feeds server

Data Plane (Internet Segment)

- DNS Armor™ engine clusters in both datacenters
- Anycast BGP routing for automatic geographic failover
- EDNS Client Subnet support for client visibility
- Real-time threat detection and policy enforcement
- High-performance caching layer

Logging and Storage Layer (Optional)

- Centralized log aggregation to Azure Blob Storage (Dubai Region)
- Optional log collection from entity-managed infrastructure
- SIEM integration via syslog using multiple protocols (UDP, TCP, TLS, HTTP, HTTPs)
- Configurable retention policies for compliance

Component	Location	Purpose
Protective DNS	DESC DC1 + DC2	DNS resolution, threat detection, policy enforcement, ML & Behavioural analysis
Control Plane	DESC DC1 + DC2	Multi-tenant management, entity onboarding and administration
Database Cluster	DESC DC1 + DC2	Configuration, analytics, audit trails
Optional Log Storage	Azure Blob Storage (Dubai)	DNS logs, security events, compliance archives
Threat Intelligence	Secure Domains Infrastructure	Malicious domain feeds, threat intelligence, web filtering feeds

3.4. Infrastructure Requirements

3.4.1. Compute Resources (Per DC)

Component	QTY	vCPU	Memory	Storage	Hypervisor	Purpose
Control Cluster Node	2	16	256 GB	1 TB SSD	VMware ESXi 6.5 or newer	Multi-tenant policy management, entity onboarding, API gateway
Database Cluster Node	2	4	16 GB	500 GB SSD	VMware ESXi 6.5 or newer	Configuration storage, analytics, audit trails

DNS Armor Engine (PDNS)	2	16	128 GB	1 TB SSD	VMware ESXi 6.5 or newer	DNS resolution, threat detection, policy enforcement, ML & behavioral analysis

Total DESC Infrastructure (Both DC1 and DC2):

- Control Cluster: 4 nodes (2 per DC)
- Database Cluster: 4 nodes (2 per DC)
- DNS Armor Engine: 4 nodes (2 per DC, scalable based on query volume)

Note: *Virtual appliance (local resolver) specifications for Deployment Models 2 and 3 are subject to entity-specific sizing guidelines based on user count, query volume, and deployment model complexity. Detailed sizing guidelines shall be provided during entity onboarding assessment.*

3.4.2. Optional Storage Resources

Component	Size	Purpose
Network Attached Storage (NAS) *Optional*	100TB High-Performance Redundant	**On-demand log download cache for DNS Armor Control Cluster** • Temporarily stores DNS logs downloaded from Azure during search operations • Maximum 14-day search window per query to prevent system overload • Required only if DESC requires log viewing through DNS Armor™ interface
Azure Blob Storage Account (Dubai Region) *Optional*	Subject to sizing evaluation	**Primary DNS log repository** • Permanent storage for all DNS query logs and security events • Control Plane downloads logs on-demand to NAS when searches are performed • Supports future data lake integration via RESTful API (subject to evaluation) • Required if DESC mandates centralized logging or out-of-box archival

Logging Architecture Notes:

- **Primary Storage**: Azure Blob Storage (Dubai Region) serves as the authoritative repository for all DNS telemetry with unlimited retention capacity and data sovereignty compliance.

- **On-Demand Retrieval Model**: The 100TB NAS provides temporary cache storage for DNS Armor Control Cluster to download logs from Azure only when search operations are initiated by DESC operations team.
- **Search Window Constraint**: Each search operation is limited to maximum 14-day time range to prevent system performance degradation from downloading and processing excessive data volumes from Azure to on-premises NAS.
- **Storage Sizing**: NAS capacity (100TB) accommodates multiple concurrent 14-day search windows. Azure Blob Storage sizing is subject to evaluation based on expected DNS query volumes, retention policies, and data lake requirements.
- **Data Lake Integration**: Custom RESTful API integration with DESC's enterprise data lake platform is subject to evaluation with the datalake vendor.

3.4.3. External Infrastructure

The DNS Armor™ platform integrates with external network and security infrastructure:

Application Delivery Controller (ADC) / Server Load Balancer (SLB)

- Quantity: 2 per datacenter (active-active or active-passive HA)
- Purpose: Load distribution and high availability for Control Plane and Database Cluster communication
- Technical Requirements:
    - Layer 4 and Layer 7 load balancing capabilities
    - Active health monitoring with customizable check intervals for backend nodes
    - SSL/TLS termination and offloading support
    - Session persistence (sticky sessions) for API gateway and management interface
    - Support for TCP and HTTPS health probes
    - Connection pooling and timeout management

DDoS Protection System

- Deployment: Internet edge / perimeter protection
- Purpose: Volumetric and protocol-level attack mitigation
- Technical Requirements:
    - Expected to be provided through DESC's existing or planned 3rd-party DDoS mitigation solution

- **Must include DNS-aware DDoS protection capabilities** with support for:
  - DNS query rate limiting per source IP
  - DNS amplification attack detection and mitigation
  - DNS flood attack (query flood) protection
  - NXDomain flood detection
  - DNS tunneling anomaly detection
- Layer 3/4/7 attack mitigation with minimum 100Gbps scrubbing capacity recommended
- Integration with upstream ISP/transit provider for volumetric attack scrubbing

3.5. Anycast DNS Architecture

How It Works:

- Unified DNS anycast VIP announced from both DC1 and DC2 via BGP
- Clients resolve DNS using the same anycast IP regardless of location
- BGP automatically routes traffic to nearest/healthiest datacenter
- Stateless design enables seamless failover without client awareness

Benefits:

- Automatic sub-second failover during datacenter maintenance or failure
- Natural load distribution between datacenters
- Sub-10ms regional latency for UAE government users
- Simplified client configuration across all deployment models
- Either datacenter can handle 100% of query load

3.6. EDNS Client Subnet (ECS) Implementation

Purpose: Preserve original client identity throughout DNS resolution chain

How It Works:

- ECS option (RFC 7871) injected at various points depending on deployment model.
- Original client IP address or user identifier embedded in DNS query.
- DESC maintains visibility of individual users across all deployment models.
- Enables granular policy enforcement at per-entity, per-subnet, or per-user level.

Benefits:

- Complete audit trails with original source attribution
- Granular security policies based on user/device identity
- Compliance with government forensic and investigation requirements
- Client IPs remain within DESC-controlled infrastructure

3.7. Multi Tenancy

The DNS Armor™ architecture separates the Infrastructure Layer (owned by DESC) from the Logical Layer (Tenants). This design allows DESC to offer DNS Security as a Service through two distinct operational models, depending on the maturity and requirements of the onboarded government entity:

- **Model A: Centralized Managed Security (DESC-Managed)**
    - **Use Case:** Ideal for smaller entities or those lacking dedicated SOC teams.
    - **Operation:** DESC acts as the sole administrator. The entity's traffic is routed to the platform, and DESC's SOC team manages policies, monitors threats, and handles incident response centrally. The entity receives periodic executive reports but requires no direct access to the system.
- **Model B: Delegated Administration (Entity-Managed)**
    - **Use Case:** Designed for large, mature entities (e.g., Police, Utilities) with their own SOC/NOC teams.
    - **Operation:** DESC provisions a dedicated "Tenant Environment." The Entity is granted **Direct Access** via RBAC (Role-Based Access Control) to their specific dashboard. They can independently:
        - Customize block pages and allow-lists.
        - View real-time traffic logs specific to their organization.
        - Integrate logs into their own local SIEM.
    - **Governance:** While the Entity manages daily operations, DESC retains "Super-Admin" privileges to enforce mandatory global blocking policies (e.g., national threat alerts) that override tenant settings.

3.8. Deployment Models

DNS Armor™ supports four distinct deployment models to address diverse government entity requirements:

3.8.1. ISP Level Transparent Interception

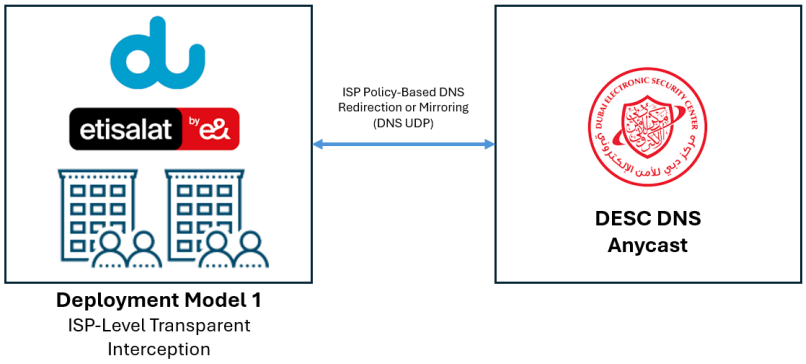


Figure 2 – Deployment Model 1

Carrier-grade DNS interception at ISP network edge transparently redirects or mirrors DNS queries from designated government entity IP ranges to DESC's DNS Armor™ anycast infrastructure without requiring any configuration changes at entity networks or end-user devices.

Traffic Flow:

1. Government entity user initiates DNS query
2. ISP edge equipment (traffic broker/DPI) intercepts DNS traffic (port 53)
3. ISP injects EDNS Client Subnet (ECS) with original source IP
4. Traffic redirected to DESC DNS Armor™ anycast infrastructure
5. DESC performs security inspection, threat analysis, and policy enforcement
6. Legitimate queries forwarded to authoritative DNS servers
7. Response returned to government entity user

Key Considerations:

- Zero-touch deployment: No entity infrastructure or configuration changes required
- ISP dependency: Protection effectiveness relies on ISP capabilities and cooperation
- Cleartext DNS: Traffic between user and ISP edge remains unencrypted (UDP/TCP port 53)
- Limited granular visibility: ECS provides subnet-level visibility, but no internal entity network context
- Suitable for: Mass protection, low-maturity entities, emergency deployment scenarios

3.8.2. Entity Proxy Mode with DoH Forwarding

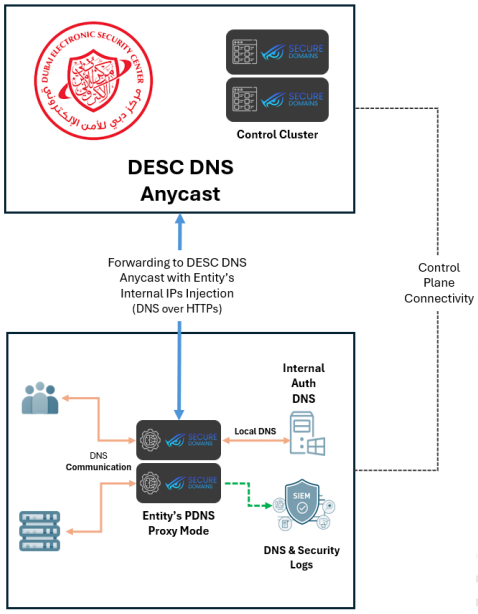


Figure 3 – Deployment Model 2

DNS Armor™ proxy resolver deployed within government entity's network which handles internal domain resolution locally while forwarding external queries to DESC's private cloud where DNS security inspection (AI-based threat detection, threat intelligence feeds, policy enforcement, etc) is performed centrally.

Traffic Flow:

1. Government entity user initiates DNS query via DHCP-assigned resolver
2. DNS Armor™ proxy (Secure Domains resolver) receives query and performs split-horizon decision
3. Internal domain query: Resolved locally via entity's authoritative DNS (Active Directory, etc.)
4. External domain query: Proxy injects ECS with user IP and forwards to DESC private cloud
5. DESC DNS Armor™ platform performs AI-based security inspection, threat feed analysis, and policy enforcement
6. Legitimate queries resolved and response returned to entity proxy
7. Proxy delivers response to user

Key Considerations:

- Centralized logging: DNS queries and security events are logged externally using DESC owned Azure storage account
- Syslog integration: Same VM can exchange syslogs with entity's SIEM for local visibility

- Cloud-managed resolver: The virtual resolver appliance is centrally managed via DNS Armor™ control cluster in DESC private cloud. Internet connectivity to control cluster required for policy updates and health monitoring
- Split-horizon DNS: Full support for internal and external domain resolution
- Centralized security: All threat detection and policy enforcement performed at DESC
- Entity infrastructure required: Minimum of two virtual machine per entity (proxy only)
- DESC dependency: Requires connectivity to DESC for external query security inspection
- Graceful degradation: Entity maintains internal DNS resolution if DESC connectivity lost
- Full client visibility: ECS preserves individual user IP addresses
- Full client visibility: ECS preserves individual user IP addresses
- Suitable for: Entities with Active Directory, internal services, medium-to-large organizations (500-5,000 users)

3.8.3. Entity Local Mode with Selective Forwarding

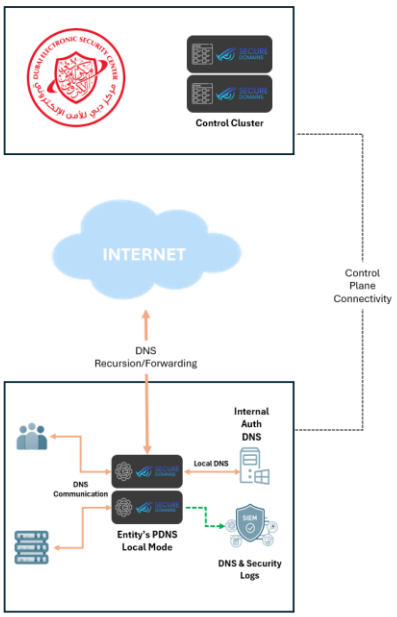


Figure 4 – Deployment Model 3

Complete DNS Armor™ engine deployed at entity premises with full security capabilities. Performs local DNS resolution AND local AI-based security inspection, threat analysis, and policy enforcement entirely within entity network with no dependency on DESC infrastructure.

Traffic Flow:

1. Government entity user initiates DNS query
2. Entity's DNS Armor™ engine (full security platform) receives query
3. **Path A - Internal Domain:** Resolved by entity's authoritative DNS locally
4. **Path B - External Domain:** Full local DNS resolution with concurrent AI-based threat analysis
5. DNS Armor™ engine performs local security inspection using:
    - AI-based threat detection algorithms
    - Locally synchronized threat intelligence feeds
    - Entity-specific policy enforcement rules
6. Malicious queries blocked locally; legitimate queries resolved
7. Response delivered to user

Key Considerations:

- Syslog integration: Same VM can exchange syslogs with entity's SIEM for local security operations
- Optional DESC integration: DNS and security logs can be forwarded to DESC Cloud for centralized visibility (optional)
- Flexible logging: Entity chooses between local-only logging or bidirectional sync with DESC
- Full autonomy: Complete DNS security platform operating independently at entity premises
- Cloud-managed resolver: The virtual resolver appliance is centrally managed via DNS Armor™ control cluster in DESC private cloud. Internet connectivity to control cluster required for policy updates and health monitoring
- No DESC dependency: Entity maintains full DNS resolution and security inspection capabilities locally
- Local AI processing: Threat detection and policy enforcement performed within entity network
- High-performance requirements: Entity VM must support full DNS Armor™ engine with AI capabilities

- Advanced IT expertise required: Entity manages local security platform
- Data sovereignty: All DNS processing and logging can remain within entity infrastructure
- Optional DESC visibility: Entity decides whether to share logs with DESC for cross-entity threat correlation
- Suitable for: Large ministries (5,000+ users), entities with strict data sovereignty requirements, organizations requiring operational independence

3.8.4. Endpoint Protection with DoH

Lightweight DNS client agent installed directly on individual endpoint devices (Windows & macOS). Agent establishes encrypted DoH tunnels from endpoint to DESC anycast, providing DNS security regardless of network location (corporate, home, public Wi-Fi, international travel).

Traffic Flow:

1. Government user device initiates DNS query from any network location
2. DNS client agent intercepts query at operating system level
3. Agent injects ECS with user identifier (email, employee ID, or device UUID)
4. Query encrypted and sent to DESC anycast via DoH tunnel (HTTPS port 443)
5. DESC performs security inspection and applies user-specific policies
6. Legitimate queries resolved and response returned via encrypted tunnel
7. Agent caches response and delivers to application
8. User application receives response transparently

Additional Capabilities:

- Centralized logging: All endpoint DNS queries and security events logged in DESC Cloud
- Unified policy management: Consistent security policies across all roaming users

Key Considerations:

- Location-independent protection: Security follows user across any network (corporate, home, travel)
- Zero trust model: All networks treated as untrusted
- Agent deployment required: Software installation on all protected endpoints
- Per-user attribution: ECS contains user/device identifier for granular policies
- End-to-end encryption: DoH protects queries from local network eavesdropping
- Mobile platform limitations: iOS/Android may require VPN-based implementation

- Potential VPN conflicts: May interfere with corporate VPN split-tunneling
- Offline resilience: Agent caches policies for degraded-mode operation
- Suitable for: Remote workers, BYOD programs, VIP personnel, field operations, contractor access

Key Differences Summary:

Aspect	Model 1: ISP Interception	Model 2: Proxy	Model 3: Local	Model 4: Endpoint
Deployment Location	ISP edge infrastructure	Entity network	Entity network	Roaming devices
Security Processing	Centralized at DESC	Centralized at DESC	Local at entity	Centralized at DESC
AI Threat Detection	DESC Cloud	DESC Cloud	Entity premises	DESC Cloud
Entity Infrastructure	None	2 VM (proxy)	2 VM (full engine)	Client agent software (Windows/macOS)
Internal DNS Support	N/A	Yes (split-horizon)	Yes (split-horizon)	Yes (split-horizon over VPN)
Cloud Management	Via DESC control cluster	Via DESC control cluster	Via DESC control cluster	Via DESC control cluster
Logging	DESC Cloud only	DESC Cloud + optional SIEM	Entity SIEM + optional DESC sync	DESC Cloud only
Data Sovereignty	Queries forwarded to DESC	Queries forwarded to DESC	All processing stays local	Queries forwarded to DESC
Network Coverage	Corporate network only	Corporate network only	Corporate network only	Any network (corporate, home, travel)
Encryption in Transit	No (cleartext DNS)	Yes (DoH)	N/A (local processing)	Yes (DoH)
Entity Visibility	Public source IP	Public & private source IPs	Public & private source IPs	Public & private source IPs

Granular policies	Public source IP	Public & private source IPs	Public & private source IPs	Public & private source IPs

3.9. Unique Features

AI & Heuristics

DNS Armor™ leverages cutting-edge Artificial Intelligence (AI) technologies to proactively detect and block sophisticated DNS threats including tunneling, fast flux, data exfiltration & infiltration, and command-and-control (C2) communications. Real-time analysis of traffic patterns and query behavior provides instant identification and prevention of suspicious activities through advanced heuristics including entropy analysis, pattern recognition, and rate-based detection. This proactive approach significantly enhances overall network security, reduces risk exposure, and ensures threats are neutralized before they can cause harm.

Reporting & Visibility

DNS Armor™ delivers comprehensive reporting and visibility through real-time and historical DNS and DNS Firewall logging, advanced trend analysis, and detailed statistics. Our solution provides extensive logging capabilities including:

- **Detailed DNS Query Logging**: Complete visibility into all DNS requests across your network
- **Detailed DNS Firewall Logging**: Comprehensive records of all security actions taken by the firewall

The statistical reporting includes:

- **Top DNS Requestors**: Identify the most active clients on your network
- **Top DNS Domains and Record Types**: Understand the most frequently accessed resources
- **Top DNS Firewall Requestors**: Pinpoint potential security issues by client
- **Top DNS Firewall Domains and Record Types**: Recognize the most blocked threats
- **Top DNS Firewall Security Policies**: Gain insights into which security policies are most actively enforced

Services Availability

DNS Armor™ operates in 52 global data centers, each offering both DNS firewall services and localized log storage in the same region. This dual-plane presence guarantees data never leaves its jurisdiction, ensuring full compliance with data sovereignty and residency

requirements. Additionally, DNS Armor™ is fully available in GCC markets, including Qatar, UAE, KSA and Egypt delivering in-country service and logs for maximum compliance and performance.

Automated Feeds

DNS Armor™ harnesses the power of automated feeds to provide robust, multi-layered protection for the network. The proposed solution includes three specialized feed categories, each continuously updated to ensure protection against the latest threats and web accessibility control:

- Multiple specialized threat feed categories including Bogons, Malware, Malware Hosts, Malware C2, Ransomware, Botnets, Phishing, etc.
- Multiple specialized web filtering feed categories including Adult, Gambling, Search Engines, Drugs, Phishing, Fraud, Social Networking, Dating, Streaming Media, Ecommerce, and Gaming.
- Multiple applications and services feed categories covering collaboration tools (Microsoft Teams, Zoom, Slack), cloud storage (OneDrive, Google Drive, Dropbox), productivity suites (Office 365, Google Workspace), and communication platforms (WhatsApp, Telegram, Signal).
- Export feeds in RPZ format to integrate with 3rd party systems.

Data Sovereignty

DNS Armor™ employs a modular, distributed architecture designed to ensure complete data residency compliance for cloud-based security processing. When utilizing **Proxy Mode** or **Endpoint Agent** deployments—where DNS queries are processed through DNS Armor™ cloud infrastructure—all DNS logs, security telemetry, and archived data remain exclusively within the customer's assigned geolocation boundary (Riyadh, Saudi Arabia).

This localized architecture guarantees that no DNS transaction data, security logs, or analytical information crosses national borders or leaves the designated region. Unlike competitors relying on centralized global storage infrastructure, DNS Armor's region-specific deployment model ensures full compliance with Saudi data residency requirements and regulatory mandates.

Key Data Sovereignty Features:

- **In-Region Processing:** All cloud-based DNS security analysis performed within Saudi Arabia infrastructure
- **Local Log Storage:** Complete DNS query logs and security event data archived within national boundaries
- **Geographic Isolation:** No data replication or synchronization to international data centers
- **Regulatory Compliance:** Meets KAMC, BAHRAIN data residency requirements and Saudi Arabian data protection regulations

Note: Local Mode deployments process all security functions on-premises, providing an additional layer of data sovereignty where DNS queries never leave the customer's infrastructure for security processing.

First Cloud DNS Firewall Locally Developed in GCC

DNS Armor™ is uniquely positioned as the first cloud DNS firewall solution developed within the GCC region. This local development ensures the solution is closely aligned with specific market challenges and regulatory frameworks faced by regional enterprises. Unlike global competitors, DNS Armor™ directly addresses regional cybersecurity threats and compliance requirements, offering customers the confidence that the solution is customized to their unique operational environment and local jurisdictional standards.

Native Multi Tenancy Support

DNS Armor™ offers robust multi-tenancy capabilities, enabling Managed Service Providers (MSPs) and organizations to manage multiple entities, views or customer environments seamlessly from a single platform. By eliminating the need for expensive, standalone tools, organizations can deliver cost-effective, scalable, and value-added security services efficiently.

Service Availability

DNS Armor™ is available across a broad network of 52 global data centers, each providing both DNS firewall services and localized log storage within the same jurisdiction. This architecture ensures compliance with data sovereignty and residency laws, a critical requirement for organizations operating within regulated regions such as the GCC. Businesses can therefore trust that their data remains securely stored locally, minimizing regulatory and compliance risks associated with cross-border data transfers.

AI-powered Detection

DNS Armor™ leverages cutting-edge Artificial Intelligence (AI) technologies to proactively detect and block sophisticated DNS threats such as tunneling, data exfiltration, and command-and-control (C2) communications. Its real-time analysis of traffic patterns and query behavior provides instant identification and prevention of suspicious activities, significantly enhancing overall network security. This proactive approach reduces risk exposure and ensures threats are neutralized before they can cause harm.

Time-based Policy Activation

DNS Armor™ is the only DNS security solution offering advanced time-based policy activation at the DNS layer. Unlike any other competitor, DNS Armor™ empowers organizations to dynamically schedule and automate DNS security policies. This exclusive capability allows precise control over DNS traffic, ensuring enhanced security measures during critical time

windows, operational peaks, or specific security-sensitive periods. With DNS Armor™, your security posture automatically adapts to your unique business rhythms, providing unmatched protection and operational flexibility.

3.10. DNS Security Use Cases

Malware Attacks

Malware exploits DNS to infiltrate and propagate within networks. DNS Armor™ blocks malicious domains at the DNS level, preventing malware from downloading or communicating with external command and control (C2) servers.

Ransomware Attacks

Ransomware encrypts files and demands a ransom for decryption keys. Attackers use DNS for key exchanges via DNS tunnels and to spread ransomware through malicious websites. DNS Armor™ mitigates this threat by blocking access to infected domains.

Phishing Attacks

Phishing scams trick users into visiting fake websites or downloading malicious software. By leveraging threat intelligence, DNS Armor™ automatically blocks access to phishing sites, reducing data theft risks.

DNS Tunnelling

Attackers use DNS queries to hide malicious data transfers or C2 communications. DNS Armor™ detects and prevents tunnelling by monitoring unusual DNS behaviour, stopping data exfiltration before it bypasses security controls using AI based techniques and heuristics including entropy, pattern and rate analysis.

Command and Control (C2) Attacks

Attackers establish C2 channels through DNS to maintain control over compromised systems. DNS Armor™ identifies and blocks unusual DNS traffic to disrupt communication with C2 servers, limiting the attack's effectiveness.

Data Exfiltration

Sensitive data is often stolen via covert DNS queries. DNS Armor™ monitors and blocks suspicious queries to prevent unauthorized data transfers, safeguarding confidential information.

DNS Fast Flux Detection

Fast flux networks rapidly change DNS records to hide malicious infrastructure behind constantly rotating IP addresses, making C2 servers and phishing sites difficult to block. DNS Armor™ employs advanced AI algorithms to detect fast flux patterns through rapid DNS resolution changes, TTL anomalies, and domain behavior analysis, effectively neutralizing this evasion technique.

Network Infiltration Detection

Advanced persistent threats (APTs) use DNS for covert network infiltration and lateral movement. DNS Armor™ leverages AI-powered behavioral analysis to identify reconnaissance activities, unusual domain query patterns, and anomalous DNS traffic indicative of network infiltration attempts, enabling early threat detection before attackers establish footholds.

Botnet Mitigation

Botnets use DNS to coordinate large-scale attacks like DDoS and spam campaigns. DNS Armor™ detects and blocks DNS queries from infected devices, disrupting botnet activity before escalation.

Domain Generation Algorithm (DGA) Attacks

DGAs generate large numbers of domain names for malware communication, making them hard to detect. DNS Armor™ leverages threat intelligence to identify and block DGA-generated domains, preventing malware from connecting to its control servers.

The First Line of Défense

DNS Armor™ provides proactive threat detection and network visibility, allowing Security Operations Centres (SOCs) to identify cyber threats early.

Enhanced Threat Visibility

DNS monitoring helps detect unusual domain requests and high DNS traffic, which may indicate C2 communication or an ongoing attack.

Integration with Security Tools

DNS Armor™ seamlessly integrates with monitoring tools, providing real-time alerts and tracking DNS record changes to detect security incidents early.

Scalability for Large Networks

DNS Armor™ efficiently manages millions of Indicators of Compromise (IoCs) without affecting performance, making it suitable for dynamic networks.

Reducing the Burden on Security Tools

By blocking threats at the DNS level, DNS Armor™ reduces the load on firewalls, intrusion detection systems (IDS), and endpoint protection solutions, improving overall cybersecurity efficiency.

Key Values to DESC:

- **Security:** Achieve a robust first line of defense with DNS Armor™, leveraging Threat Intellegence, AI& ML to block emerging and sophiticated DNS based threats and web filtering for all governmnet users and etities from anywhere.

- **Customisation:** A custom built private cloud (including control and data planes) giving DESC the ability to customise the platform operations, UI, plocies and much more to tailor fit current and future requirements.

- **Flexibility:** Ability to leverage different hybrid deployment models, direct forwarding, provision local DNS resolvers within the Dubai Governmnet entities and via endpoint agents.

- **Scalability:** Leverage the power of SaaS and the cloud from DESC's DCs. Provision new nodes/ local resolvers across new DC s, within entities or abroad on private/ public clouds. Expand the scope for Non-Government DNS traffic in the future if needed to apply DNS security, monitoring and web filtering.

- **Agility:** Gain visibility and analytics on users and devices generating legitimate and malicouis DNS hits leveraging the DNS Armor™'s flexible deployment models supported by a multi-tenant architecture to support a tenant per entity with RBA support.

- **Integrations:** Full native integration with the ecosystem, including TIP, datalake, SEIM and others.

- **Data Residency & Sovereignty:** DESC cloud is a private cloud platform fully segregated from Secure Domains' public cloud ensuring no data, meta data or log exchanges.

3.11. Appendix – Datasheet

4. Threat Intel Platform- Anomali

In today's rapidly evolving cyber threat landscape, organizations face immense challenges in transforming raw threat data into actionable intelligence. The Anomali ThreatStream platform, part of Anomali's comprehensive security suite, addresses these challenges by empowering organizations to operationalize threat intelligence, streamline their security operations, and stay ahead of adversaries.

Anomali is proud to submit our proposal to DESC to provide a threat intelligence platform capable of housing and maintaining up-to-date and relevant threat intelligence for threat hunters and mission partners. Our company was founded to solve the specific cyber challenges that you are addressing with this effort. We have a deep heritage in threat intelligence, big data, and analytics. We have worked with our customers through the years to solve complex problems specifically related to cyber intelligence.

Anomali Threat Platform is an advanced threat intelligence platform that will significantly improve the efficacy and efficiency of DESC cyber security operations. By automating many manual and error-prone cyber security related tasks, security professionals will have unprecedented and near real time insight into malicious cyber activity and be able to take timely action to protect the business and its employees from harm.

The Anomali platform uniquely addresses DESC requirements with a consolidated cyber threat database for use by DESC teams to aggregate, analyze, and operationalize IOCs and other threat and vulnerability data. Furthermore, our native integrations with SIEMs/Data Lakes will substantially unlock additional value from your existing investments. We are excited to work closely with your team during the implementation of a Threat Intelligence Platform to meet the business and technical use cases to ensure we meet – and exceed – your requirements.

Key Challenges and Solutions

1. **Transforming Raw Data into Actionable Intelligence**
   Threat intelligence often consists of massive, redundant data streams from multiple sources. Anomali ThreatStream consolidates, deduplicates, and enriches this data, offering a unified view of threat indicators (IoCs) and threat models. This process enables faster and more accurate decision-making, allowing teams to focus on high-priority threats.
2. **Ensuring Contextual Relevance**
   Not all threats are equally significant to every organization. ThreatStream applies scoring and confidence levels to identify threats most relevant to a company's industry, geography, and existing vulnerabilities. By tailoring intelligence to specific contexts, organizations can prioritize resources and respond to the most significant risks effectively.
3. **Providing Real-Time Threat Intelligence**
   Cyber threats evolve rapidly, and delayed responses can lead to significant damage. ThreatStream ensures real-time ingestion and processing of threat data, providing up-to-the-minute insights that enhance situational awareness and reduce the window of exposure.
4. **Effective Dissemination Across Security Infrastructure**
   Distributing the right intelligence to the right tools is critical. ThreatStream integrates seamlessly with SIEMs, firewalls, endpoint solutions, and other security controls. It automates data sharing and ensures that actionable insights reach the appropriate systems without manual intervention, accelerating responses and minimizing errors.
5. **Fostering Collaboration and Sharing**
   Cyber threats often affect entire sectors or industries. Anomali's Trusted Circles feature enables secure and efficient sharing of threat intelligence among industry peers, government bodies, and partner organizations. This collaborative approach strengthens defenses across the broader cybersecurity ecosystem.

Advanced Capabilities

Anomali's platform extends beyond ThreatStream with cutting-edge tools such as:

- **Anomali Copilot**: Powered by machine learning and natural language processing, Copilot correlates historical and live data to predict and mitigate emerging threats proactively. It identifies patterns beyond known attack signatures, enhancing threat detection and prevention.
- **Anomali Security Analytics**: This next-generation SIEM integrates threat intelligence with internal telemetry to provide actionable insights, helping organizations anticipate and neutralize attacks before they materialize.

Business Benefits

By operationalizing threat intelligence with Anomali, organizations can:

- Reduce manual workload and streamline security operations.
- Improve the speed and accuracy of threat detection and response.
- Enhance their overall security posture through proactive measures.
- Strengthen collaboration and information sharing within their industry.

Why Choose Anomali?
With over 200 integrations and curated access to the world's largest threat intelligence repository, Anomali delivers unmatched scalability, speed, and precision. Its innovative solutions empower security teams to transition from reactive to proactive strategies, enabling them to combat today's threats while preparing for the future.
Anomali offers a unique blend of simplicity, power, and advanced analytics, making it the ideal partner for organizations aiming to modernize their cybersecurity operations.

The Anomali platform was purpose-built to harness threat data, information, and intelligence to drive effective cyber security decisions. It is a platform that automates detection, prioritization, and analysis of the most serious threats to DESC. With machine learning, automation, and an expansive partner ecosystem, Anomali empowers DESC to leverage threat intelligence for better insights and response to cyber-attacks – while integrating with the existing systems and workflows of your teams.
Anomali helps organizations:

- Identify targeted threats to the organization
- Automate detection and analysis of threats
- Improve response with insights into threat actors and behaviors
- Save time and resources by reducing impact of attacks
- Allow for collaboration between the DESC technologies and teams.

Anomali ThreatStream is the Threat Intelligence Platform built for analysts to create threat intelligence and investigate security incidents. With ThreatStream they can collect, contextualize, and risk/rank complex, high-volume indicators with machine learning to prioritize alerts and guide security strategy. ThreatStream can:

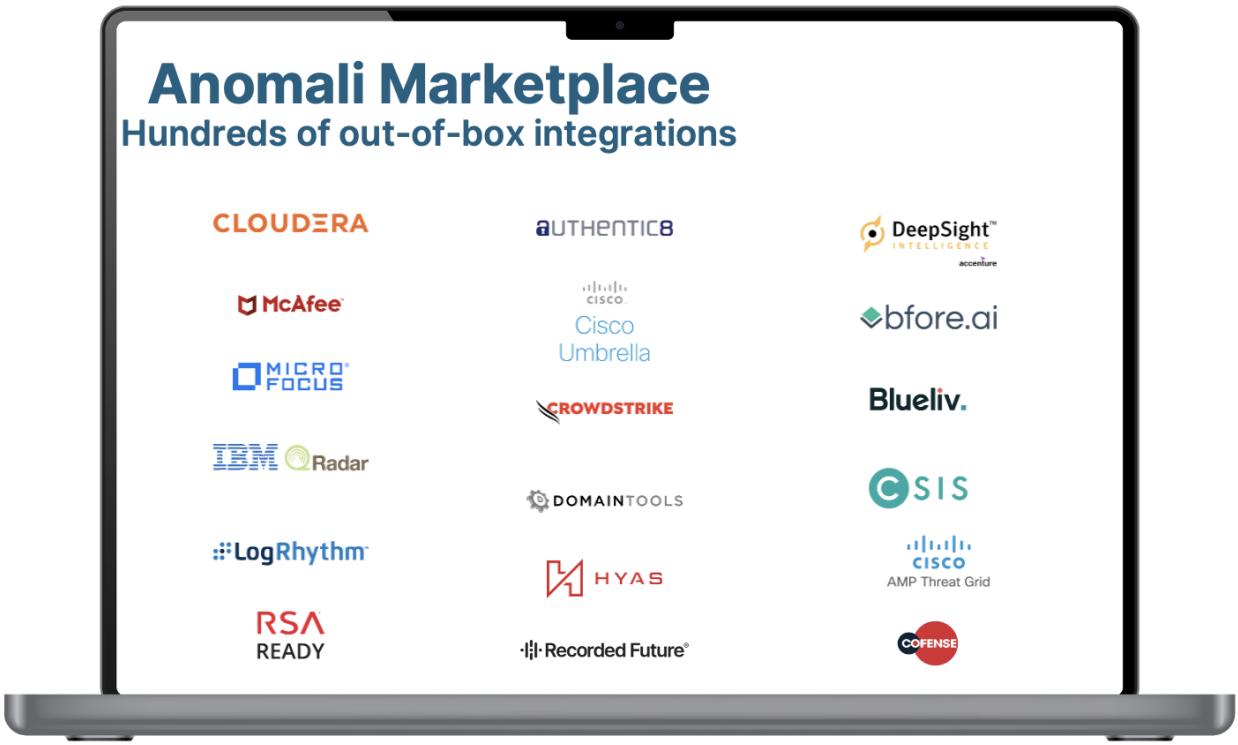
- Map threat intelligence to threat models (Actor Profiles, Campaigns, and TTPs)
- Aggregate OSINT, 3rd party premium feeds, Anomali Labs Research, and ISAC data (e.g. DHS AIS, CISCP, and more)
- Automate workflows for quicker analyst insights
- Securely share and collaborate threat intelligence with trusted partners
- Integrate with SIEMs, Data Lakes (LogRhythm, Splunk, Elastic, Devo, etc.), Firewall, Endpoint, Proxy, IDS, API, Orchestration Tools, Ticketing Systems, and more

Anomali Integrator: Will provide SOAR like capabilities with native integrations into DESC technologies. Integrator is truly an automation engine that takes threat intelligence collected by DESC and makes it actionable in already existing investments.

Dedicated Customer Success Manager – One of the advantages of choosing Anomali as your business partner and Threat Intelligence platform is our team of subject matter experts. Your dedicated CSM will schedule bi-weekly cadence calls with the DESC team to assist with implementation, tuning, training, enabling new features, and ultimately furthering the adoption of our platform, creating efficiencies for your team, and focusing on continuous improvement to your overall CTI program.

Thank you for the opportunity to compete for your business and work with your team. We are looking forward to taking the next steps with the DESC team in the coming weeks to ensure the success of this vital program.

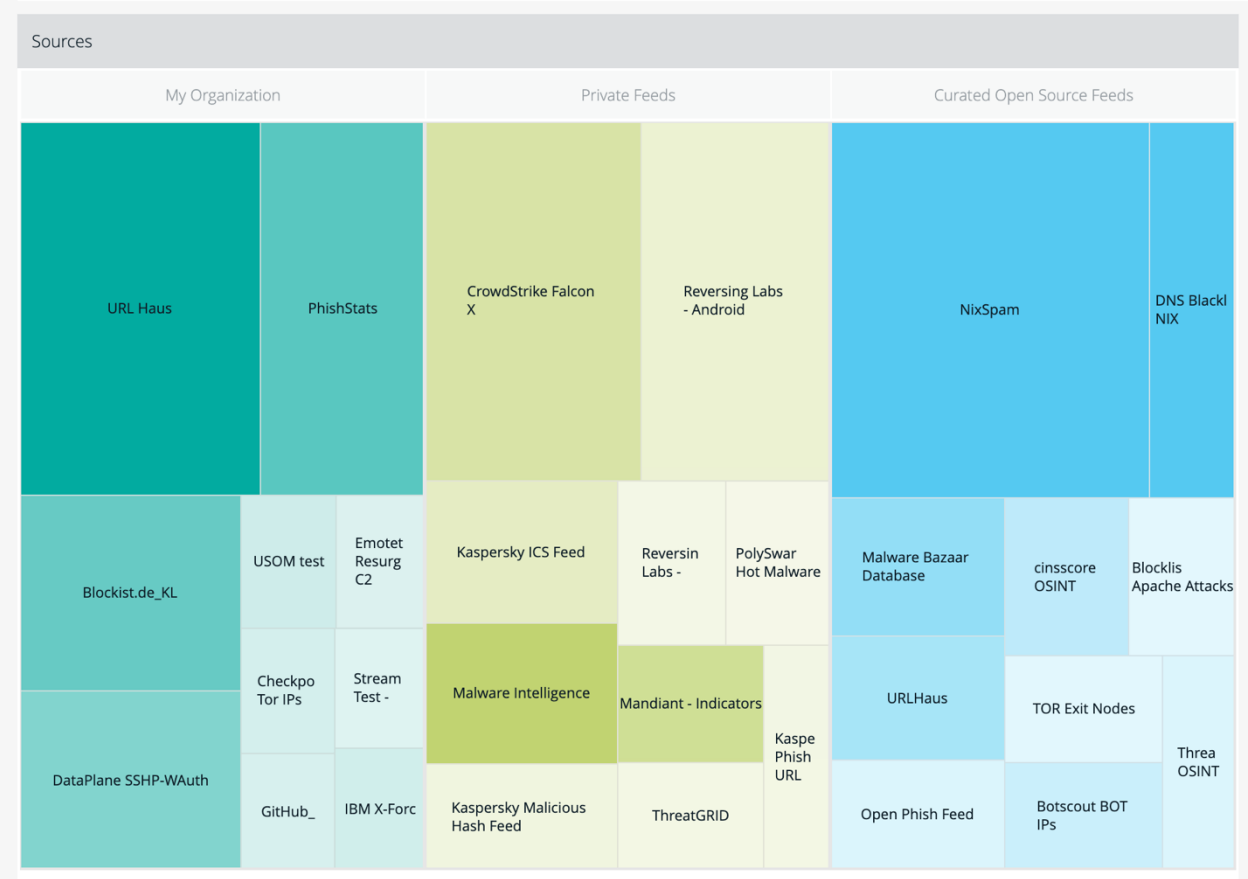
Anomali ThreatStream provides a significant advantage over standalone **Threat Intelligence Feeds** by delivering a centralized, comprehensive, and highly efficient framework for managing and operationalizing threat data. While feeds supply essential threat information, Anomali ThreatStream consolidates intelligence from multiple sources into a unified platform, streamlining workflows and enabling organizations to address threats with greater agility and effectiveness.
A key benefit of Anomali ThreatStream is its ability to enrich and correlate data from multiple sources, providing a broader context to threat indicators. By connecting data points to relevant threat actor profiles, tactics, techniques, and procedures (TTPs), the platform enables security teams to assess threats in a more comprehensive manner. This facilitates better prioritization of responses and ensures that critical risks are addressed promptly, ultimately reducing the time and resources required to manage threats effectively.



Integration capabilities further underscore the value of Anomali ThreatStream. The platform seamlessly integrates with an organization's existing security tools, including SIEMs, SOAR platforms, firewalls, and endpoint protection systems. By automating processes such as data ingestion, alert triage, and incident response, Anomali ThreatStream reduces operational overhead, minimizes the likelihood of human error, and enables security teams to focus on strategic initiatives. This automation leads to measurable cost savings by optimizing the use of human and technical resources.

The ROI of **Anomali ThreatStream** becomes evident when compared to standalone feed providers. Feed providers often deliver valuable threat data but require additional tools and manual effort to aggregate, analyze, and operationalize the information effectively. In contrast, Anomali ThreatStream reduces these inefficiencies by centralizing and enriching the data, improving accuracy, and streamlining threat management. This results in a higher utilization of purchased threat intelligence feeds and reduces wasted spending on unused or underutilized data.
Additionally, Anomali ThreatStream excels in standardizing and correlating data from diverse sources, ensuring consistency and uncovering relationships between seemingly isolated threat indicators. This enhanced situational awareness helps organizations identify emerging trends and proactively address potential risks. The platform also includes advanced threat scoring and

prioritization mechanisms, enabling security teams to focus on the most critical issues, further improving operational efficiency and maximizing the return on security investments.



Collaboration and information sharing are core features of Anomali ThreatStream. The platform facilitates secure intelligence sharing within organizations and across external partnerships, promoting a collective defense approach. Furthermore, it offers sophisticated reporting and visualization tools that allow stakeholders to track key metrics, such as threat trends, response times, and overall effectiveness. These insights enable organizations to demonstrate the value of their threat intelligence programs to key stakeholders, further highlighting the ROI of the platform.

Automation and scalability are integral to Anomali ThreatStream. By automating key workflows, the platform improves efficiency and ensures that organizations can scale their threat intelligence operations to meet the demands of an evolving cybersecurity landscape. This scalability ensures that investments in the platform continue to yield dividends as organizational needs grow.

In summary, Anomali ThreatStream not only enhances the utility of threat intelligence by centralizing, enriching, and operationalizing data but also delivers clear financial and operational benefits. By optimizing resource utilization, improving threat visibility, and reducing response times, Anomali ThreatStream provides a compelling return on investment compared to standalone feed providers. For organizations seeking to strengthen their cybersecurity posture and streamline their threat management processes, Anomali ThreatStream represents a highly strategic and effective solution.

4.1. Anomali Proposed Portfolio

Anomali AI Security Platform has a comprehensive capabilities and offerings including ThreatStream TIP, Security Analytics, IT Ops, Enterprise Observability and others

The included set of products in proposed solution as following:

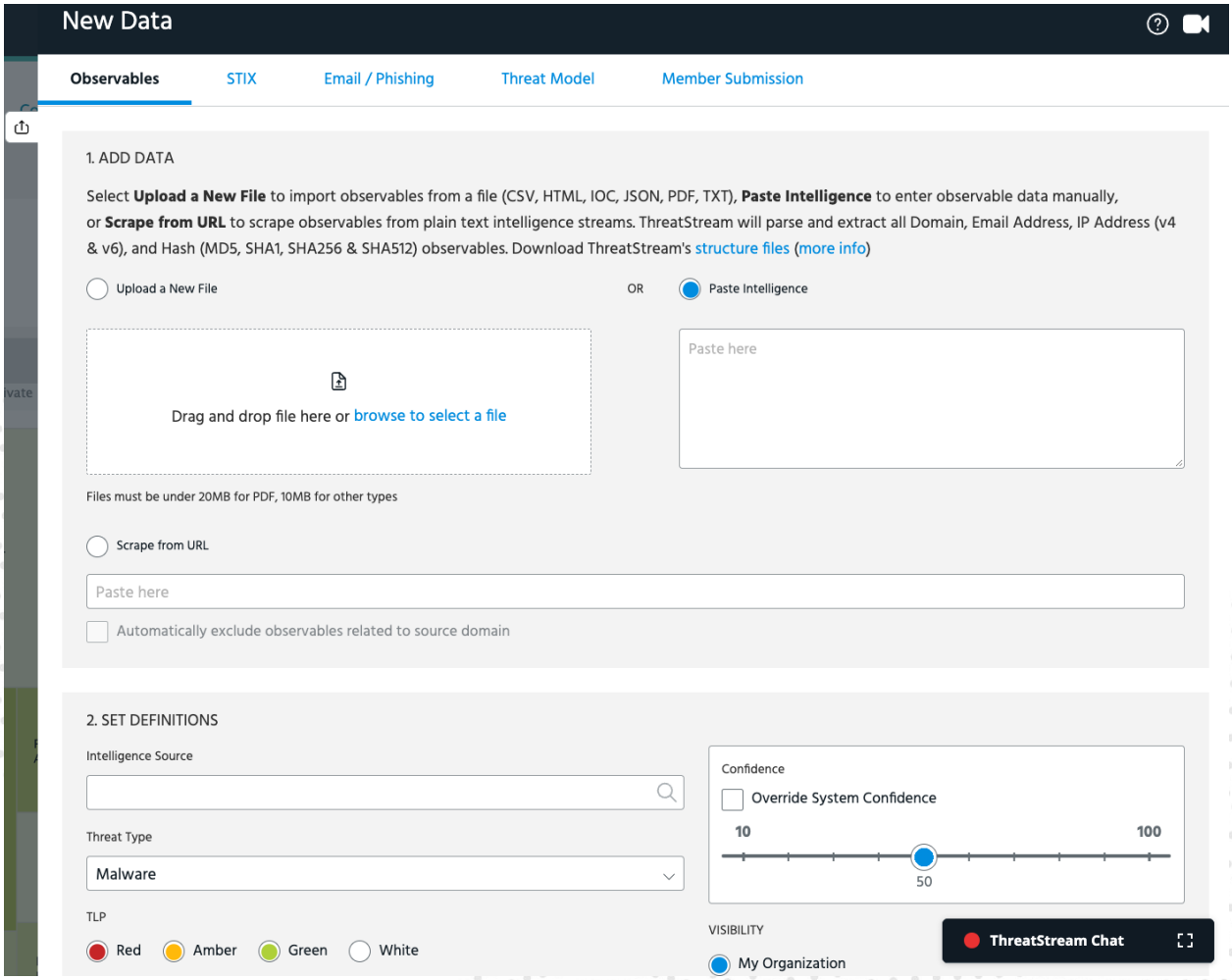
4.2. ThreatStream TIP

Anomali ThreatStream is a Threat Intelligence Management solution that unifies threat data and information into high-fidelity intelligence, automatically disseminates it to security controls, and integrates a suite of research tools to support efficient threat investigations. ThreatStream automates the collection of threat intelligence data from hundreds of external and internal sources, including open source threat intelligence; commercial threat feeds; shared intelligence; and internal intelligence from investigations, sandbox detonations, etc. The product normalizes and deduplicates these feeds into a common taxonomy, leveraging machine learning algorithms to remove false positives, enrich the data, and risk-score the intelligence for severity and confidence. ThreatStream then operationalizes the intelligence via automated distribution of machine-readable threat indicators to security controls (e.g., SIEM, firewall, EDR, IPS, SOAR, etc.). The product also provides tools for analysts and SOC teams to do model-based investigations using the Diamond, Kill Chain, STIX, or MITRE ATT&CK frameworks. The
investigations workbench includes a comprehensive set of data enrichment sources; a powerful visual Explorer tool for indicator expansion and pivoting; integrated sandbox detonation for malware and phishing URLs; and threat bulletin collaboration, authoring, and publication.

4.2.1. Threat Intelligence Ingestion

Anomali ThreatStream provides a core capability to receive information and intelligence from as many source types as possible including:

- Anomali's APP store, which provides fully integrated feeds from all major commercial feed providers with a *'click to subscribe'* ease of use model.
- OSINT sources - over 100 are configured out-of-the-box.
- Streams, which are user configured HTTP/S scrapers for the ingestion of threat data from custom sources such as Twitter and other social media.
- Public Trusted Circles, which include threat sharing communities such as ISACs.
- TAXII servers, which allow bi-directional threat intelligence sharing via a STIX/TAXII.
- Sandbox - ThreatStream offers multiple sandbox configurations you can leverage for Malware detonation
- MISP - Anomali offers bi-directional integration with this source of intelligence.
- User imports via the web browser user interface, the API or Anomali Copilot, see the figure below.
- Anomali Copilot, which is a web browser plug-in allowing users to scan and identify threat data in any web-based content in seconds.

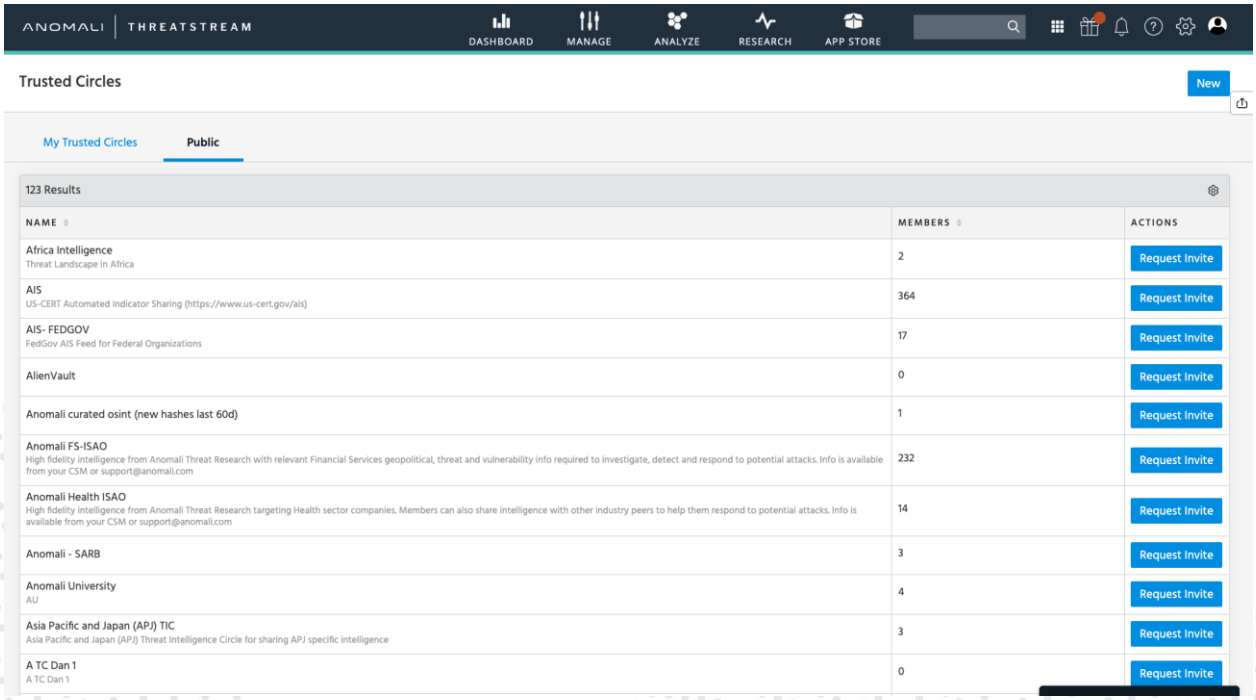


Anomali Manual Threat Intelligence Ingestion

4.2.2. Trusted Circles

Anomali ThreatStream's Trusted Circles are communities within ThreatStream in which you can participate, share threat intelligence in real-time, and get access to information others have shared. Trusted Circles are made up of organizations with similar threat intelligence interests (due to their affiliation to an industry, supply chain, Incident, and so on) and enable these organizations to collaborate and discuss threat activities they have observed around a specific campaign, adversary, or Incident. In addition to organizations that participate in Trusted Circles, the Anomali Threat Research team contributes and shares intelligence to the industry-specific Trusted Circles available on ThreatStream. There are two types of Trusted Circles, public and non-public.

- Public—The names of these Trusted Circles are visible to all organizations. Any organization can request an invite to these circles. The request must be approved by the Trusted Circle owner before an organization can join that circle. The Public Trusted Circles are listed in the “Public” Trusted Circles table, as shown in the figure below.
- Non-Public—The names of these Trusted Circles are not visible to all organizations but only to the members of the organization that created the circle and any other organizations that may have been explicitly invited to join them. If your organization participates in any of such circles, they are listed in the “My Trusted Circles” table.



Anomali Trusted Circles

4.2.3. Dashboards

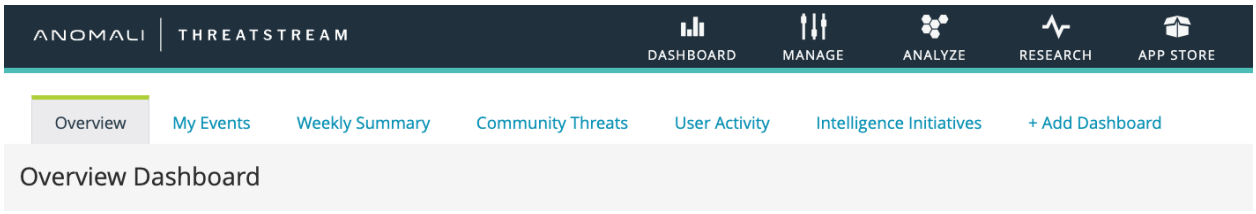
ThreatStream enables your organization to surface Threat Intelligence data of interest and customize your landing page experience through the creation of custom dashboards. Each dashboard can contain up to 20 customizable widgets. Widgets display Threat Intelligence data on chart types of your choosing based on saved observable or Threat Model search filters. You can drill into data sets on the observables or Threat Model search screen by clicking any of the data visualizations, such as a section of a pie chart, a line on a sparkline chart, a number chart, and so on.

There is no limit on the total number of custom dashboards an individual ThreatStream user can create. However, at most 10 custom dashboards can be shown on their home screen at any time. There is no limit on the total number of dashboards across all users in an organization.

By default the dashboards in the below picture are enabled for all users, here is a description of each one:

- **Overview**: Get a real-time overview of observables relevant to your organization and view alerts that require your immediate action.
- **MyEvents Map**: Visualize the geographic location of threats around the world.
- **Weekly Summary**: Visualize the quality of data coming through the various feeds supplying your organization with intelligence.
- **Community Threats**: View the most **Watched**, **Starred**, **Liked**, and **Commented** observables and Threat Model entities in your community over the previous 30 days.
- **User Activity:** Generate reports on user activity within your organization.
- **Intelligence Initiatives:** Gain a high level view of open intelligence initiatives created by your organization.

- **+ Add Dashboard:** Add a custom dashboard to your home screen.

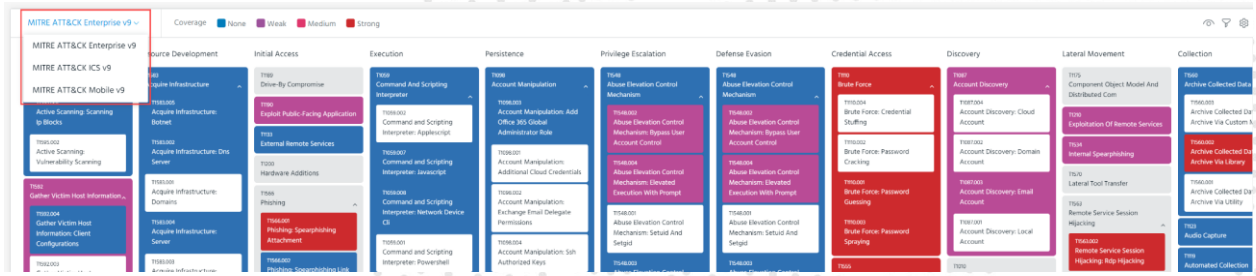


4.2.4. MITRE ATT&CK

The ThreatStream investigations workspace includes an on-board implementation of the MITRE ATT&CK Framework, which enables you to build visual representations of MITRE ATT&CK associations and insights into the impact of the threat under investigation with regard to the MITRE ATT&CK Framework. ThreatStream also enables you to use the MITRE ATT&CK to log the security coverage implemented by your organization. After configuring your security coverage, you can overlay it on MITRE ATT&CK models within investigations to get a snapshot of your coverage for a particular threat.

Depending on the MITRE ATT&CK version, you can also choose one of the following MITRE ATT&CK Framework types:

- **Enterprise**: Shows a comprehensive matrix of tactics and techniques applied against enterprise infrastructures. Available for all supported MITRE ATT&CK versions.
- **Mobile**: Shows a comprehensive matrix of techniques involving Android and iOS devices access and network-based effects that can be used by attackers without device access. Available for MITRE ATT&CK v7.X and above.
- **ICS**: Shows how attackers achieve a tactical goal by performing an action. Available for MITRE ATT&CK v8.X and above.



Anomali MITRE ATT&CK Overview

4.2.5. Rules and Tagging

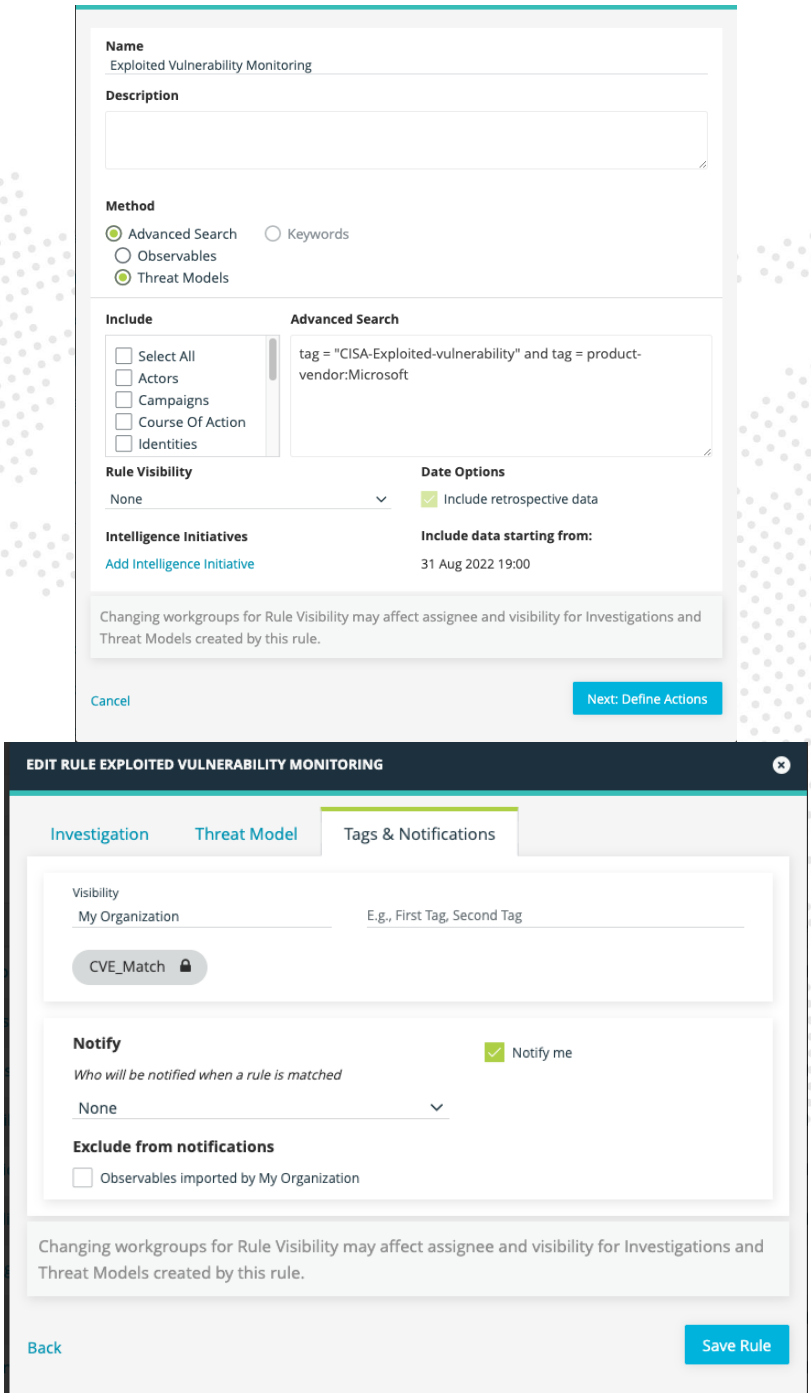
ThreatStream provides a Rules engine to provide automated action upon the ingestion of identified Threat Intelligence. Rules can be defined to search for specific keywords, REGEX or the same Boolean logic utilized within our Advanced Intelligence searching functionality.

This gives users the ease of converting any search they've used to identify desired intelligence into a Rule to take action whenever similar intelligence is added to the platform.

Rule actions let users automate these functions automatically as matching intelligence is added to their environment:

- Add additional intelligence to a new or existing Investigation

- Update Existing Threat Models (i.e. Actor Profiles, Campaigns, Threat Bulletins) with additional Intelligence Associations
- Provide User Notification (within console or via E-mail)
- Apply customized Tagging

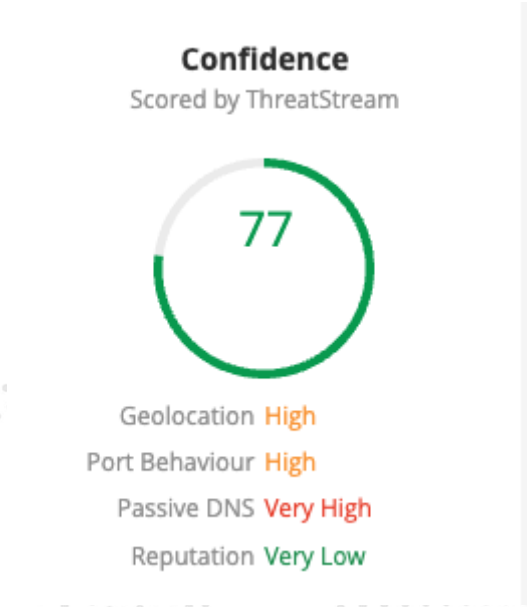


Tagging allows ThreatStream users to add customized information to threat intelligence without the burden of creating private clones of the Observables or Threat Models themselves. Tags can convey free-form information users wish to associate with threat intelligence and become another mechanism to assist in sorting and identifying pertinent information for any given scenario. By incorporating Tag application to Rules, ThreatStream allows users to highly automate this functionality.

Additionally, ThreatStream provides users the ability to define an extensive list of “Preferred Tags” as a system-wide function to ensure that organizations leverage a consistent taxonomy.

4.2.6. Macula Scoring

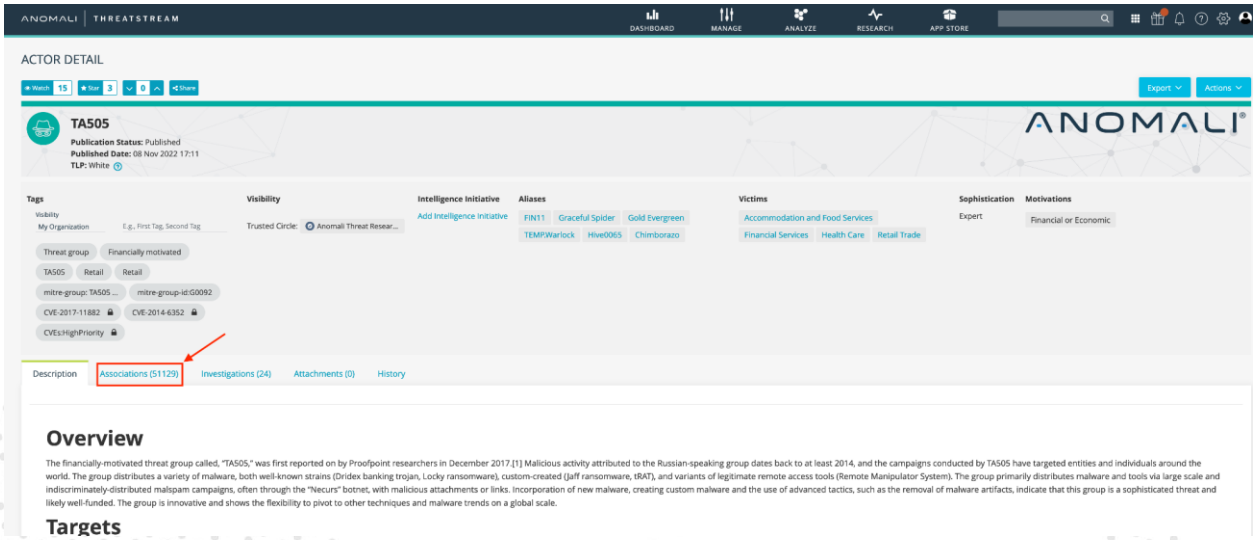
Anomali employs a machine learning algorithm to deduplicate, reduce false positives and assign or adjust Confidence ratings on Observables as they are imported into clients’ IOC databases. We have named this platform Macula. Macula reviews factors such as Geolocation, Port Behavior, Passive DNS information and Reputational analysis (i.e. number/reputation of reporting sources) to more accurately define a confidence value for indicators and allow users to make more intelligent decisions on which are valid and of greatest concern.



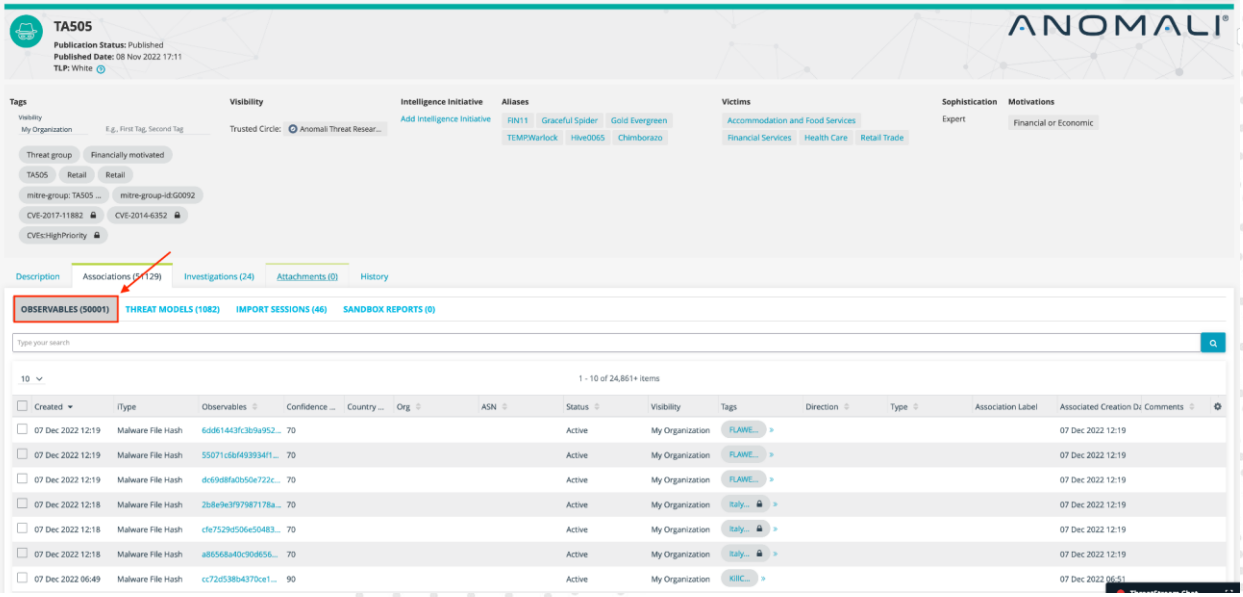
4.2.7. Intelligence Correlation

Anomali ThreatStream allows for the automatic association between indicators of compromise and Threat Models within the platform. This is presented in the “Associations” tab on the Threat Model Detail page. In addition to bidirectional associations between observables and threat model entities, ThreatStream enables you to associate observables with other related observables. Associations appear in the Associations table on observable details pages.

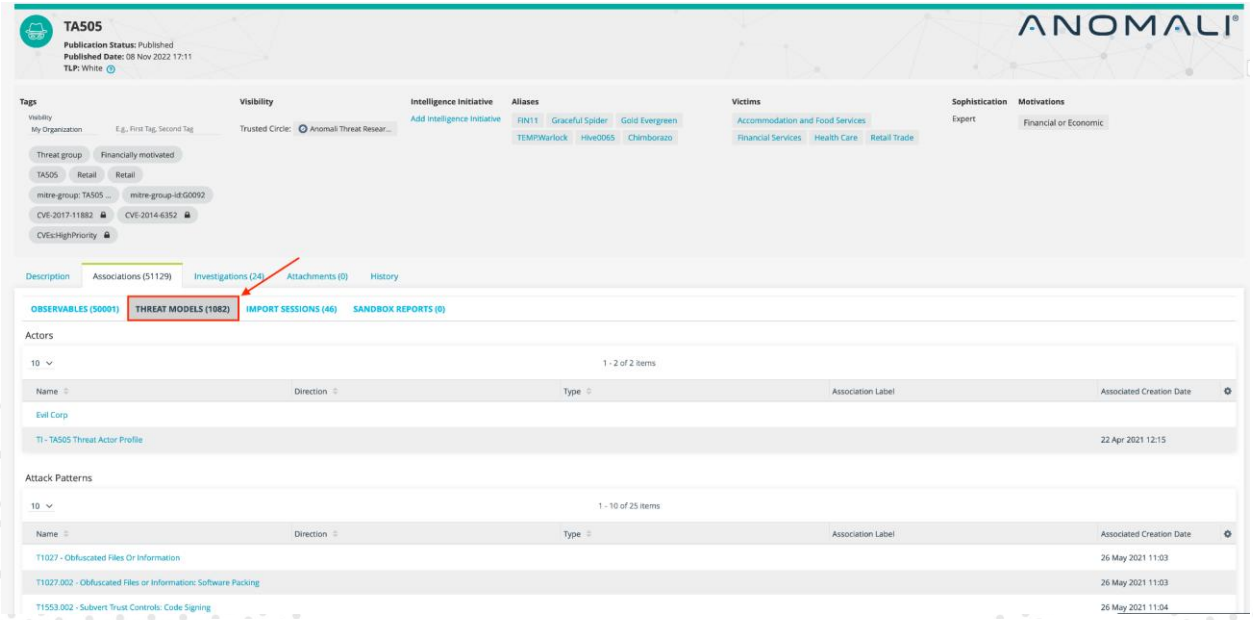
This allows for quicker time to research since there is the ability to intelligently pivot from an IOC to a Threat Model, Threat Model to an IOC, or an IOC to an IOC. All new and existing intelligence is automatically associated as it is ingested if there is a relationship between the entities.



Associations tab present in Actor Detail Threat Model



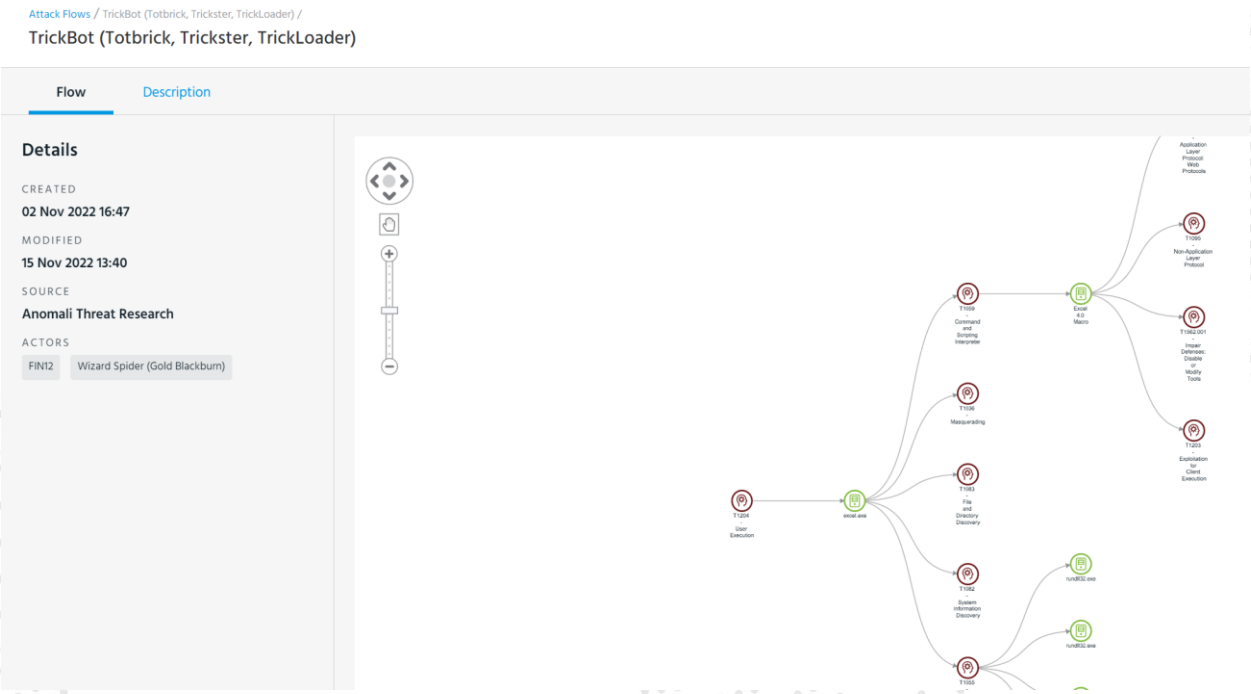
Pivoting from an Actor Detail Threat Model to associated IOCs



Pivoting from Actor Profile Threat Model to other Threat Models

4.2.8. Attack Flows

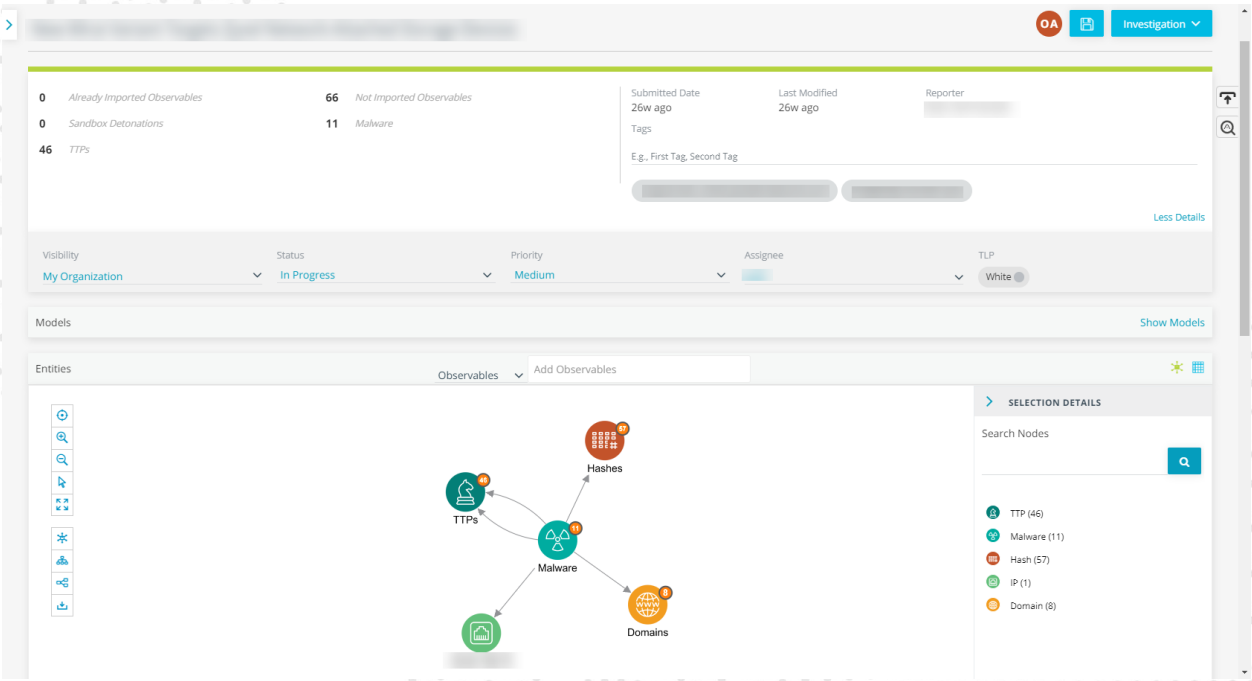
The Attack Flow library in ThreatStream is a collection of common MITRE Attack Flows (MAF), which provide a way to fingerprint attacks. The Attack Flows enable users to visualize the sequence of techniques used in an attack, the relationships between techniques, and other information that can be extremely valuable to cybersecurity practitioners. By identifying the presence of an actor, a campaign, or malware at an early stage of an attack flow, practitioners can stop or prevent further attacks on DESC environments.



Sample Attack Flow of TrickBot

4.2.9. Investigations

Investigations is a collaborative and flexible workspace that you can use to perform daily tasks. After creating an investigation, users can centralize threat data as it becomes available and perform pivoting to understand linkages. Investigation tasks can also be tracked and assigned to organization users. After completing research, you can create new intelligence in the form of threat model entities or newly imported observables. Additionally, an integration with ServiceNow enables you to push investigation information to Security Incident Tracking systems.



Within an investigation, you can leverage the ThreatStream Explore tool to make connections between the entities you are researching and other data, both internal and external to ThreatStream. Using the Explore tool, you may discover external data of interest that is not yet imported to ThreatStream. From the investigation DESC will be able to initiate an import session for all not-yet imported observables, thus adding them to your threat intelligence on ThreatStream.

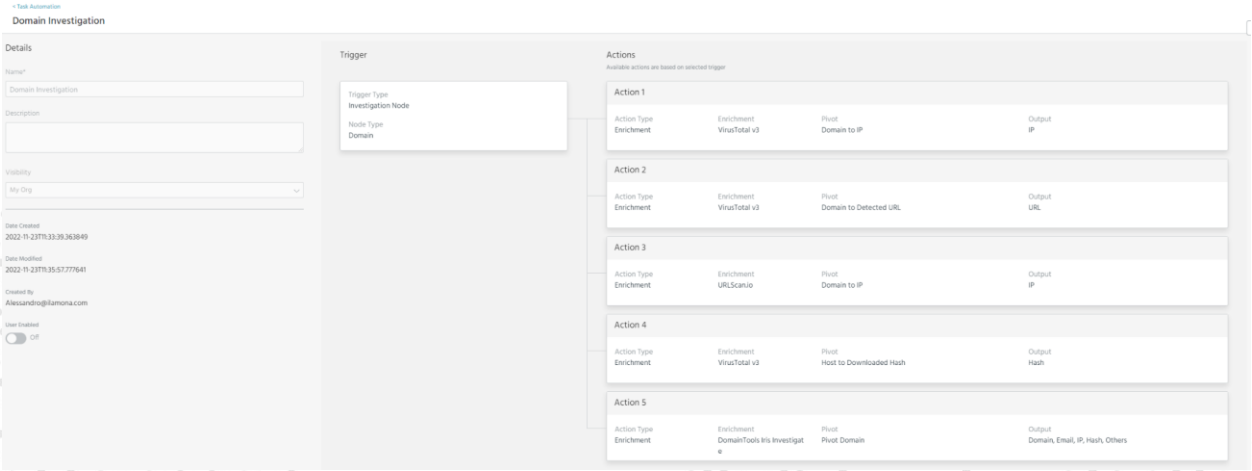
4.2.10. Task Automation

In ThreatStream, DESC will be able to automate investigation tasks. When users need to run several checks on an observable they can use an automated task - a predefined sequence of enrichments applied to a specific type of the observable during the investigation.

Automated task can be run on the following types of nodes

- Domain
- Email
- IP
- Hash
- URL

Automated tasks can be created by anyone from your organization. You can create your own custom automated tasks. You can delete your automated tasks except those that are active and being used by others in your organization.



Sample Domain Investigation Automated Task

4.2.11. Threat Models

The Anomali Threat Model is STIX (v1.2, v2.0, and v2.1) compatible and supports adding, managing, importing, and exporting contextual, relationship, and workflow information for these types of Threat Model entities: Actors, Attack Patterns, Campaigns, Courses of Action Custom Objects, Identites, Incidents, Infrastructure, Intrusion Sets, Malware, Signatures, Tools, Threat Bulletins, Tools, TTPS, and Vulnerabilities.

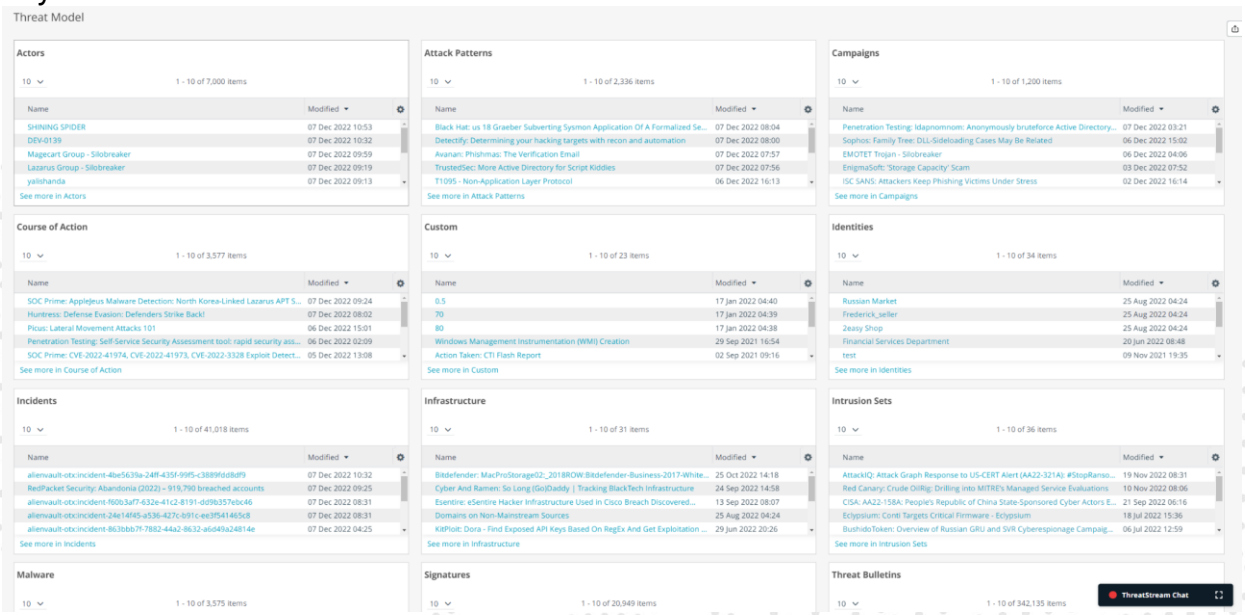
Although the Threat Model is pre-populated with a large set of information, you can add additional Actors, Campaigns, Incidents, TTPs, and Signatures through the ThreatStream UI or import this information. Observables can be imported using Import Assistant. You can also export the Threat Model information from ThreatStream.

Maintaining relationships across Threat Model entities provides additional context around threats and will allow DESC for a deeper analysis of observables rather than viewing atomic observables. The rich contextual data and relationship information can be useful in making better policy decisions for SIEM and other security automation use cases for DESC infrastructure.

The Anomali Threat Model provides bidirectional associations between entities of all threat model types, including entities of the same threat model type. Therefore, the UI always displays a bidirectional relationship between two entities. For example, if an Actor is shown to be related to a Campaign then that Campaign is also shown as related to the Actor. Bidirectional associations can also be created between Threat Model entities and Observables, Threat Bulletins, and Vulnerabilities. Threat model entities of all types can also be associated with Sandbox Reports, though these associations are unidirectional and not displayed on the Sandbox Report details page. Additionally, you can add labels to Threat Model and observables to track contextual information.

4.2.12. Threat Model Dashboard

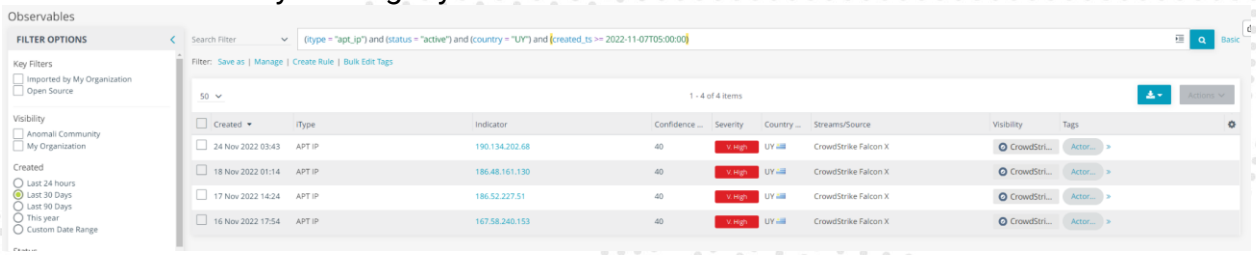
The Threat Model dashboard displays the five most recent Threat Model entities of each type that were updated on ThreatStream. If DESC analysts would like to dig deeper into a specific entity or view the entire list they can easily dive into the additional information by clicking on any Model.



ThreatStream ThreatModel Dashboard

Advanced Threat Model Searches
Anomali ThreatStream provides advanced Threat Model search functionality for cases involving specialized searches. This provides a simple and easy to use boolean search operation for Analyst to quickly and easily identify specific threat models they are researching.

As seen in the below image we are able to quickly and easily identify IP's associated with APT's in the Country of Uruguay.



Advanced Search Query Capabilities

4.2.13. Administration

Users who DESC identifies as Administrators will be given the permission of Org Admin. Users with Org Admin privileges in ThreatStream can configure vital organization settings. If you have Org Admin status, you can add and edit organization users, configure multi-factor authentication, update your organization exclude list, and set alerts for your organization, among other tasks.

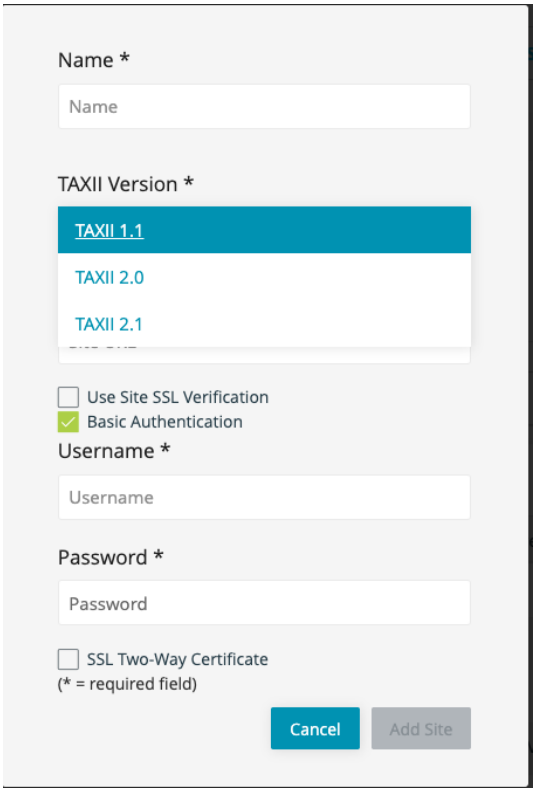
The following are the key capabilities that Administrators will have the access to do.

- Viewing and Editing Organization Settings
- Mailbox Configuration for Receiving Observables
- Multi-Factor Authentication
- Managing Organization Users
- Customizing New User Emails
- Configuring Single Sign On (SSO)
- Updating the Organization Exclude List
- Configure and setup Integrations with Third-Party Services
- Audit User Activity
- Share intelligence via TAXII Services
- Manage User Workgroups
- Manage DESC Preferred Tags
- Manage Description Templates
- Manage DESC Never Scan Lists for the Copilot Plugin
- Manage all user privileges

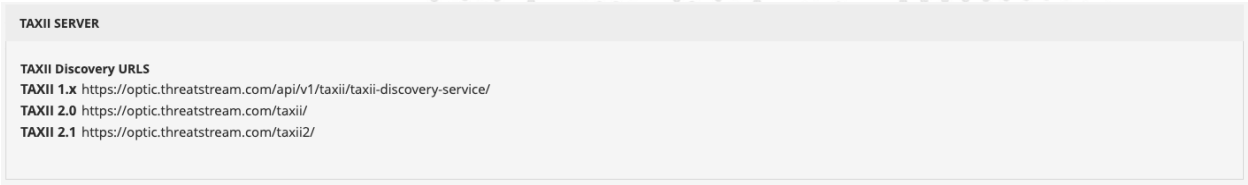
4.2.14. TAXII

Anomali ThreatStream provides users with both TAXII Client and Server functionalities, giving users robust access to industry standard Intelligence sharing functionality.

As a TAXII client, ThreatStream can be configured to poll TAXII enabled intelligence sources to aggregate intelligence data in a single location. Leveraging the ThreatStream UI, users can define the discovery URL of their provider and provide their authentication information then select any feeds to which they are entitled to, define a polling frequency and specify their own custom Feed Name to easily identify the source of their intelligence as it is ingested.

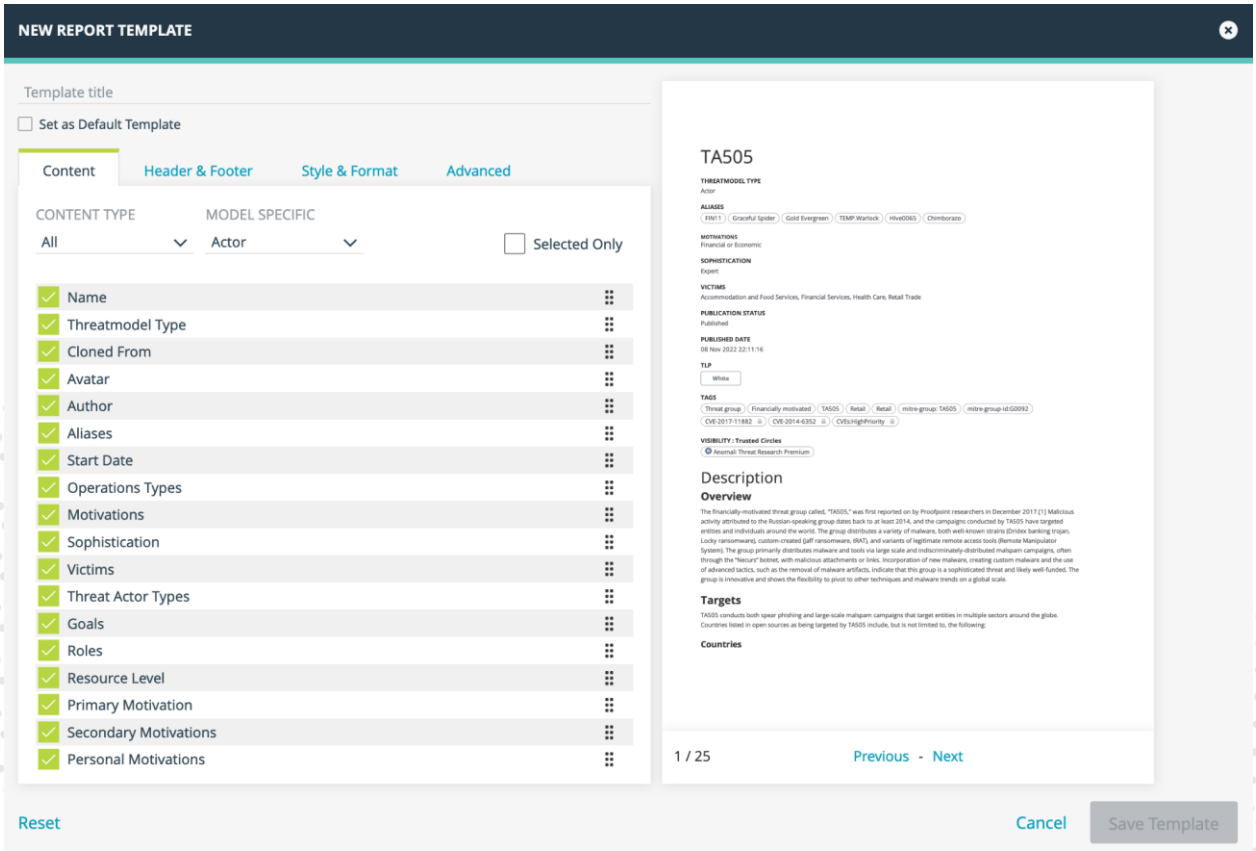


Additionally, ThreatStream can act as a TAXII server, again supporting versions 1.x, 2.0 and 2.1 and allow clients to define any Saved Search as a pollable repository. Leveraging this, clients can define multiple search filters, specifying the relevant intelligence for any given scenario and create a quick and easy export functionality to any TAXII enabled platform.



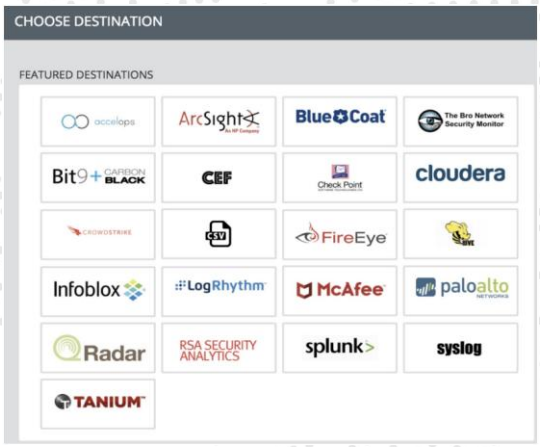
4.2.15. Reporting

PDF Report exports enable you to generate PDFs based on customizable templates for sharing with a wider audience outside of ThreatStream. PDF Reports are generated using templates, which can be customized to include specific fields, headers, footers, company logos, and text styles. This allows for users to create reports of all levels and retain the templates to be used again and again. Users have the ability to include specific data within the report, which means that an organization can have a template with all of the deep technically detailed data to disseminate to other members of their team, or high level summary reports to send to upper management. These details can include associated IOCs and Threat Models, comments, tasks, etc.



4.3. Integrator

Anomali Integrator acts as an integration layer between the ThreatStream Platform and the downstream systems that consume intelligence from the platform, such as SIEMS, endpoint protection systems, web proxies, and next-generation firewalls. Hence, the data conveyed by integrator are primarily atomic IOCs.



Integrator UI with destination selection screen

Integrator performs scheduled queries to the ThreatStream API to periodically receive new intelligence from the platform. A single instance can apply a filter condition to selectively pull the subset of intelligence relevant to the use cases, and then push those indicators to one or more configured destinations, using the API or transport and format appropriate to that destination. Filter conditions can be applied on a per-destination basis, such as sending network-relevant intelligence to a SIEM, while sending file-relevant intelligence to an endpoint protection system.

4.4. Anomali University

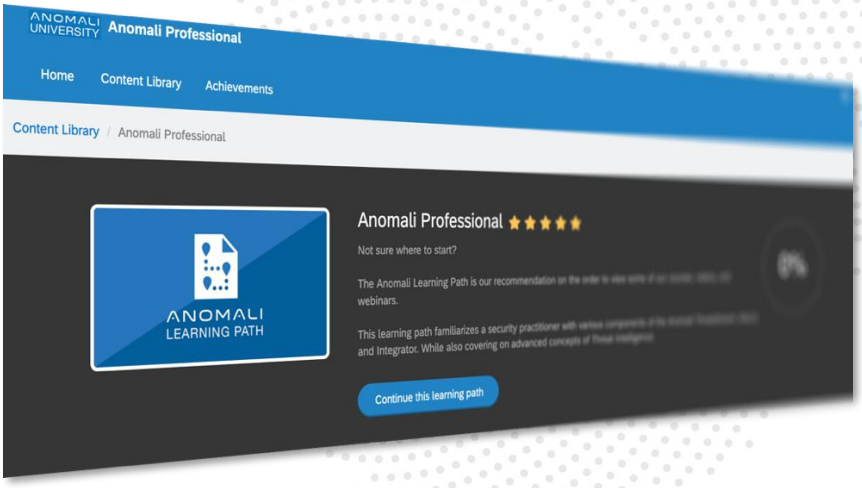
Anomali University (AU) is a service that offers courses designed by threat intelligence experts. Our courses cover an array of topics ranging from foundational information security concepts to advanced threat intelligence theories and their relevant applications. In addition, Anomali offers focused courses associated with how to most efficiently and effectively leverage our solutions. o

These are in-depth courses that walk you through all of the features and functionality in the platform. These courses have been designed to accommodate all types of learners. You control the pace of each module and can complete the training on your own schedule. These courses boast a range of interactive activities, including demos, knowledge checks, and exercises for you to practice what you have just learned. Simple enough for beginners, and powerful enough for experts.

ANOMALI VERIFIED ✓

Do you hold an industry certification that requires renewal (CEU/CPE) credits to keep the credential up to date? Do you want to prove that you understand how to use the tools that you learned about in this lesson? You should sign up for the **Anomali Verified ✓** program for eligible courses.

While Anomali provides access to our product training content via Anomali University, we also recognize that some customers want to go to the next level and show their understanding of the course content to certification providers, employers, and peers in the cyber-security field. We've designed **Anomali Verified ✓** to test the knowledge that you have gained in this course through a comprehensive assessment and meet the documentation requirements of the major cyber-security certification organizations.



4.5. Anomali Ecosystem

ThreatStream CTI Integration Partners

Anomali is partnered with the great majority of Cyber Threat Intelligence vendors and subscription services providing Threat Intelligence. ThreatStream customers can enable access to existing subscription content through the ThreatStream platform (APP Store), or customers can opt to trial and evaluate our partners through ThreatStream to ascertain the added value of subscribing to them.

Anomali APP Store

The Anomali Preferred Partner (APP) Store is the only platform-integrated marketplace for threat intelligence, enrichments and integrations.

Anomali Threat Platform clients can easily trial and manage threat intelligence feeds and enrichments from APP Store partners. Find the right intelligence for your organization, industry, geography, threat type, and more.

Security Integration Partners

ThreatStream integrates seamlessly with many Security and IT systems to operationalize threat intelligence. The Developer SDK allows organizations to build custom integrations as well.

In 2018, Anomali announced the expansion of the partner ecosystem with the release of three software development kits (SDKs). These new SDKs enable easier and faster integration with the Anomali Threat Platform and APP Store, allowing clients immediate access to partner content, integrations and analytics. The SDKs address three critical integration areas:

- **Threat Intelligence Feeds SDK:** Integrate proprietary threat intelligence feeds and make these accessible via the APP Store
- **Integration SDK:** Integrate threat intelligence from the Anomali Threat Platform into third party products and solutions
- **Enrichment SDK:** Integrate 3rd party threat analysis and data enrichments into the platform to understand what others know about the intel in question.

Commercial Partners

Anomali is also part of an ever-growing ecosystem of commercial partners, including 30+ Technology companies, Consultants or Service Integrators, Managed Security Service Providers, and Resellers. Together these partnerships make up the Anomali “Cyber Pillar Acceleration Partner Program.” These partnerships provide advanced security solutions and proactive defense for customers, along with a competitive advantage and new revenue opportunities for partners. For a selection of partners please see: https://www.anomali.com/partners.

4.6. Anomali BOQ & System Requirements & Compliance Matrix

From experience in similar projects, Anomali put the following BOQ according to the design to get the best deployment and benefit from it.

4.7. Bill of Quantity (BOQ):

Anomali Security and AI Platform:

No.	Part Number	Part Description	Qty
	Anomali - Threat Stream - Enterprise SaaS Edition - Anomali's CTI - Threat Intelligence Platform		
1	**TS-100-SAAS- ENT**	**Anomali Threat Stream Enterprise SaaS - Threat Intelligence Platform:** **- Unlimited Users.** **- Unlimited Integrations.**	1
		Anomali University: Unlimited Access Continuous Online E-learning includes courses and certifications	
		Anomali TAM: Dedicated TAM During the Subscription Period for Onboarding, Adoption, Integrations, Quarterly Success Review, Regular Calls	
	Anomali ThreatStream ONPREM Hosted License		
2	**TS-103-ONPM-ENT**	**Anomali Threat Stream - Enterprise - ONPREMISE Hosted License for ONPREMISE Deployment**	1
	Anomali ThreatStream DR Hosted License		
3	**TS-103-ONPM-ENT**	**Anomali Threat Stream - Enterprise - DR Hosted License**	1
	Anomali ThreatStream HA Hosted License		
4	**TS-103-ONPM-ENT**	**Anomali Threat Stream - Enterprise - HA Hosted License**	1

Additional Optional Offerings:

No.	Part Number	Part Description	Qty
	Anomali Premium Feeds - Intelligence Channels		
5	IC-721-MIC-0000	**Anomali TS Intelligent Channels: Malware**	1
6	IC-725-TAMIC-0000	**Anomali TS Intelligent Channels: Adversary**	1
	Anomali - Training - Instructor Led F2F Training		
8	PS-402-TRNG-TSO	**Training: 3 days of Instructor Led Training by an Anomali Trainer on ThreatStream, Copilot and Integrator** maximum of 12 students per course. Delivered either remotely via web-conferencing. - **ONE TIME FEE**	1

4.8. System Requirements:

4.8.1. ThreatStream SaaS

4.8.1.1. Network Requirements

Analyst Use	source	destination	Destination Port
Web access for analyst to TS Service	Analyst IP	ui.threatstream.com	443
ANOMALI INTEGRATOR ONPREM	source	destination	Destination Port
Admin Web UI	Admin IP	INTEGRATOR ONPREM IP	8080
Intelligence Download	INTEGRATOR IP	api.threatstream.com	443
Admin CLI (SSH)	Admin IP	INTEGRATOR IP	22
Snapshot files, updates and documentation.	INTEGRATOR IP	https://ts-optic.s3.amazonaws.com	443
SIEM Integration			
Firewall Integration	Firewall IP	INTEGRATOR IP	443

4.8.1.2. ONPREM Integrator System Requirements:

Platform	OS Specifications	Hardware Requirements
Linux (64-bit)	• RedHat 8.x, 9.x • Ubuntu 18.x, 20.x, 22.x	**Recommended (for up to 5 destinations)** **CPU:** 6-core **RAM:** 8 GB **Swap memory**: Enabled **Free Disk Space:** 300 GB for up to 50 million indicators. Add 30 GB if your system also includes 30 days of threat models. This should be in the same partition as the installation. **Note:** If you intend to configure more than 5 destinations, provide one more CPU core per additional destination and scale RAM proportionally. In cases of very large numbers of downloaded indicators, add 3 GB of free disk space per one million additional observables. If your system needs to handle more than 30 days of threat models, then add 4 GB for each additional 10 days. **Minimum (for up to 3 destinations)** **CPU:** 4-core **RAM:** 8 GB **Swap memory**: Enabled **Free Disk Space:** 150 GB. This should be in the same partition as the installation.

4.8.2. ThreatStream On-Premises

4.8.2.1. ThreatStream ONPREM Network Requirements

Product Set			
Analyst Use	**Source**	**Destination**	**Destination Port**
Web access for analyst to TS Service	Analyst IP	ui.threatstream.com	443
	Analyst IP	TS On-Prem IP	443
On-Prem THREATSTREAM	source	destination	Destination Port
UI For On-Prem THREATSTREAM	Analyst IP	TS On-Prem IP	443
SaaS feed into THREATSTREAM On-Prem	TS On-Prem IP	api.threatstream.com	443
documents Admin CLI (SSH)	TS On-Prem IP Admin IP	ts-optic.s3.amazonaws.com TS On-Prem IP	443 22
Email Configuration	TS On-Prem IP	Email Server IP	25 and if other ports are required for email notification, please add it here
NTP	TS On-Prem IP	NTP Server IP	123
ANOMALI INTEGRATOR	source	destination	Destination Port
Admin Web UI	Admin IP	INTEGRATOR IP	8080
Intelligence Download	INTEGRATOR IP	TS On-Prem IP	443
Admin CLI (SSH)	Admin IP	INTEGRATOR IP	22
Snapshot files, updates and documentation.	INTEGRATOR IP	https://ts-optic.s3.amazonaws.com	443
SIEM Integration			
Firewall Integration	Firewall IP	INTEGRATOR IP	443

4.8.2.2. ThreatStream ONPREM OVA System Requirements (ONPREM TS, DR and HA Requirements)

System Requirements

This release of ThreatStream OnPrem is supported on systems meeting the following requirements.

Operating System

OS	Version
Ubuntu	Ubuntu Server 22.0.4 LTS

Virtual Machine

OS	VM Support
Ubuntu	• VMware ESXi server v5.5, v6.0, v6.5, v6.7U3, or v7.0 • Microsoft Azure • Amazon Web Services AMI

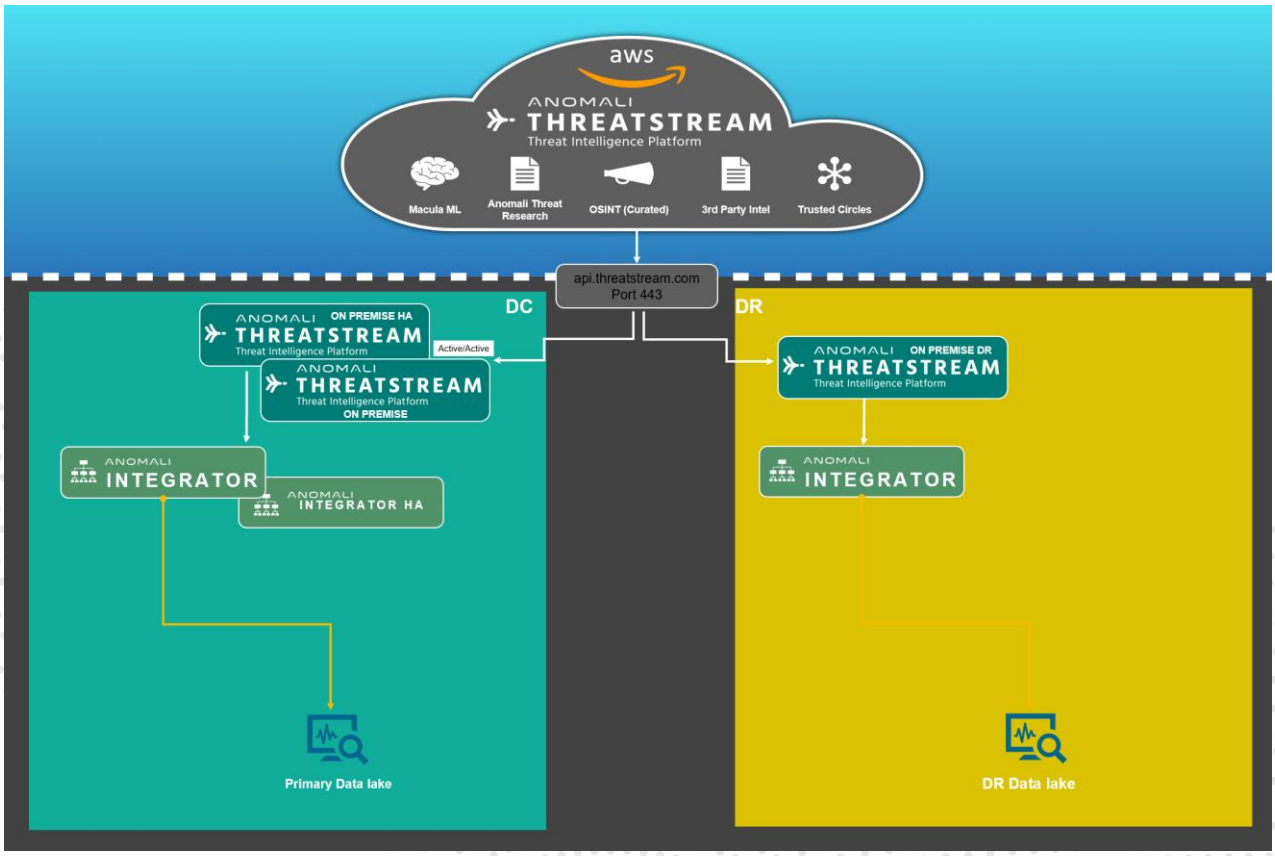
Deployment Size	Parameters	CPUs	Memory*	Primary Disk	Data Disk
Small	1-25 analysts, 0-5k observables per day, *or* 2 integrations	8-10	16 GB	64 GB	80 GB, unpartitioned SSD drive
Medium	15-25 analysts, 5-10 Anomali Lens users*, 5-10k observables per day, *or* 3-4 integrations	10-12	32 GB	64 GB	100 GB, unpartitioned SSD drive
Large	25-50 analysts, 10-15 Anomali Lens users*, 10-15k observables per day, *or* 5-6 integrations	12-16	64 GB	64 GB	200 GB, unpartitioned SSD drive

4.9. Compliance Matrix

DESC TIP Requirements	Anomali Response
Deploy a foundational Threat Intelligence Platform to enhance DNS security monitoring, integrating initial multi-source threat feeds such as: DNS-specific threat indicators (e.g., known phishing domains, malware C2 servers) from open-source feeds (e.g., OpenPhish, Abuse.ch) and commercial providers (e.g., DNSSense,	Fully Complaint. Anomali Platform integrates with over 200 threat intelligence sources, including Premium, OSINT, and RSS feeds. The platform supports standards-based threat intelligence feed integration using STIX, TAXII, and other formats through its App Store. Specialized threat intelligence feeds cover phishing and

Cisco Talos). Regional threat data relevant to UAE/Dubai (e.g., malware campaigns targeting government entities).	fraudulent activity, with multiple ingestion methods including HTTP(S) Streams, TAXII, RESTful API, and Email Inboxes.
Enable basic correlation of threat intelligence with DNS logs in the Data Lake, identifying matches (e.g., blocked queries linked to known threats) and flagging them for the Analytics Stack.	Fully Complaint. Anomali's IOC correlation engine matches indicators from ThreatStream intelligence feeds with ingested event logs
Provide a feed ingestion pipeline (e.g., via REST APIs or STIX/TAXII protocols) with a capacity to process 10,000 threat indicators daily, storing them in a searchable index tied to the Data Lake.	Fully Complaint. Anomali ThreatStream provides API-based threat data ingestion through REST API and STIX/TAXII protocols. The platform supports multiple formats including STIX 1.x/2.x, TAXII, CSV, JSON, PDF, TXT, and XML files. The system automatically processes indicators including IPs, domains, URLs, file hashes, and emails, analyzing and removing duplicates and inconsistencies.
Deliver initial threat reports summarizing correlated findings (e.g., top threats by type, volume of hits).	Fully Complaint. Anomali delivers initial threat reports summarizing correlated findings through customizable dashboards that provide clear overviews of current threats, trends, and organizational impact. The platform delivers customizable dashboards with automated creation and scheduled distribution of reports covering threat trends, intelligence sharing, and security metrics, including malicious IP activities, threat actors, and emerging trends. The system enables extensive tagging for effective automation and team analysis of IOCs, with detected IOCs including contextual tags for threat actors, campaigns, malware, and vulnerabilities.
Expand Phase 1 feeds with IP-based (e.g., botnet IPs) and geopolitical threat data, scaling ingestion to 20,000 indicators/day.	Fully Complaint. Anomali supports IP addresses as indicator types and ingests threat intelligence from over 800 sources in real-time. Specialized threat intelligence feeds cover geopolitical threats. Anomali Architecture removes limitations associated with legacy solutions and scales with proven performance
Enable real-time correlation across DNS and Internet traffic, flagging complex threats for the Analytics Stack, with weekly reports on combined insights.	Fully Complaint. Anomali monitors DNS-based threats through real-time tracking of malicious IPs, domains, and phishing campaigns. The platform provides continuous analysis of network traffic, monitoring and alerting on threats in real-time across all network telemetry. The advanced correlation engine employs sophisticated analytics to detect complex attacks, while generating actionable insights through AI-enriched threat analytics and GenAI-powered reporting capabilities.
The Threat Intelligence Platform correlates this data with expanded feeds processing daily indicators to identify risks like phishing, botnets, and state-sponsored attacks, enhancing detection across both traffic types.	Fully Complaint. Anomali's platform ingests and correlates threat intelligence in real-time from over 800 sources, automatically matching indicators with event logs from security devices including firewalls, IDS/IPS, endpoint detection tools, and network devices.

4.10. Anomali Proposed Design and Architectures



High-Level Design Description

1. **ANOMALI THREATSTREAM SaaS** is hosted on Amazon AWS. It contains billions of indicators and makes use of our Machine Learning engine (Macula) to provide our customers with the most accurate threat intelligence collected from hundreds of data sources. THREATSTREAM is also driven by research from our ATR (Anomali Threat Research) team who publishes Threat Models (Actors, TTPs, Campaigns etc) that are always up to date with the latest intelligence.
2. **ANOMALI THREATSTREAM On Premise** is a locally deployed threat intelligence platform that aggregates, enriches, and operationalizes threat data within secure, private infrastructure.
3. **ANOMALI THREATSTREAM On Premise HA** Second Instance of Anomali Threatstream to provide high availability in primary site in active-active mode
4. **ANOMALI THREATSTREAM OnPremise DR** Anomali ThreatStream Instance to be deployed in DR site which takes copy of backups from primary site instances
5. **ANOMALI INTEGRATOR** will integrate the threat intelligence with the customer's security solutions: Firewall, EDR, SIEM, and Others
6. **ANOMALI INTEGRATOR** second instance of Anomali Integrator in Primary site to provide high availability

4.11. Scope of Work

The information following under Work To be Performed is aligned with the Task information requested by DESC in the Statement of Work Documentation.

4.11.1. Project Management and Technical Services Support

Two key personnel will be assigned to DESC for the Project Management and Onboarding of the solution's deployment, as well as the ongoing Customer Success Manager.
These two individuals manage customers at Anomali and will be instrumental in driving the success of deploying and utilizing a Threat Intelligence Platform at DESC. They will with ease meet the deliverables set forth by DESC and ensure that DESC gets a very quick time to value.

4.11.2. Design, Configure, Test, and Deploy

Anomali will work with DESC upon the start of the contract to provide Architecture reviews and drawings. Every customer has a unique infrastructure and deployment methodologies may need to be adjusted specifically for DESC.

There are two key areas of the architecture that Anomali looks at with customers. One is the ingestion of intelligence from Open Source, Premium 3rd Party Vendors, STIX TAXII, ISAC, ISAO and more. The dedicated Onboarding Manager and Customer Success Manager will work with DESC to ingest all relevant intelligence that is needed to meet the mission.

4.11.3. High-level Project Plan

As required by DESC Anomali will also deliver an implementation plan with steps and dates to be agreed upon by both parties. We will actively ensure that test plans and deployments meet the standards that DESC has put forward.

Milestone Description	Start	No. Days
1: Kick-off Meeting/Planning	**TBD**	**TBD**
Present Anomali Kick-off PowerPoint/ Business Owner/Technical Team/Analyst Team	**TBD**	**TBD**
Define Specific Use Cases/Goals for Anomali Systems	**TBD**	**TBD**
List of Requested Feeds & Integrations	**TBD**	**TBD**
Architecture Readiness	**TBD**	**TBD**
Setup Weekly Sync & Monthly Health Check Meetings	**TBD**	**TBD**
2: Training & Documentation*	**TBD**	**TBD**
Register for Anomali University (Anomali Provided Documentation)	**TDB**	**TDB**
Take Anomali University Course THST - 101 (Take additional courses as needed)	**TDB**	**TDB**
Download Technical Guides and Installation Instructions	**TDB**	**TDB**
3: Configuration /Installation	**TBD**	**TBD**
Configure ThreatStream SaaS	**TBD**	**TBD**
Install and configure ThreatStream OnPrem	**TBD**	**TBD**
Install and configure software (Integrator)	**TBD**	**TBD**
Configure/Enable Feeds (From List of Requested Feeds & Integrations)	**TBD**	**TBD**
Review Integrations & Feed Streams to ensure accuracy, volume size, usability	**TBD**	**TBD**
4: Initial & Active Usage	**TBD**	**TBD**
Present ThreatStream Features/Capabilities/Services	**TBD**	**TBD**

Total Number of Days in case all requirements required by DESC are ready = **31** Days**
*Training & Documentation are required by DESC
** Indicative Number Only – Final Project Plan follows kick off session.
***The man-days for the consultancy run in parallel with the implementation

4.12. Operations and Maintenance (O&M)

Anomali Customer Care is available 24X7X365 and can be reached through a support portal, e-mail or phone as shown below.

- Anomali Support Portal: https://support.anomali.com
- Anomali Support Email: support@anomali.com

Anomali Support Teams are located in: Redwood City, Belfast and Singapore. We provide "follow-the-sun" support models in order to handle critical (SEV1) cases while ensuring standard and low priority tickets remain in the region that your business resides so that we can optimize time during standard business hours to work with you on a resolution. Additionally, the Anomali support organization has built in mechanisms to monitor for the "human factor" of everyday life (e.g. illness, unforeseen absences, support representatives workload, etc.).

4.12.1. Level of Services Offered

Our mission for software support is to provide you with services that will allow you to quickly remedy and fix any issues. Customers with Software Versions that are currently supported by Anomali and current Support contracts will receive Support Services as follows.

- **Product Usage**: Assistance with questions regarding the usage of Anomali products and associated functionality
- **Error diagnosis**: This includes analysis of Anomali error messages, the identification and isolation of the source of the problem and obtaining information and status on existing problems.
- **Resolving Errors**: This includes obtaining solutions to problems, methods to avoid problems without compromising system performance and potential temporary workarounds to errors.
- **Bug Fixes**: Provision of corrective Software to fix Errors.
- **Maintenance**: This includes Upgrades and Updates

4.12.2. Service Level Agreements

Different problems have different impacts on our customers' businesses. Anomali uses a formal ranking system to prioritize tickets. Ranking is intended to reflect the importance of a ticket to your business and ensures.

- Appropriate speed of response
- Appropriate application of resources
- Escalation as it becomes necessary

The Criteria below are used to define the severity of a ticket. During the life of the open ticket, the ranking may be adjusted to reflect the current impact on your business. For example, if a previously low severity problem becomes more urgent its priority level can be increased;

likewise, if a suitable workaround is implemented a problem may be downgraded to a lower severity level.

In summary, the use of the ranking system enables us to focus on the problems most important to you.

- **Severity 1**: Critical means a critical technical issue resulting in a total loss of core functionality in the Appliance and/or the Software or inoperability of the Software in production (e.g. a down system) that critically affects the customer's business operations. No Workaround is Available.
- **Severity 2**: High means a major technical issue resulting in severe performance problems in the Appliance and/or Software having a severe impact on customer's business operations No Workaround is Available.
- **Severity 3**: Medium means a non-critical component is malfunctioning, causing moderate impact on customer's business operations. For example, a Workaround (i) forces a user and/or system administrator to use a time-consuming procedure to operate the system or (ii) removes a non-essential feature.
- **Severity 4**: Low means a minor technical issue where the customer can use the Appliance and/or Software with only slight inconvenience.

4.12.3. Response Times (SLA)

Anomali will use commercially reasonable efforts to respond to tickets within the response times set forth below. These response times are targets only, not guarantees. Anomali does not guarantee resolution times or delivery dates. These response times are subject to change depending on the nature and complexity of the ticket.

Severity	Response Time	Update Interval
1 "Critical"	Less than 1 Hour	at least once a day
2 "High"	2 Hours	at least every other day
3 "Medium"	4 Hours	at least once a week
4 "Low"	8 Hours	as appropriate

- Response time is defined as the time between the creation of the ticket and the first attempt of an Anomali support engineer to contact the customer who opened the ticket.
- Above severities and response times apply to systems in production. Errors in nonproduction systems (e.g. test, development, sandbox) will be automatically downgraded one severity level.
- Problems with the installation of the Anomali Software shall have at most a severity ranking of "High"
- Support services for Software installation is an environment which is not in compliance with our sizing and technical recommendations will automatically be downgraded by one severity level.

- Response times apply only if e-mail communication is made via the alias. support@anomali.com, a ticket opened via the Customer Support Portal and/or if phone communication is made by calling the official and posted hotline numbers.
- If Anomali Support staff determines that an issue is fixed in a released patch, Anomali may require the customer to apply this patch before Anomali continues troubleshooting.

4.13. Training

4.13.1. Self-Based Training Anomali University

Anomali University offers threat intelligence-focused courses that are designed by industry experts that deal with and address Threat intelligence solutions spanning the creation of our product suite to help you enrich/identify/correlate valid threat intelligence data and response efforts. This training provides an accessible, self-paced learning environment that provides exams for DESC employees to validate their learning.

Anomali University was created to not only help you obtain a border understanding of threat intelligence and its applications, but also will help provide courses on how best to use and integrate our products and solutions within the DESC infrastructure. The courses provided will help DESC employees gain a stronger foundation for core threat intelligence concepts as well as practical understanding of the threat intelligence platform. Anomali University will be included with the subscription of Anomali and available on-demand to every user of the Anomali platform at DESC.

The current list of key courses that will be of immense benefit to DESC are as follows.

- Integrator: Anomali Verified
- ThreatStream: Fast Track Onboarding
- ThreatStream for End Users 101
- ThreatStream for Administrators 102
- FAST TRACK: Threat Research and Production
- FAST TRACK: Phishing Email Ingestion Workflow
- FAST TRACK: Feedback Loop Workflow
- Anomali Copilot
- Integrator Fundamentals

Additionally, Anomali University is continually expanding its content and accepts customer feedback for enhancements and creating new courses. Request for specific new training to be created can be notified to the DESC Customer Success Manager or by emailing training@anomali.com

4.14. Risk Mitigation Plan / Plan of Action and Milestones

In the event of a scan resulting in vulnerabilities in the system Anomali will provide a Risk Mitigation Plan of Action to include the data below requested by DESC

- Total number of Low, Medium and High vulnerabilities as defined by NVD
- Identification of each vulnerability
- Review the risk associated with each vulnerability
- Description of the mitigation plan

4.15. Final Technical Architecture Diagram

Anomali will provide DESC with a final architecture diagram upon completion of design of implementation. This will include all communications, security devices and interconnected resources. As the Anomali Platform will be entirely a SaaS solution there will be no hardware from the Anomali Threat Intelligence platform.

4.16. Continuous Monitoring

Anomali provides continuous monitoring of the status of the SaaS service directly at status.anomali.com. We will assist DESC in their continuous monitoring efforts as well and include the following

- monitoring the implementation of security requirements
- updating security documentation
- performing requisite vulnerability scans
- ensuring compliance to regulations, programs, policies, and procedures within DESC on an ongoing basis.

4.17. Site Security Reviews

In accordance with task 12 the Soc 2 Type II report has been submitted with the response.

4.18. Post-award Risk Assessment

Anomali is extremely familiar with complete risk assessments for our customers on an annual basis. The Customer Success Manager aligned with DESC will ensure that we complete risk assessment in a timely fashion from when they are requested from Anomali.

4.19. Appendix A: About Anomali

4.19.1. Company Overview

ANOMALI was founded in 2013 with a vision to help organizations improve security operations, accelerate threat detection, and optimize response by incorporating threat intelligence more efficiently with the security stack – and better enable the analysts. ANOMALI is backed by GV (Google Ventures) as a handful of Cyber Security solutions in its stable.

As the former pioneers of the SIEM market (ANOMALI's founders and executives also founded ArcSight), we understand the fundamentals of the challenge's security operations teams face. Specifically, most security monitoring and alerting tools look at logs/traffic to identify suspicious or malicious activity. ANOMALI identified an essential element missing from this approach – the need to attain 100% visibility on the external threat landscape alongside the 100% visibility that organizations have on their internal networks.

ANOMALI has established itself as the clear leader in the Threat Intelligence Platform space, an assessment which is based on empirical evidence (levels of investment, employee numbers and size and growth of customer-base, press coverage, maturity and partnerships).

ANOMALI launched THREATSTREAM, the Threat Intelligence Platform in 2013. THREATSTREAM has achieved great success versus its competitors given the completeness of the platform, breadth of features and workflows to support security analysts/teams, and the depth of integrations with 3rd party products (SIEMs, firewalls, endpoint systems, etc).

ANOMALI ENTERPRISE (now ANOMALI | MATCH) was launched in 2016 to accelerate and enable threat discovery by identifying any matches between hundreds of millions of indicators against billions to trillions of log events extended periods of historical data. The latest addition to the ANOMALI product suite is MATCH, MATCH is purpose-built to perform intelligence matching on this massive scale. Coupled with ANOMALI COPILOT, the ANOMALI ecosystem of products greatly assists organizations to identify the RELEVANT threats to the business with lightning speed enabling them to deploy countermeasures faster and more effectively.

4.19.2. Our Investors

GENERAL CATALYST

INSTITUTIONAL VENTURE PARTNERS

PALADIN CAPITAL GROUP

LUMIACAPITAL

CAPITAL PARTNERS

TELSTRA

SOZO VENTURES

4.19.3. Our Advisors

The Honorable Dana Deasy
Former CIO, US Department of Defense

Tom Doughty
Former Vice President and CISO, Prudential

Governor Larry Hogan
Former Governor, State of Maryland (US)

Christian Karam
Senior Advisor, Former Managing Director at UBS

Joe Sykora
SVP, Worldwide Channels and Partner Sales at Proofpoint

4.20. Anomali's Knowledge & Experience

In all matters Cyber Threat Intelligence related, as the market leader, ANOMALI is well positioned to cater to the current requirements of the NCSA. Significant investment in ANOMALI, the company's focus on Research & Development and the global nature of the ANOMALI business (with a major European R&D and Technical Support hub in Belfast and London UK as well as in the ME), means we are also uniquely positioned for innovation and can assure large headquartered organisations like NCSA, that as they progress, their future requirements will also be met.

Our capabilities are underpinned by Threat Intelligence, enabling our customers to become intelligence-led and allow for a more proactive cyber security stance. Our platforms and services are designed to greatly improve speed, agility through automation and improve the efficiency/performance of existing investments in security tools, as well as drive our customer's maturity forward, from a people and processes perspective.

ANOMALI is also uniquely positioned to support any interest the NCSA has in collaboration with peers, through the sharing of Cyber Threat Intelligence securely and effectively, via Anomali's Community Edition module, providing Trusted Circles capability and our position as the technology partner of choice to many of the world's ISAC/Intelligence Sharing communities.

ANOMALI has collaborated with similar Frameworks and has approximately 400+ Enterprise class customers with more than 1500 organizations interacting with an Anomali platform somewhere on the globe. ANOMALI has significant pedigree working with large organizations internationally, across many different verticals including Banking, Government and Oil and Gas companies.

Information of the references who granted us the permissions to disclose the partnership are available to be shared with NCSA upon request.

Notable activities in the Middle East

UBF ISAC Platform (UAE) – Threat Intelligence Sharing and collaboration between commercial banks1


BUSINESS

Banking Aviation Property Energy Analysis Tourism Markets Retail Personal Finance

UBF launches first cyber threat sharing platform for UAE banks

Banks to share cyber security intelligence on Anomali ThreatStream

STC Partnership (KSA) – STC Partners with Anomali to boost Cybersecurity and Threat Intelligence2

[1] https://gulfnews.com/business/banking/ubf-launches-first-cyber-threat-sharing-platform-for-uae-banks-1.2090165

[2] https://www.arabnews.com/node/1366806/corporate-news

Detection and Research of "Bad Tidings" Campaign targeting Middle Eastern Governments3

In-Depth research and analysis of Shamoon v3 malware4

[3] https://threatpost.com/phishing-campaign-saudi-gov/142998/

[4] https://www.securityweek.com/shamoon-3-attacks-targeted-several-sectors

4.21. References and Testimonials

“As one of the prominent banks in the United Arab Emirates, we manage assets and transactions for thousands of customers. One of our main commitments to our customers is security and we achieve this through solid partnerships with industry experts such as Anomali. By bringing in industry experts, we expect to gain advanced levels of security that will help us to further heighten our defenses and intercept any possible exploitation by cybercriminals.”
K.S. Ramakrishnan
Chief Risk Officer, RAKBANK

“We leverage market-leading tools to give our company a competitive advantage and our 24/7 SOC a leg up on bad actors. With Anomali, we improve on both of these goals. By adding intelligence, we achieve a high level of certainty that enhances prioritization of the most serious threats our customers face, while improving our mitigation decisions.”
Grant Leonard
Co-Founder, Castra

“The time it takes to analyze a threat has gone down from 30 minutes to just a few minutes, time that adds up over the course of investigating many malicious IPs every week. There has been a substantial decrease in terms of meantime-to-know.”
Arindam Bose
Senior Vice President & Security Officer, Bank of Hope

4.22. Appendix B: Anomali Resources

ANOMALI has a pool of resource that support their operations in Middle East and Africa and distributed around the region, upon project kickoff resources from that pool get assigned to Anomali Clients to complete the onboarding, adoption, integrations and regular engagements with Anomali's Clients.

Few examples for Anomali's resources profiles as following:

Profile 1

Based out of Abu Dhabi, United Arab Emirates

Information Security Professional

12+ Years in Information Security | - Implementation & Architecture -Operations -Customer Success -Customer Support

Core Competencies

- Senior Technical Account Management and Customer Success roles
- Deployment and implementation of different information security tools.
- SIEM Architecture and planning.
- Threat intelligence architecture.
- Security operations canter engineer (SOC)
- Network Engineer & Planning.

Professional Experience

- Senior Technical Account Manager & Onboarding Manager - Anomali | Feb 2021-present
- Senior Security Analyst – RSA NetWitness Platform - RSA Security | 2018 - 2021
- Cloud Operation Engineer – Orange Business Services | 2017-2018
- Senior network security engineer (SOC) – Orange Business Services | 2014-2017
- Network Engineer – Orange Business Services | 2013-2014

Certifications: CISSP | CISM | CEH | RHCE | CCNP | CCSA | ZCCA

Education:

- Bachelor Degree – Faculty of Engineering – Communication & Computer Engineering at Cairo University (2013)

Tools & Technologies

- Anomali Security Operations Platform | Splunk| RSA NetWitness | UEBA| Firewalls | Proxy | virtualization (VMware).

Profile 2

Based out of Abu Dhabi, United Arab Emirates

Accomplished Cyber Security Professional || Customer Success | | Cyber Défense, SOC Architecture, Vulnerability Management

Offering 16+ years of rich experience in designing, deploying, managing, troubleshooting and maintaining Cyber Défense/ SIEM/SOC Platforms.

Core Competencies

- **Technical account management / Customer Success offering strategic consulting and technical advice** to help customers maximize value and achieve business goals in Cyber Threat Intelligence and Detection Defense.
- **Established Security Operations / Cyber Defense capabilities from scratch for organizations**, including a leading KSA Bank and an MSSP Provider, achieving CMMI Level 4 for SOC Architecture.
- Provided advanced technical consulting on proposals, solution design, system management, and tuning of various infrastructure solutions, ensuring compliance with security requirements.

Professional Experience

- Principal Technical Account Manager – Anomali | Apr 2021 – Present
- Chief Cyber Security Engineer – Sirar by STC | OCT 2018 – Mar 2021
- Information Security Monitoring Section Head – Banque Saudi Fransi | Jan 2013 – Oct 2018
- Information Security Monitoring Analyst – Banque Saudi Fransi | Jan 2011 – Dec 2012

Key Projects

- Managed and architected the successful implementation of several Security Technologies such as SIEM Infrastructure, Anti- Malware Source Code Security Scanner, Data Leakage Prevention Solutions, Endpoint Monitoring Solutions and Vulnerability Scanning Solutions and Cyber Threat Intelligence Platforms.
- Led efforts to build Managed Security Services capabilities from Scratch at MSSP which helped launch Managed Security Services such as Managed SOC, Managed Firewall, Managed E-Mail Security, Managed SIEM and Digital Signing Services.

Certifications:

- GIAC Advisory Board Member for scoring more than 90% in GCDA Certification
- SANS GCDA Certified (Capture the Flag Contest Winner)
- CEH V|8 (Certified)
- ArcSight Certified Expert
- Splunk Certified Power User and Admin
- SANS GCIH Course Completed (Capture the Flag Contest Winner)
- PMP Course Completed
- Kaspersky Incident Response Training, FireEye training for endpoint and network attack analysis

Education: B.Tech in Electronics and Communication Engineering (2011)

Tools & Technologies

Anomali Security Operations Suit | Splunk, ArcSight, ELK | SOAR | Firewall/IDPS | EDR/NDR | DLP | VMS | Email Security

Profile 3

Based out of Abu Dhabi, United Arab Emirates

Information Security Leader | SIEM & SOC Architect

13+ Years in Information Security | Strategy • Architecture • Operations • R&D

Core Competencies

- Technical account management / Customer Success
- SIEM/SOC Architecture Planning, deployment & operationalization
- Security Engineering, Threat Detection & Hunting, Automation & Orchestration
- IT/OT/IoT Security, Threat Intelligence, MSSP, Cyber Defense Strategy

Professional Experience

- Senior Technical Account Manager – Anomali | Jun 2024 – Present
- Principal Engineer – CPX | Sep 2022 – Jun 2024
- Senior Engineer – Digital 14 | Aug 2021 – Aug 2022
- SIEM/SOC Architect – Emirates Group | Nov 2019 – Jul 2021
- Senior Consultant / SOC Manager – EY | Mar 2016 – Nov 2019
- Earlier: Principal Engineer – Mphasis, Technical Specialist – Wipro, Analyst – EY & Wipro (2011–2016)

Key Projects

- Dual-tier SIEM architecture for global aviation company (Splunk)
- National OT security strategy – UAE Energy Sector
- IAM Analytics | RPA Security | AI Discovery using Splunk / ELK

Certifications:

- TOGAF 9.2 | CEH | Splunk Architect | LogRhythm LRDE | ArcSight Admin | IBM Resilient

Education: B.Sc. Electronics – University of Calicut (2011)

Tools & Technologies

- Anomali Security Operations Suit | Splunk, ArcSight, QRadar, LogRhythm, ELK | SOAR | Firewall/IDPS | EDR/NDR

4.23. Appendix C: Feed Sources

4.24. OSINT Feed Sources

#	Source Name	Description	Type	Intelligence Channel
1	Anomali Malware Intelligence - OSINT	ATR Curated Intelligence focused on providing additional context and insights on known and suspected malware samples.	OSINT	Intelligence Channel
2	Anomali Mobile Threat Defense - OSINT	ATR Curated Intelligence focused on mobile OS systems (Android, iOS) in addition to the malware/smishing threats that target these platforms.	OSINT	Intelligence Channel
3	Abuse.ch - Feodotracker - C&C Hosts	Feodo Tracker is a project of abuse.ch with the goal of sharing botnet C&C servers associated with the Feodo malware family (Dridex, Emotet/Heodo).	Open Source Feed	OSINT
4	Abuse.ch - Feodotracker - IP blocklist	Feodo Tracker is a project of abuse.ch with the goal of sharing botnet C&C servers associated with the Feodo malware family (Dridex, Emotet/Heodo).	Open Source Feed	OSINT
5	Abuse.ch - MalwareBazaar	MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors, and threat intelligence providers.	Open Source Feed	OSINT
6	Abuse.ch - SSL Blacklist - C&C IPs	The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers.	Open Source Feed	OSINT
7	Abuse.ch - SSL Blacklist - File Hashes	The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers.	Open Source Feed	OSINT
8	Abuse.ch - SSL Blacklist - Malware File Hashes	The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers.	Open Source Feed	OSINT

9	Abuse.ch - URLHaus - Hashes	URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.	Open Source Feed	OSINT
10	Abuse.ch - URLHaus - URLs	URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.	Open Source Feed	OSINT
11	Alien Vault OTX	Open Threat Exchange (OTX) is the neighborhood watch of the global intelligence community. It allows the community to collaborate and share the latest information about emerging threats, attack methods, and malicious actors.	Open Source Feed	OSINT
12	Blocklist.de - Apache	Blocklist.de is provided by a fraud specialist, whose servers are often attacked via SSH, Mail-Login, FTP, Webserver, and other services.	Open Source Feed	OSINT
13	Blocklist.de - Bots	Blocklist.de is provided by a fraud specialist, whose servers are often attacked via SSH, Mail-Login, FTP, Webserver, and other services. This feed contains Bot IPs which have been associated with Cybercrime.	Open Source Feed	OSINT
14	Blocklist.de - Brute Force	Blocklist.de is provided by a fraud specialist, whose servers are often attacked via SSH, Mail-Login, FTP, Webserver, and other services. This feed contains IPs related to brute forcing Apache auth.	Open Source Feed	OSINT
15	BotScout	BotScout tracks the names, IPs, and email addresses of bots involved in forum spam.	Open Source Feed	OSINT
16	Botscout - Bot IPs	BotScout tracks the names, IPs, and email addresses of bots involved in forum spam.	Open Source Feed	OSINT
17	BruteForcer IP Blocklist	Abusive IPs reported via BruteForceBlocker from rulez.sk.	Open Source Feed	OSINT
18	bsdly.net - POP3 Groper	Provided by Peter N. M. Hansteen - These hosts have tried and failed to log on to the pop3 service at bsdly.net.	Open Source Feed	OSINT

19	CI Army List	CI Army is an open source IP reputation list driven by collective intelligence of Sentinel IPS's MSSP customer base.	Open Source Feed	OSINT
20	CINSscore.com - ci-badguys	CINS Army feed is harvested from Emerging Threat's CINS system. It consists of IPs that either have a poor Rogue Packet score factor, or tripped a designated number of trusted alerts across their Sentinels.	Open Source Feed	OSINT
21	Cisco Talos - IP Blacklist	IP Blacklist from Cisco Talos.	Open Source Feed	OSINT
22	Dan.me.uk - TOR Exit Nodes	List of TOR Exit nodes. Provided by Dan.me.uk.	Open Source Feed	OSINT
23	Darklist.de	Darklist.de is an IP blacklist that uses multiple sensors to identify network attacks (e.g. SSH brute force) and spam incidents.	Open Source Feed	OSINT
24	Digitalside MISP	The Digitalside MISP feed contains IOCs relating to malware and C2 infrastructure with a focus on URLs and IPs.	Open Source Feed	OSINT
25	Disconnect.me Malware and Malvertising	This OSINT Feed contains malware/malvertising domains provided by Disconnect.me.	Open Source Feed	OSINT
26	Emerging Threats - Compromised	Rules to block known hostile or compromised hosts.	Open Source Feed	OSINT
27	Emerging Threats - Compromised IPs	Compromised IPs from Proofpoint Emerging Threats.	Open Source Feed	OSINT
28	Emerging Threats C&C Server	Emerging Threats fwrules rules.	Open Source Feed	OSINT
29	GreenSnow.co - Blocklist	GreenSnow is a team consisting of the best specialists in computer security, we harvest a large number of IPs from different computers located around the world. GreenSnow is comparable with SpamHaus.org for attacks of any kind except for spam.	Open Source Feed	OSINT
30	Haley's Brute Force IPs	IP addresses launching SSH dictionary attacks. Provided by charles.the-haleys.org.	Open Source Feed	OSINT

31	Internet Storm Center - Daily Sources	Internet Storm Center offers an open source feed of the most suspicious domain names.	Open Source Feed	OSINT
32	Internet Storm Center - DShield Scanning IPs	Internet Storm Center offers an open source feed of scanning IPs.	Open Source Feed	OSINT
33	Internet Storm Center - Top IPs	Internet Storm Center offers an open source feed of the top Attacking IPs.	Open Source Feed	OSINT
34	Maxmind - Anonymous Proxy List	Maxmind Anonymous Proxy IPs.	Open Source Feed	OSINT
35	NixSpam - DNS Blacklist	This DNS blacklist is permanently regenerated by the NiX Spam project of the German IT magazine iX. It contains IP addresses of spam senders. The blacklist can be used to protect mailservers against spam.	Open Source Feed	OSINT
36	NixSpam - IPs and Hashes	This DNS blacklist is permanently regenerated by the NiX Spam project of the German IT magazine iX. It contains IP addresses of spam senders and hash values (fuzzy checksums) of incoming spam. The blacklist can be used to protect mailservers against spam.	Open Source Feed	OSINT
37	NVD CVEs	CVEs from NVD site.	Open Source Feed	OSINT
38	OpenPhish.com	OpenPhish launched in June 2014 as a result of a 3-year research project on phishing detection, which yielded a set of autonomous algorithms for detecting zero-day phishing sites. These are used to produce an open source phishing URL feeds.	Open Source Feed	OSINT
39	PhishTank - Phishing URLs	PhishTank is a free community site where anyone can submit, verify, track and share phishing data. PhishTank is operated by OpenDNS, a company founded in 2005 to improve the Internet through safer, faster, and smarter DNS.	Open Source Feed	OSINT
40	Project Honeypot	Project Honeypot, created by Unspam, is a community-sponsored Honey Network and reports malicious IPs worldwide.	Open Source Feed	OSINT

41	Snort - IP Blocklist	Snort is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.	Open Source Feed	OSINT
42	The Spamhaus Project - Drop List	spamhaus.org - The Spamhaus Project is an international nonprofit organization that tracks spam and related cyber threats.	Open Source Feed	OSINT
43	The Spamhaus Project - Extended Drop List	spamhaus.org - The Spamhaus Project is an international nonprofit organization that tracks spam and related cyber threats.	Open Source Feed	OSINT
44	Threatfox OSINT	OSINT Malware IOCs, powered by Abuse.ch.	Open Source Feed	OSINT
45	VoIPBL.org - VoIP Blacklist	VoIPBL is a distributed VoIP blacklist that is aimed to protect against VoIP Fraud and minimizing abuse for networks that have publicly accessible PBX's.	Open Source Feed	OSINT
46	VoIPBL.org by ScopServ	VoIPBL is a distributed VoIP blacklist that is aimed to protect against VoIP Fraud and minimizing abuse for networks that have publicly accessible PBX's.	Open Source Feed	OSINT
47	VXVault - URLs	VXVault is run by a security researcher who publishes malicious URLs, IPs, and file hashes found in malware samples.	Open Source Feed	OSINT

4.25. Freemium Feed Sources

No.	Service Name	Description	Type
1	AbuseIPDB	AbuseIPDB provides a central list for web administrators, system administrators, and other interested parties to report and find IP addresses that have been associated with malicious activity online.	Free Enrichment
2	Anomali Free Sample Malware	Free access to 5 of the top 300 Malware/Ransomware families that the Anomali Malware Intelligence Channel covers. This channel includes a subset of the available Hashes, IPs, Domains and URLs. Powered By PolySwarm.	Free Feed
3	Anomali GeoIP	This enrichment allows users to determine geographical information of IP Addresses.	Free Enrichment
4	Anomali Open Ports	Anomali Open Ports provides a history of open ports and services for IP addresses throughout ThreatStream.	Free Enrichment
5	Cybersixgill Darkfeed™ Freemium	Cybersixgill Darkfeed™ Freemium is a subset stream of malicious Indicators of Compromise, extracted in real-time from the largest collection of deep & dark web TI data, alerting to emerging threats at the earliest stage of the illicit supply chain.	Free Feed
6	Cybersixgill Reports Freemium	Accelerate time-to-intel with automated reports harnessing Cybersixgill's best-in-market threat intelligence from the deep and dark web, to inform better security decisions and clear visibility into the organizational threat landscape.	Free Feed
7	DNSTwister	DNSTwister allows users to generate a list of registered variations of an inputted domain name, helping to determine phishing, typosquatting, and attack domains associated to the initial domain name.	Free Enrichment

8	Flashpoint Technical Intelligence	Flashpoint Technical Intelligence is a "Freemium" report feed to help users determine tactics, techniques and procedures (TTPs) and threat actor motivations associated with malicious activity. This is a subset of our Flashpoint Intelligence Reports.	Free Feed
9	Have I Been Pwned?	Have I Been Pwned? enables you to quickly assess if an email address has been put at risk due to a data breach.	Free Enrichment
10	Hybrid Analysis	Falcon Sandbox Public API transform	Free Enrichment
11	RiskIQ	This integration allows users to view additional enrichments from Risk IQ, such as Passive SSL, on Observable Details Pages and pivot from Domains to Certificates on the Graph UI.	Free Enrichment
12	Shodan Database	Shodan helps users to profile Internet connected devices, determine device manufacturer and type and evaluate services based on its comprehensive search engine.	Free Enrichment
13	VirusTotal	If your organization subscribes to the Virus Total service, you can enter your API key to receive Virus Total enrichments.	Free Enrichment
14	Whois History	By leveraging data from various providers and internal databases this enrichment provides details of the target host.	Free Enrichment

5. Assumptions

- Only solutions in BOQ is part of scope
- All the BOQ will be implemented in customer environment, no infrastructure components included in this scope.

6. About Paramount Computer Systems

6.1. Corporate Profile

"We are the product of our own thinking processes and whatever we are thinking of today is Paramount for our tomorrow."

Paramount, the regional leader in cyber-security enables customers to protect their critical Information Assets and Infrastructure through a prudent combination of People, Process and Technology. Founded in 1992, transformed into an Internet Security Solutions Provider in 1999, reconfigured in 2007 through a Management Buy Out (the first MBO of an IT Company in Dubai Internet City) and being reinvented in 2015 to morph into a trusted cyber-security solutions provider, Paramount always remains a work in progress company. The company started as early as 2001 at the ISO level and graduated through the EFQM framework by introducing and sustaining a culture of continuous learning, quality and focus on individual value-add inside and outside the organization. Paramount today, is the only IT services company in the entire Middle East to have secured an amazing gamut of certifications and unbiased recognition: **ISO 9001; ISO 20000; ISO 27001; ISO 22301; DQAP; Mohammed Bin Rashid Award - Business Excellence; Dubai SME 100; GPTW (Great Place to Work) and Dubai Chamber CSR Label.**

Over 515+ strong work force with Security Consultants and Engineers make Paramount one of the largest reservoirs of security talent in the Arabian Gulf region. Paramount's Management Team has over 200 man-years of industry experience including 93 man-years in the cyber security arena. The essence of Corporate Governance at Paramount is not only to allow the Management the freedom to propel the company forward, but to exercise that freedom within a governance framework that assures transparency, accountability, effective operational control, and management of risk.

It is the consistent focus on Quality and Excellence that has enabled Paramount to acquire a huge base of customers across the Arabian Gulf region (UAE, Oman, Bahrain, Kuwait, Qatar, and Saudi Arabia) in all verticals – Oil & Gas, Finance, Government, Airlines & Transportation, and large Corporates.

Our Growth Timeline

STORY SO FAR

1997
Founded

1998
Diversified into a Cyber Security

2007
Opened offices in Bahrain, Kuwait & Qatar

2008
First MBO in DIC

2012
Great Place to Work with 100 HC

2013

2014

2015

2016
Opened a New Office in Kenya

2017

2018

2019

2020

2021

2022
Happiest work place in GCC (Best Employee Engagement , Best Employee Wellness & Diversity & Inclusion Awards)

2023
Launched India office as Cybersecurity Nxxt Pvt Ltd; and as Ahlan Cyber in KSA

2024
Wellbeing at Workplace Award (WAW)

2025
Paramount CyberNxxt Pvt Ltd - Australia has been officially incorporated

Our Vision & Mission

Our Vision

Mounting Value for all our stakeholders, year on year, through Customer Insight, Industry Foresight, Collaboration and Execution Excellence.

Our Mission

- Be the most Respected Company in Information Security space of the Gulf Region
- Be an Employer of Choice for Information Security Professionals
- Be a metrics driven organization ensuring predictable, sustainable, profit and revenue growth
- Contribute 2% of our Net Profit every year to a well-designed CSR Program

Awards

GREAT PLACE TO WORK®

Information Security Management System ISO 27001 Certified

CERTIFIED ISO 9001:2008 COMPANY

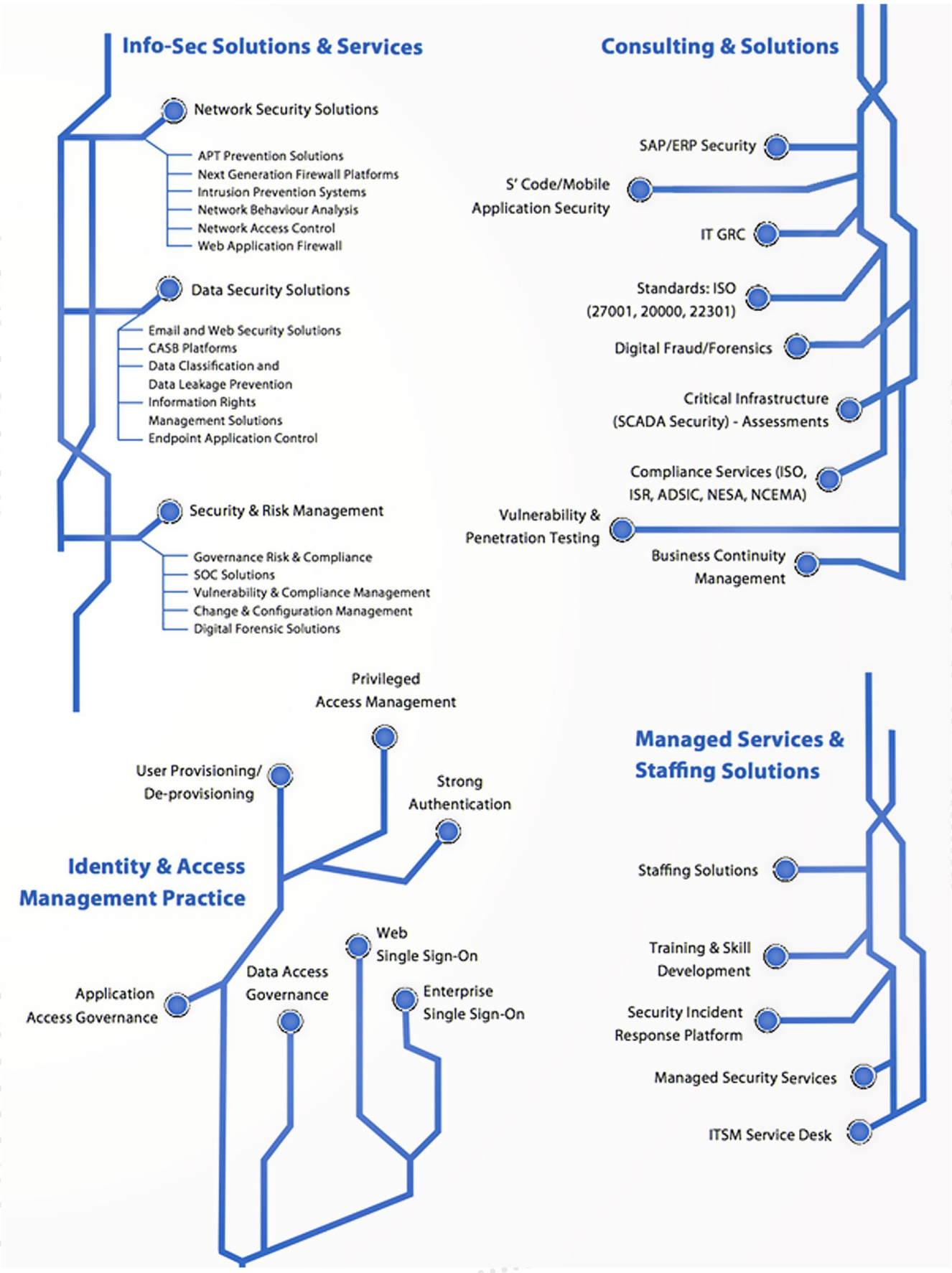
INVESTORS IN PEOPLE

جائزة محمد بن راشد آل مكتوم للأعمال
MOHAMMED BIN RASHID AL MAKTOUM BUSINESS AWARD

SME 100 Award 2013
FAST MOVING COMPANIES

Customers

What We Do



Technology Services

Secure Content Management

- Web Security
- Email Security
- Data Classification, DLP & DRM
- Database Security
- Endpoint, Server Security
- Encryption Solutions

Perimeter & Network Security

- NGFW, UTM & SSL VPN
- Intrusion Prevention Systems
- APT & Advanced Malware Detection
- Network Access Control
- Web Application Firewall
- Application Delivery Controllers
- Network Behaviour Analysis

Risk Management

- Security Incident & Event Management
- Security Operations Centre
- Vulnerability & Compliance Management
- Change & Configuration Management
- Forensic Investigation
- Governance Risk & Compliance

Identity & Access Management

- Strong Authentication
- Identity Management & User Provisioning
- Enterprise & Web Single Sign-on
- Privilege Access Management
- Application & Data Access Governance

Consulting Services

Assessment Services

- Vulnerability Assessment & Penetration Testing
- Risk Assessment & Mitigation Plan
- Business Impact Analysis

Compliance Services

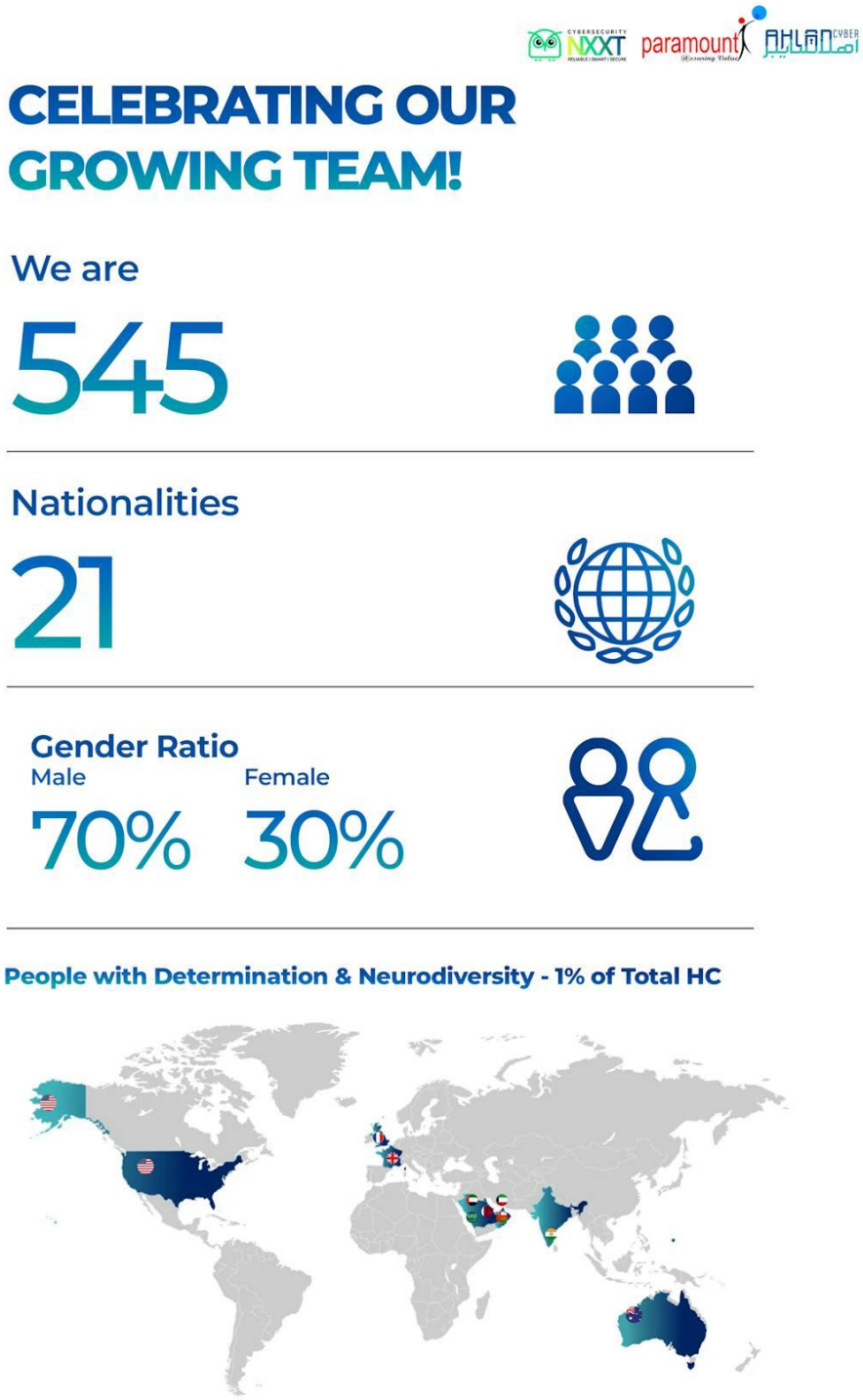
- ISO 27001 , ISO 20000 , ISO 22301 Consultancy
- ISR , NESA , ADSIC, NCEMA Consultancy
- Business Continuity & Disaster Recovery Planning

Specialized Services

- SAP Security
- Critical Infrastructure Security (SCADA) Assessments
- IT GRC Consulting & Solutions

People-Our Strength

Paramount has one of the best security teams in Middle East. Being the pioneers in Information Security Technologies and Services in Middle East, Paramount has total staff strength of over 545+ as of Mar 2025.



Certifications

Paramount focuses only on providing Information Security Technology and Services and offer local Project Management, Security Consulting, Quality Assurance and Client Relationship to its Customers. The list showcases the certifications that our Consultants with International work experience hold.

Certifications held with Technical Team

List of Certifications held with Consulting Team

ISO22301	Balanced Score Card	COBIT Foundation	CISSP
ISO9001	CCNA	COBIT Assessor	GICSP (OT Security)
ISO 27001 LA	RSA Archer Certified	CISM	CBCI
ISO 2701 LI	ISO19011:2002	CCSK	CCNP
ISO20000	Offensive Security Certified	Certified IT DR Specialist	SABSA
ITIL	Certified Ethical Hacker (CEH)	CISA	ABCP

Corporate Social Responsibility

Since the company's inception, Paramount has sought to contribute to society while coexisting harmoniously with the community in which it operates. Even while the company was in its initial growth phase, Paramount launched philanthropic initiatives designed to strengthen ties with local communities.

Paramount Value Add

Paramount Computer Systems leverages a proven methodology that includes interactive information gathering sessions, process and mechanisms assessments, scans – if required, and manual testing and review. Paramount is in an exceptional position to bring immense Benefits to the deliverables of the project and would exceed the expectations of the project stakeholders given the following.

- Experience in Consulting on Global Security Standards and Regional Regulations (ISR&ADSIC)
- Holistic information Security Company offering solutions and services that cover the entire spectrum.
- Representing clear and growth-oriented Information Security Solutions
- Regional presence scalable Internationally
- Outstanding company reputation, Awards & Certifications (ISO27001, ISO 9001-2000, DQAP, Investors in People, MRM Award, top 50 in Dubai SME 100 etc.)
- Best of Breed – technology partnerships and Clearly Drafted methodologies and processes
- Leadership having rich experience in the Information Security business.
- Highly qualified consultants with years of work experience and industry certifications such as CISSP, CISA, CISM, ISO 27001 LA, CEH, CGEIT etc.
- Excellent Track record of implementing comprehensive Security practices in several Government, Semi-Government, private and SMEs.
- World-class consultants who have immense expertise, skills, and experience in similar projects.
- Proven review and risk assessment standards and working methodologies that can easily be used to mitigate.

7. Terms and Condition

Quote Validity	8th April 2026
Delivery Time	8-10 weeks from the date of Receipt of Order/PO
Other Comments	Any shipping or government charges will be billed on actuals
Payment Terms	Hardware and Software License 100% on Delivery **Professional Services**: • 25% upon project initiation (kick-off) • 25% upon approval of detailed design • 25% upon completion of User Acceptance Testing (UAT) • 25% upon final project completion and sign-off
VAT	All prices are exclusive of VAT
Exclusions	Rack mounting and power points

8. Point of Contact

Sales:

Name	Mohammad Khaled
Designation	Customers Success & Vendors Allianz Manager
Email Id	Mohammad.k@paramountassure.com
Phone No.	+971 5647 60007
Address	Paramount Computer Systems FZ LLC, 102, Building #1, Dubai Internet City, P.O. Box 25703, Dubai, UAE