NETSCOUT | Arbor

NETSCOUT Threat Vault

Mike McNerney
sr. Director Product Management – Threat Intelligence

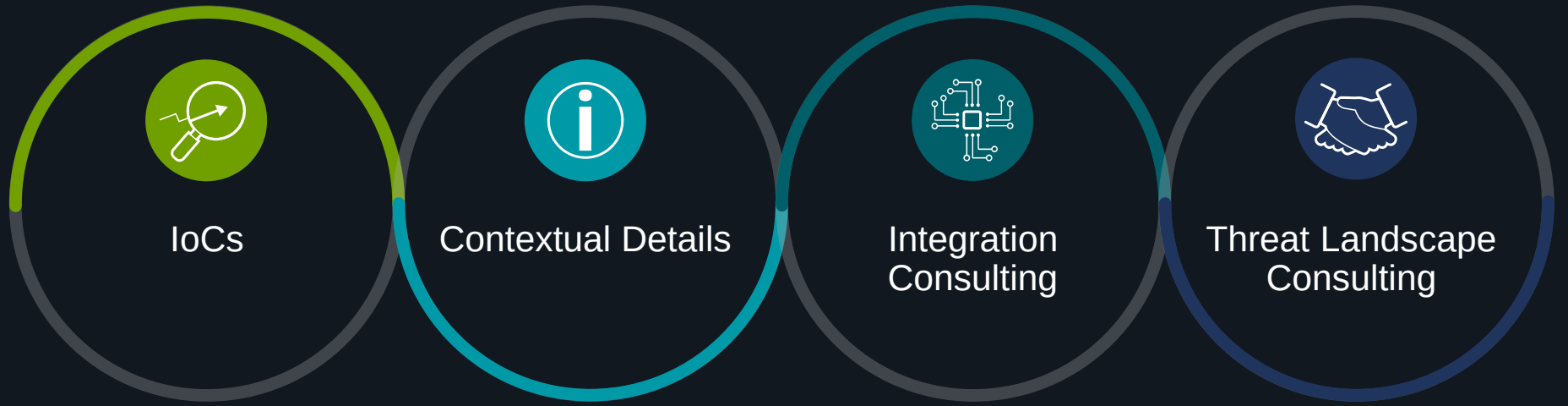
Why is NETSCOUT Threat Vault Important?

1. Increase and promote NETSCOUT’s credibility and brand recognition in the eco-system

2. Organize our Threat Intel assets for external consumption.

3. *Monetize our intelligence capabilities beyond what's directly relevant for our products.*

NETSCOUT Threat Vault



NETSCOUT Threat Vault

Coverage

Reputation

- Indicator based
- Policy oriented
- Network focused IPs, Domains, URLs, MD5s, Mutex, Register Key, etc.

- Dynamic Updates for Accurate, Timely Protection
- Threat Validity and Prioritization

- Attack Infrastructure and Methods
- Gauge Risks
- Prioritize Security Operation Tasks
- Take Proactive Measure with Confidence

Context

Rich contextual information derived from wide range of data sources available via API

Industry standard formats (STIX, CSV, etc.) for easy integration

NETSCOUT Threat Vault

Coverage

Threat Indicator Categories	
Location-Based Threats	• Traffic Anonymization Services • TOR • Proxies • Sinkholes • Scanners • Others
Email Threats	• Spam • Phishing
Targeted Attacks	• APT • Hactivism • RAT • Watering Hole • Rootkits
Mobile	• Mobile C&C • Spyware • Malicious Apps

Malware Coverage	
Malware	• Webshell • Ransomware • Fake Anti Virus • Banking • Cryptocurrency • Social Network • DDoS Bot • Dropper • Ad Fraud • Worm • Credential Theft • Backdoor • Point of Sale • Others

NETSCOUT Threat Vault

Use Cases

Use Cases	Enterprises	Service Providers / MSSPs	Gov. Agencies | CERTs
Threat Intel. Operationalization – Integrate into 3rd Party Security Solutions	✓		
Threat Research | Investigation	✓	✓	✓
Increase MSSP Service Effectiveness & Accuracy		✓	
Infected Traffic Blocking		✓	

Operation and Research focused offering

NETSCOUT Threat Vault

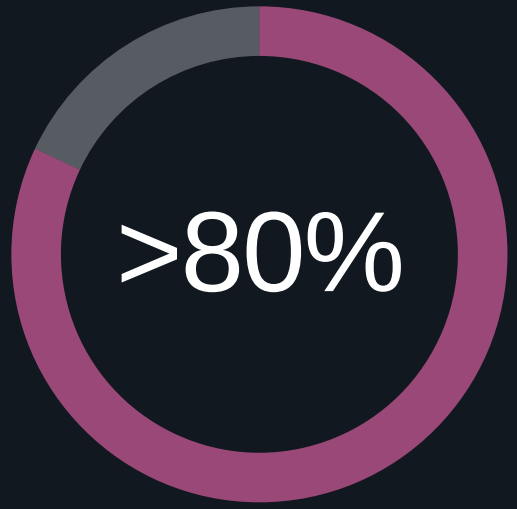
Key Value Differentiators

High Fidelity

Contextual Rich

Proof – IoCs in NTV

Curated



Unique

Highly selective and unique IoCs for optimal edge protection

NETSCOUT | Arbor

NETSCOUT Threat Intelligence

What Makes Up ATLAS Intelligence?

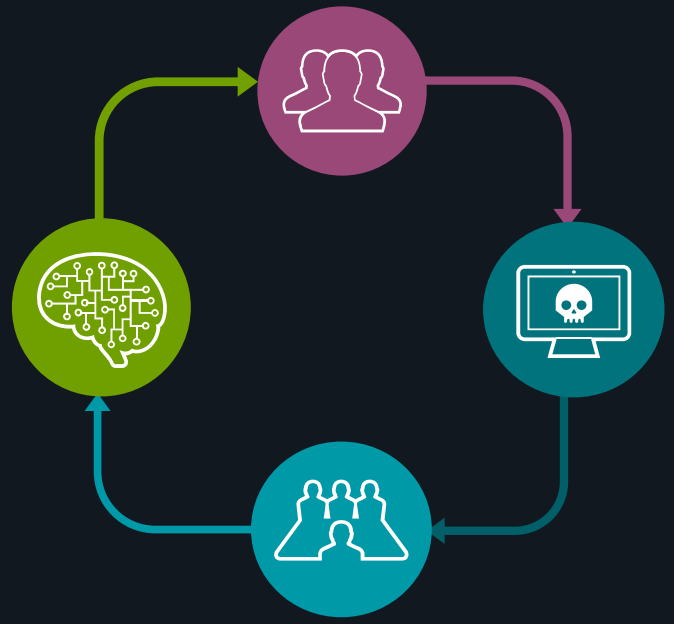
Impactful Threat Intelligence

Impactful Intelligence = Dedicated Expertise + Global Collections + Rigorous Process

People

ATLAS Security Engineering & Response Team (ASERT)

Industry renowned elite security research group



Key influencers of NETSCOUT Security Solution

Collection and analysis of malware at the scale of Internet for over a decade

Collaborate with hundreds of CERTs and government agencies

Focus. Expertise. Dedication

Collections

Unparalleled Data Collection

Public Data Sources

High quality public data source

Private Intel. Partners

20+ malware sharing partners

Commercial Intel. Feeds

Complementary commercial threat intelligence feeds

Darknet Forum Monitoring

Partnership with Underground Forum/Darknet monitoring organizations

Botnet Monitoring System

Monitoring and tracking 50+ botnets activities

Product Feedback Data

- 350+ Sightline deployments worldwide
- 200+ APS / AED deployments worldwide
- Attack information, malware matches, etc.

Honeypot

IoT Honeypots deployed around the world capturing exploitation attempts, brute-force botnet propagation, and DDoS attacks.

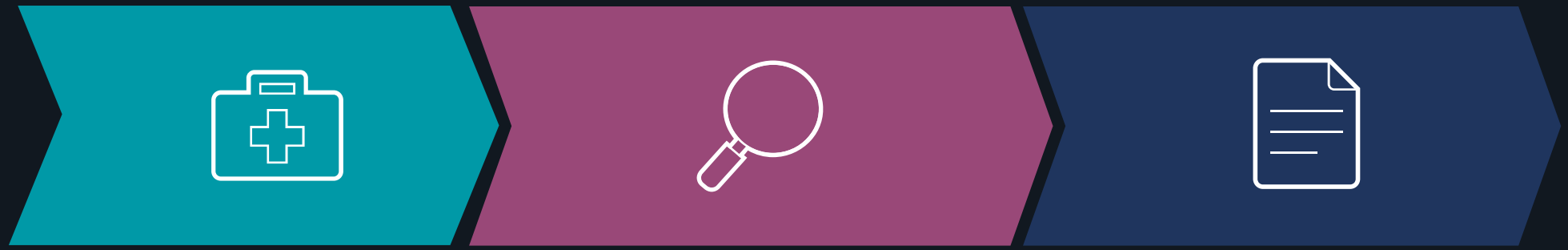
Sinkhole

Maintain 5000+ domains. Over 100+ malware families check in from all over the world

Scanner

Operate a full 10Gbps scanner, capable of scanning the entire IPv4 address space in minutes

Process



Enrichment

- Geo-location
- NAIC
- ASN

mCorral Engine

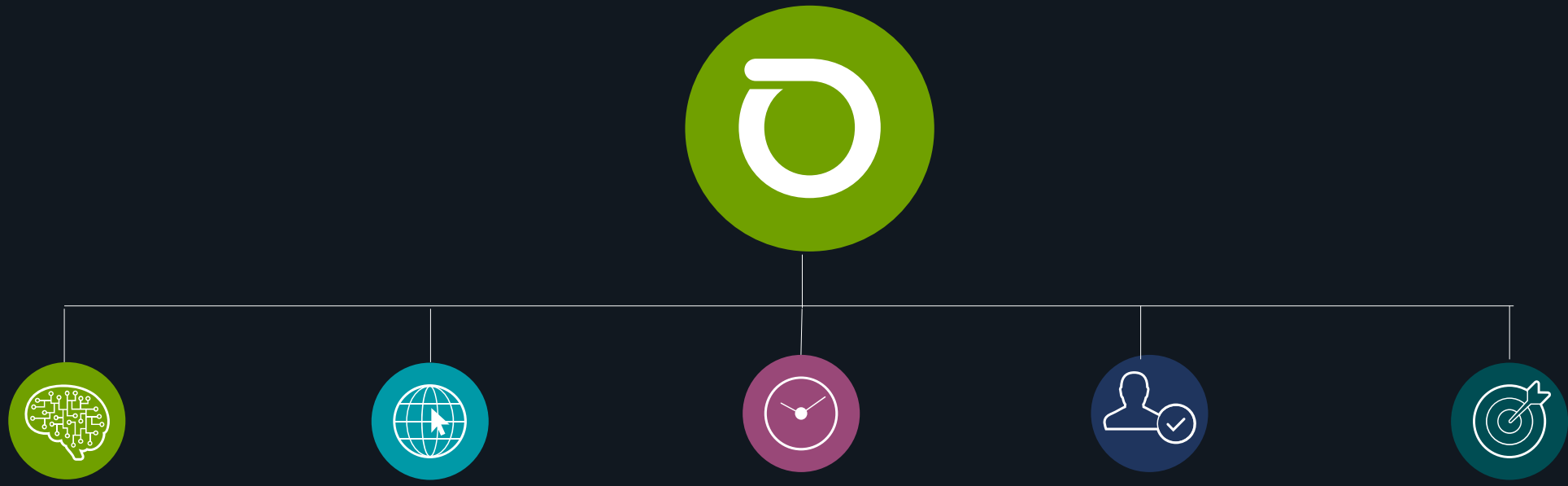
- Deep Behavioral Analysis
- Recursive Introspection & Extraction

Validation

- Age. Severity
- Blacklist. Whitelist
- Reputation. Sinkhole. Abuse

10+ year malware analysis expertise. 200,000+ malware samples processed daily

ATLAS Intelligence - Differentiation



Industry renowned elite security research group

Unparalleled data collections

Deep Behavioral Analysis

Recursive Introspection / Extraction

Accurate & effective scoring

People. Collection. Process

Thank You.

Mike.McNerney@netscout.com

www.netscout.com