

Vulnerability & Attack Surface Management Program

Vulnerability Scanning

Networks (internal & external scans) + Applications

Vulnerability Prioritization

Security Intelligence Driven Risk Based Prioritization

Technical Readouts

Cadenced Analysis Of Key Threats, Newly Identified Vulnerabilities & Remediation Progress

Vulnerability Hunting & Notification

Active Analysis Of Existing Asset Inventor, Vulnerabilities To New & Trending Threats & Vulnerabilities

Attack Surface Management

Continuous Discovery Of Known & Unknown Assets & Exposures

Validation & False Positive Elimination

Evaluate Exposure To Determine Impact, Compensating Controls & Remediation Activities

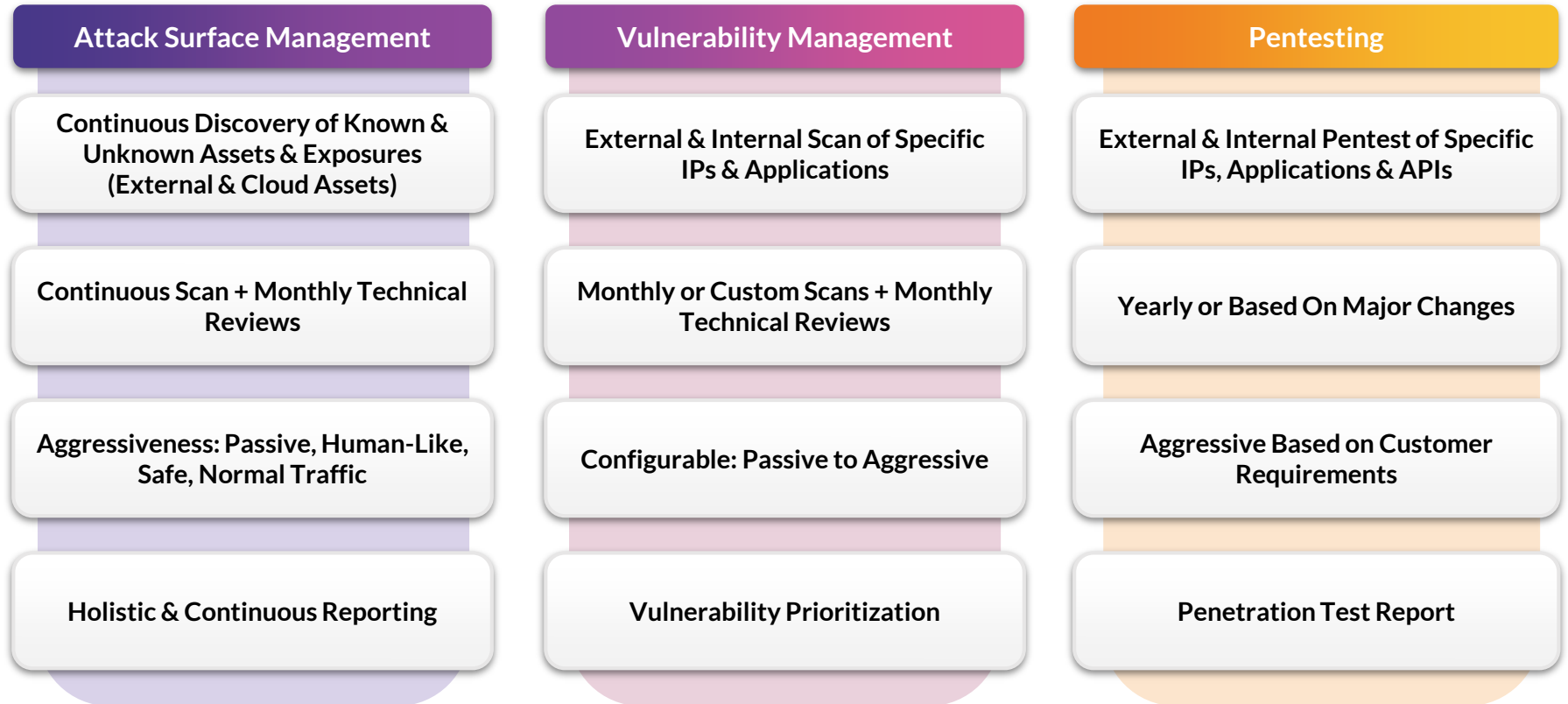
Quarterly Business Review

Stakeholder Program Review Of Key Accomplishments, Ongoing Projects & Identify Where Help Is Needed

Rapid Response

Immediate & Continuous Action To Identify & Validate Impact of New Threats

Attack Surface Management Enables Vulnerability Management & Penetration Testing



Attack Surface Management

Continuous Discovery of Known & Unknown Assets & Exposures (External & Cloud Assets)

Continuous Scan + Monthly Technical Reviews

Aggressiveness: Passive, Human-Like, Safe, Normal Traffic

Holistic & Continuous Reporting

Vulnerability Management

External & Internal Scan of Specific IPs & Applications

Monthly or Custom Scans + Monthly Technical Reviews

Configurable: Passive to Aggressive

Vulnerability Prioritization

Pentesting

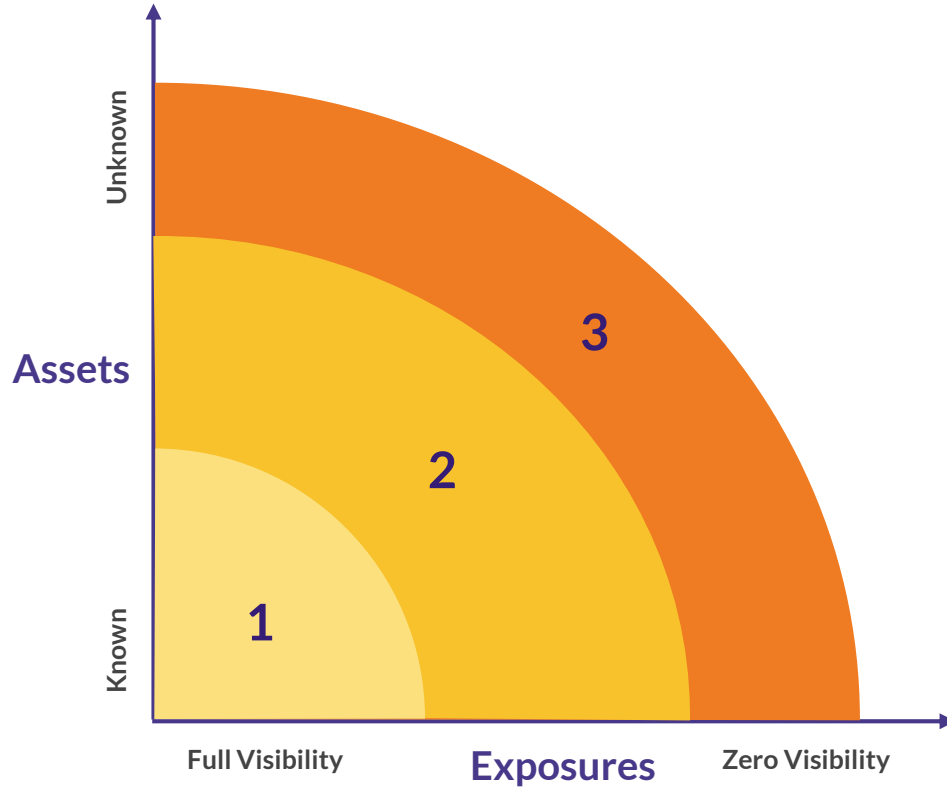
External & Internal Pentest of Specific IPs, Applications & APIs

Yearly or Based On Major Changes

Aggressive Based on Customer Requirements

Penetration Test Report

Continuous Monitoring: Maintain Strong Security Posture



1 **Known Assets & Exposures**
Official domains + VPN Servers +
Valid Certificates

2 **Possible Insights**
Misconfigured Databases & S3
Buckets + Exposed RDP

3 **Unknown Assets & Exposures**
Shadow IT + Exposed Non-Production
Systems + Legacy Systems

Darknet Layer Details

Commodity Data

- Public paste site collection
- Clear web forums
- Social media
- Automated collection

Medium Value Data

- Less common datasets
- Data is valuable enough to sell
- High volume collection: automated collection is complex but possible
- Collection requires some knowledge of underground markets

High Value Data

- Complex and unique data
- Data is breached and traded by advanced actors and professionals
- Individual relationships & reputation required to collect on this level
- Databases often unique and very high value - used for active criminal targeting

Very High Value Data

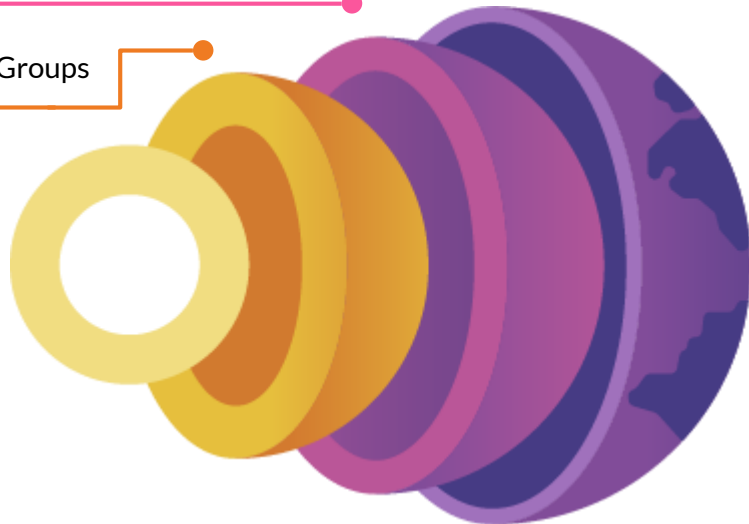
- Small, dangerous communities sharing extremely sensitive corporate user data
- Malware data and corporate access sold by sophisticated actors, often to syndicated
- Collection requires longstanding and intimate relationships
- Operational security is paramount

SURFACE Open Forums

MIDDLE Vetted Forums

LOWER Closed Groups

CORE Offline Groups



Discovery Focuses on the Lower & Core layers of the Darknet