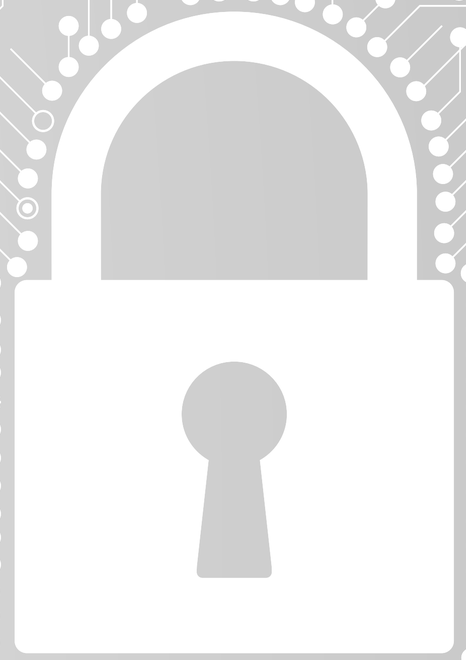
INFORMATION SECURITY DEPARTMENT

SMT GROUP



TURNING CYBER DEFENSE INTO CYBER RESILIENCE

EXECUTIVE SUMMARY

SMT PROTECTS GOVERNMENTS, TELECOMS, AND FINANCIAL INSTITUTIONS THROUGH ITS CYBER FUSION CENTER **(CFC)**

OUR 24/7 SOC DETECTS AND CONTAINS ATTACKS I**N UNDER 3 DAYS – COMPARED TO THE 200+ DAY AVERAGE WITHOUT A SOC**

AI-DRIVEN OPERATIONS (CARA ENGINE) AND CERTIFIED EXPERTS DELIVER RAPID, MEASURABLE RESILIENCE

INDUSTRY CONTEXT

AVERAGE DETECTION TIME WITHOUT SOC: **>200 DAYS (IBM DBIR 2025).**

WITH AI-ASSISTED SOC: **DETECTION <3 DAYS, CONTAINMENT <24 HOURS**

80% OF ATTACKS START WITH CREDENTIAL THEFT OR PRIVILEGE MISUSE

SMT GROUP IN NUMBERS

15+ COUNTRIES | **50+** TECHNOLOGY PARTNERS | **5,000+** CUSTOMERS | **80+** EXPERTS | **15M+** USD REVENUE

FOUNDED 2005 – EVOLVED INTO A CYBER FUSION ECOSYSTEM INTEGRATING TRAINING, CONSULTING, AND MANAGED SERVICES

CYBER FUSION CENTER (CFC)

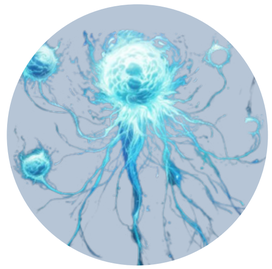
NOT A CONVENTIONAL SOC – A COGNITIVE AI-DRIVEN DEFENSE HUB

IT'S A SOC **THAT THINKS, NOT JUST REACTS**

INTEGRATES CARA **(CYBER AI ANALYST)** AND SMT'S PROPRIETARY SKILL & ACTION FRAMEWORK

BUILT FOR **PROACTIVE DETECTION, REASONING, AND AUTOMATED CONTAINMENT**

SMT PRODUCT SUITES (CYBERHEROES)



I.O (Intelliorbit)

(INTELLIORBIT): CENTRAL HARMONIZER AND COORDINATION ENGINE

طوق

CORE

(CYBER OPS & RESILIENCE ECOSYSTEM): SOC & MDR LAYER

فارس

TITAN

(TACTICAL INTRUSION TRACKING & NETWORK SECURITY):NETWORK DEFENSE

حارس

ELITE

(EDUCATIONAL LEARNING IN IT & CYBER EXCELLENCE): LABS & TRAINING

خبير

TIAID

(THREAT INTEL & AI DEFENSE):

مُهدِّد

SOC PROCESS HIERARCHY

L1 – ALERT MONITORING, ENRICHMENT, AND HEALTH CHECKS.

L2 – DEEP ANALYSIS, CONTAINMENT, AND ESCALATION

L3 – IR LEADERSHIP, FORENSICS, AND THREAT INTEL

SOC MANAGER – SLA GOVERNANCE AND STRATEGY ALIGNMENT.

PEOPLE AND EXPERTISE

14+ CERTIFIED SOC ANALYST (CSA), 15+ CEH, 6+ CTIA, 3+ CHFI, 5+ ISO 27001 LA, 7+ LI, CISM, CISA, PMP, ITIL

CONTINUOUS TRAINING THROUGH SMT ACADEMY AND ELITE LABS

SMT GUARANTEE & SLAS

P1 TRIAGE ≤ 5 MINUTES, CONTAINMENT ≤ 15 MINUTES

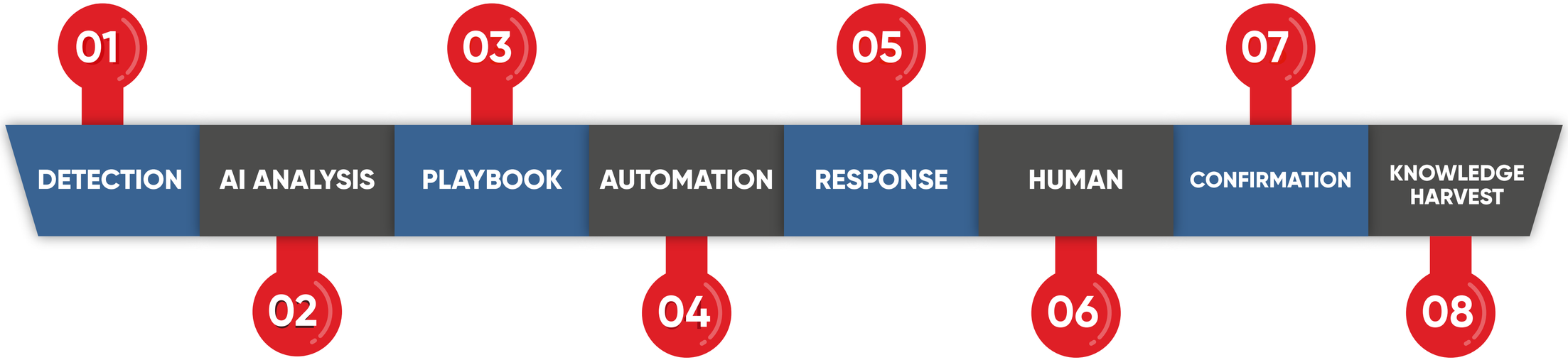
COMPREHENSIVE SLA ENSURING UPTIME, CONTAINMENT SPEED, AND CLIENT REPORTING

24/7 MANAGED DETECTION, RESPONSE, AND RECOVERY

CORE TECHNOLOGIES

-UNIFIED PLATFORM AND AI – STRIKEREADY
-SIEM – IBM QRADAR
-SOAR – IBM RESILIENT
-EDR/MDR – CROWDSTRIKE FALCON COMPLETE
-ASM – GROUP-IB
-SOURCE CODE SCAN – BLACKDUCK (COVERITY)
-NDR – ARISTA
-CASB AND MOBILE PROTECTION– LOOKOUT
-EMAIL PROTECTION – PROOFPOINT
-THREAT INTEL – CROWDSTRIKE, IBM PREMIUM, STRIKEREADY, GROUP-IB

SOC WORKFLOW (CFC PLATFORM)



AUTOMATED TRIAGE AND PRIORITIZATION WITH CARA LEARNING ENGINE

THREAT INTELLIGENCE (TIAID)

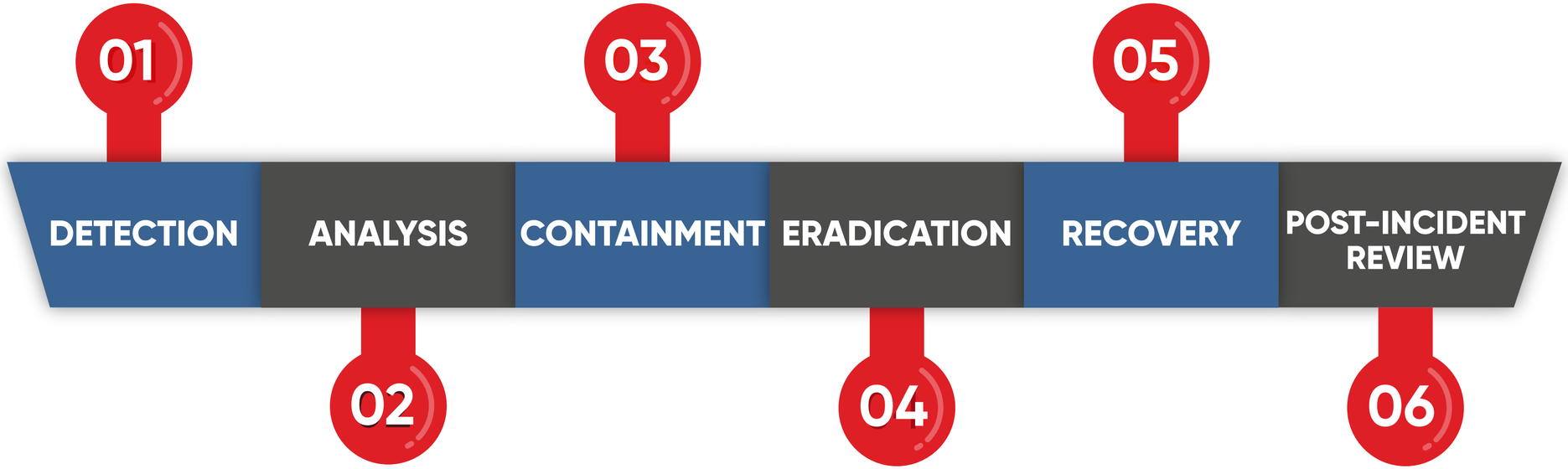
AI-DRIVEN FEEDS ENRICHED WITH HUMAN VALIDATION

PREDICTIVE THREAT MODELING AND ACTOR MAPPING

REGIONAL FOCUS: MENA-SPECIFIC TTPS AND INTELLIGENCE SOURCES

INDUSTRY FOCUSED THREAT FEEDS

INCIDENT LIFECYCLE



VALIDATED THROUGH CFC AUTOMATION AND HUMAN OVERSIGHT

AI SUPPORT (CARA ENGINE)

NATURAL LANGUAGE UNDERSTANDING FOR CONTEXTUAL ALERT TRIAGE

GUIDES ANALYSTS TOWARD HIGH-CONFIDENCE DECISIONS

CONTINUOUSLY LEARNS FROM RESOLVED INCIDENTS

CLOUD & IDENTITY SECURITY

LOOKOUT CASB PROVIDES UNIFIED VISIBILITY AND CONTROL OVER **SAAS, IAAS, AND PRIVATE CLOUD APPLICATIONS**

DEPLOYED AS PART OF SMT'S **CFC CLOUD DEFENSE ARCHITECTURE**, IT CONTINUOUSLY MONITORS USER ACCESS, DATA SHARING, AND APPLICATION BEHAVIOR

DATA PROTECTION: ADVANCED DLP AND CONTENT INSPECTION PREVENT SENSITIVE DATA EXPOSURE ACROSS OFFICE 365, GOOGLE WORKSPACE, AND CUSTOM APPS

ADAPTIVE ACCESS CONTROL: ENFORCES CONDITIONAL POLICIES BASED ON USER RISK SCORE, DEVICE POSTURE, AND REAL-TIME THREAT CONTEXT

THREAT DETECTION: USES MACHINE LEARNING TO IDENTIFY ANOMALIES SUCH AS INSIDER EXFILTRATION, OAUTH ABUSE, OR SESSION HIJACKING

INTEGRATION WITH SIEM & SOAR: LOOKOUT'S TELEMETRY FEEDS DIRECTLY INTO IBM QRADAR AND RESILIENT, ENABLING END-TO-END MONITORING AND AUTOMATED RESPONSE.

OUTCOME: ENSURES SECURE, COMPLIANT, AND MONITORED CLOUD ADOPTION — WITH VISIBILITY FROM THE ENDPOINT TO THE CLOUD WORKLOAD

VA/PT AND APPSEC

AUTOMATED + MANUAL PENETRATION TESTING

SECURE CODE REVIEW AND SDLC ALIGNMENT

APPSEC TRAINING INTEGRATED INTO DEVELOPER LIFECYCLE

SOC AUTOMATION (SOAR)

PLAYBOOKS FOR EDR, IAM, AND NDR CONTAINMENT

AUTOMATED NOTIFICATIONS AND STAKEHOLDER UPDATES

REDUCED MEAN-TIME-TO-RESPONSE THROUGH ORCHESTRATED WORKFLOWS

CONTINUOUS IMPROVEMENT

QUARTERLY PURPLE-TEAM TESTING AND TABLE TOP EXERCISES

DETECTION CONTENT UPDATES ALIGNED WITH MITRE ATT&CK

PERFORMANCE REVIEWS AND ADAPTIVE TUNING

PERFORMANCE METRICS

MTTD (MEAN TIME TO DETECT) – <3 DAYS

MTTR (MEAN TIME TO RESPOND) – <24 HOURS

FALSE POSITIVE RATE <10%

DETECTION COVERAGE >90% OF MAPPED ATT&CK TECHNIQUES

CASE STUDY

SMT CFC CONTAINED A RANSOMWARE INCIDENT IN UNDER 15 MINUTES

PREVENTED LATERAL MOVEMENT AND DATA EXFILTRATION

IMPLEMENTED NEW IDENTITY GUARDRAILS AND DETECTION RULES

KNOWLEDGE HARVESTING

EACH INCIDENT FEEDS SMT'S KNOWLEDGE HARVESTING INFRASTRUCTURE

DATA USED TO TRAIN AI MODELS AND UPDATE TI FEEDS

ENSURES CONTINUOUS LEARNING ACROSS ALL CFC SERVICES AND TEAMS

REPORTING & DASHBOARDS

EXECUTIVE DASHBOARD: RISK TRENDS AND SLA ADHERENCE

OPERATIONAL DASHBOARD: TICKET FLOW, COVERAGE, AUTOMATION METRICS

ENGINEERING DASHBOARD: RULE PERFORMANCE AND DATA HEALTH

KEY DIFFERENTIATORS

AI-DRIVEN SOC (CFC + CARA)

REGIONAL PRESENCE AND CULTURAL AWARENESS

HIGHLY CERTIFIED ANALYSTS AND PROVEN SLAS

COMPREHENSIVE PRODUCT ECOSYSTEM INTEGRATION

IMPACT SUMMARY

SMT SOC REDUCES DETECTION TIME FROM 200+ DAYS TO <3 DAYS

DRASTICALLY IMPROVES NATIONAL AND ENTERPRISE CYBER RESILIENCE

COMBINES AI PRECISION WITH HUMAN JUDGMENT

THANK YOU