cor.

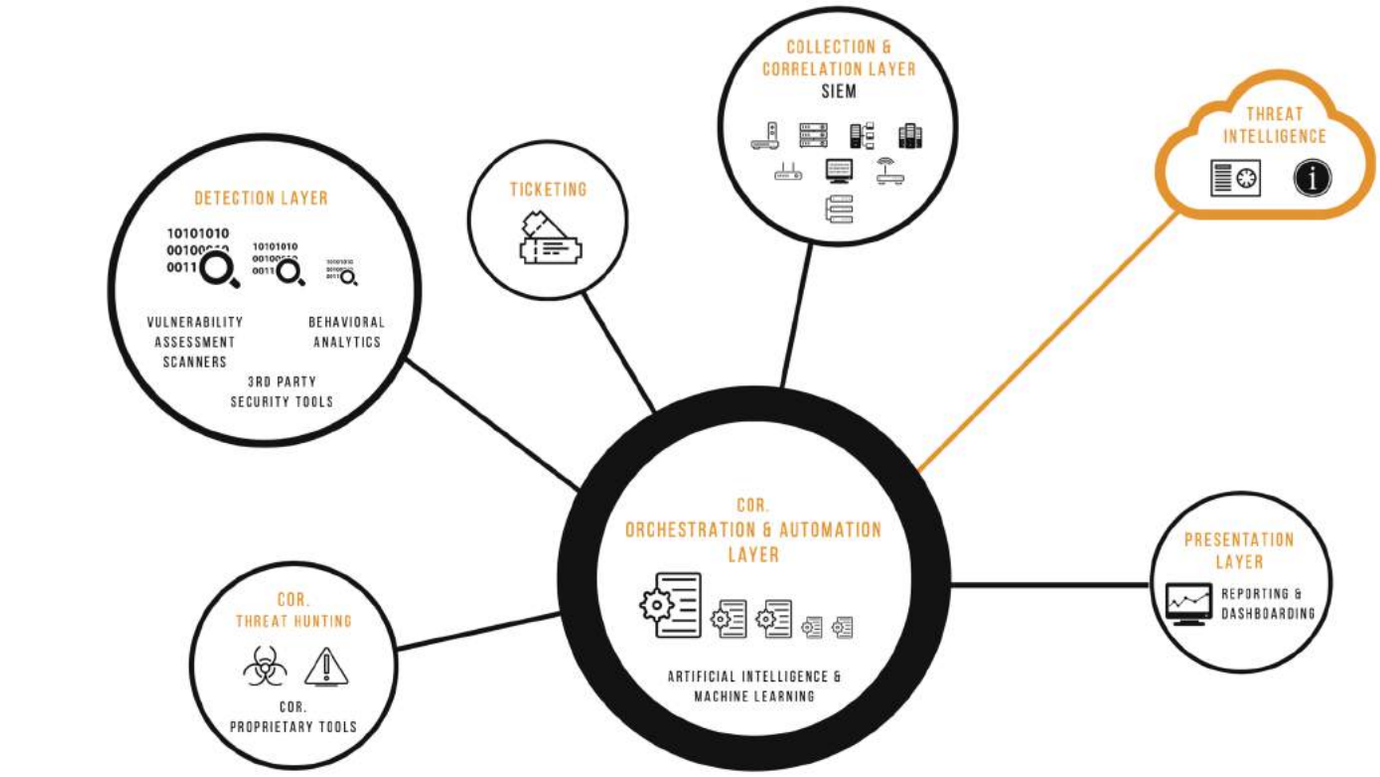
PLATFORM DATASHEET

Integrated stack of advanced security solutions that enables the delivery of Cyber Security Managed Detection & Response services for our clients.

Version 1.0a

OVERVIEW

cor. the platform integrates within the enterprise environment while enabling the delivery of advanced cybersecurity services across detection, prevention preemption, and response.
Overlaid by Coordinates continuous monitoring services (Security Operation Center), our platform offers an industry-leading approach to defend against cyber threats through automation and orchestration of detection and response.



DATA RESIDENCY

cor. technology stack is engineered to take into consideration heightening requirements for data residency. cor. platform collects, normalizes, stores & correlates within the client environment in full compliance to the client own security policies. Data never leaves the client premise.

TAILORED COMMUNICATIONS

We manage all client communications through a highly secure and customizable ticketing system - tailored to suit client-specific communication and escalation requirements.
24x7 access to our Cybersecurity analysts through multiple channels: Chat, Ticket, Email and Phone.

coordinates

MULTILAYER CORRELATION

At the core of our Cybersecurity Technology & Service delivery is our overarching architecture of Orchestration and Automation.
This layer allows our Incident Response teams to trigger advanced analytics and correlation playbooks to significantly reduce the time to triage and respond to validated threats.
It also enables pervasive correlation of events across all elements and log sources; it enriches our analysts' capabilities by instantly identifying threats across the enterprise environment with the exact context for an effective response.
Those capabilities not only dramatically reduce false-positives incidents and time to remediate but enables our team to automate tactical response to detected threats.

REPORTING & REAL-TIME DASHBOARDS

Dashboard and Reporting repository capabilities are integrated into cor. platform; This will ensure secure client access to their information and consistent compliance and respect to Data Residency across all the services life cycle.

CURATED THREAT INTELLIGENCE

Our platform incorporates Advanced Threat Intelligence subscription.
Our team curates and tailors the threat feeds to the enterprise-specific environment, industry, geography, threat actors among other factors.
Threat Intelligence from more than fifty different sources of threat feeds is regularly curated and automatically pushed to the cor. platform. This critical process enriches the enterprise environment to enable actionable intelligence and augment our Incident Response team with the proper tools to effectively and timely defend from imminent threats

PROACTIVE THREAT HUNTING

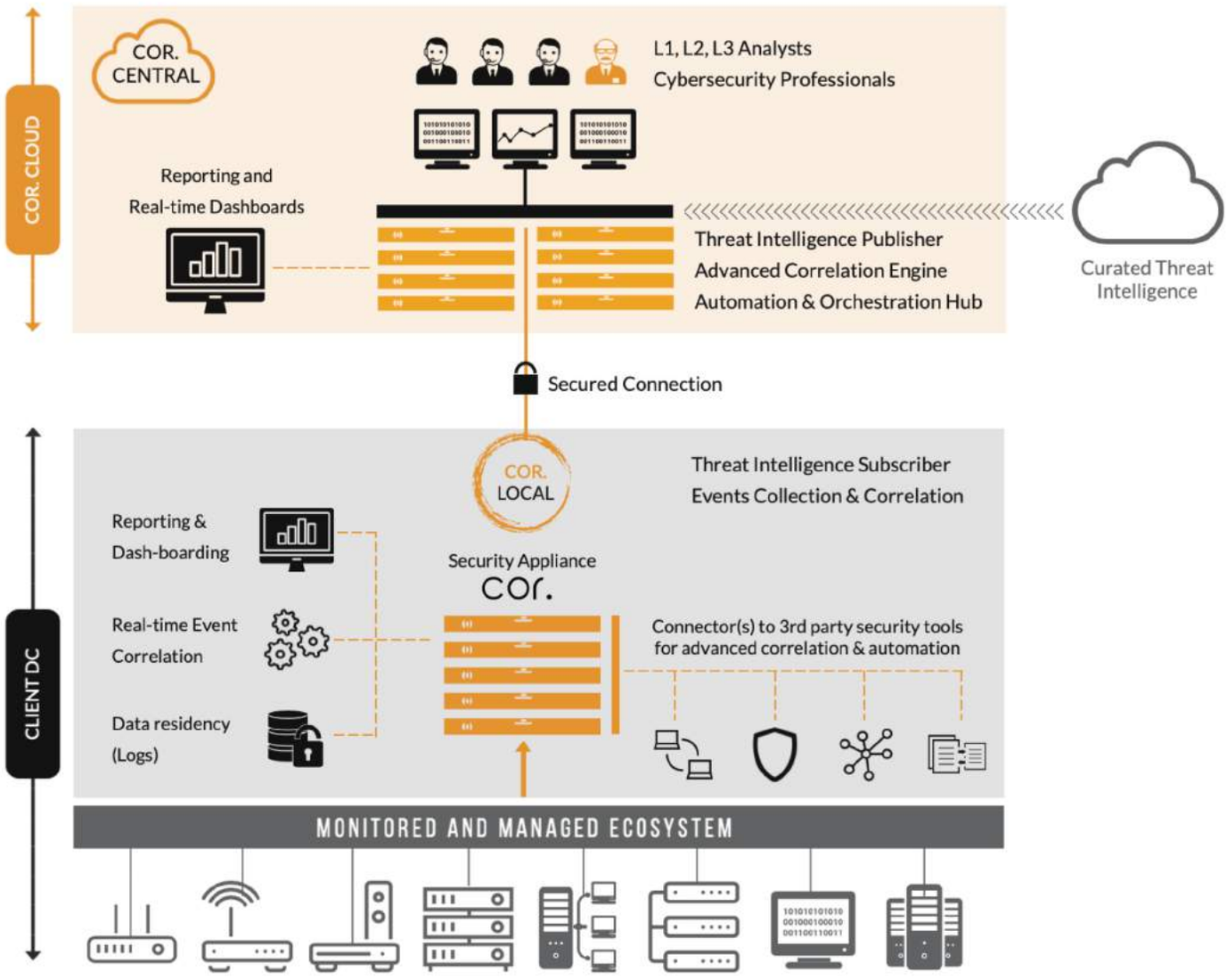
Armed with automated threat detection and analytics technology, curated threat intelligence, and proactive threat hunting methodology, our specialized security analysts, perform deep inspection of the enterprise environment to identify Indicators of Compromise (IOCs), undetected vulnerabilities, suspicious insider behavior and other malicious activity on your network.
Our Proactive Threat Hunting identifies gaps in enterprise security architecture and detects threats that typically evade traditional security controls.

TECHNOLOGY STACK

#1	Events Collection & Correlation	1st Layer of correlation at the SIEM Level 2nd Layer of correlation at the Orchestration & Automation Level
#2	Threat Intelligence	50+ Sources (Commercial & Open Source)
#3	User/Network Behavioral Analytics	Built-in the cor. platform via tailored use cases for each customer using a pre-defined baseline
#4	Proactive Threat Hunting	cor. proprietary tools, methodologies and scripts integrated into our automation platform and used by our cybersecurity threat hunters.
#5	Continuous Vulnerability Assessment Management	Offered out-of-the-box in the cor. platform
#6	Security & Workflow Automation	cor. proprietary tools, scripts and automation playbooks
#7	Security Integration Layer	Integration with security tools (e.g. EDR Solutions, Endpoint Protection) to provide more accurate cyber threat visibility on client infrastructure

PLATFORM ARCHITECTURE

cor. distributed architecture allows us to offer scalable monitoring across our client infrastructure regardless of the technology used in the datacenter or the remote sites.
cor. Local being deployed at the client site for advanced on-premises correlation and data residency compliance.
A unidirectional threat intelligence feed is pushed from our data centers to cor. Local subscriber allowing the detection of the latest threats occurring world wide.
Event Logs concentrators (VM) are deployed in all remote sites with a high ratio compression before sending it to the main cor. appliance for events correlation, minimizing the impact on the client's inter-site bandwidth.

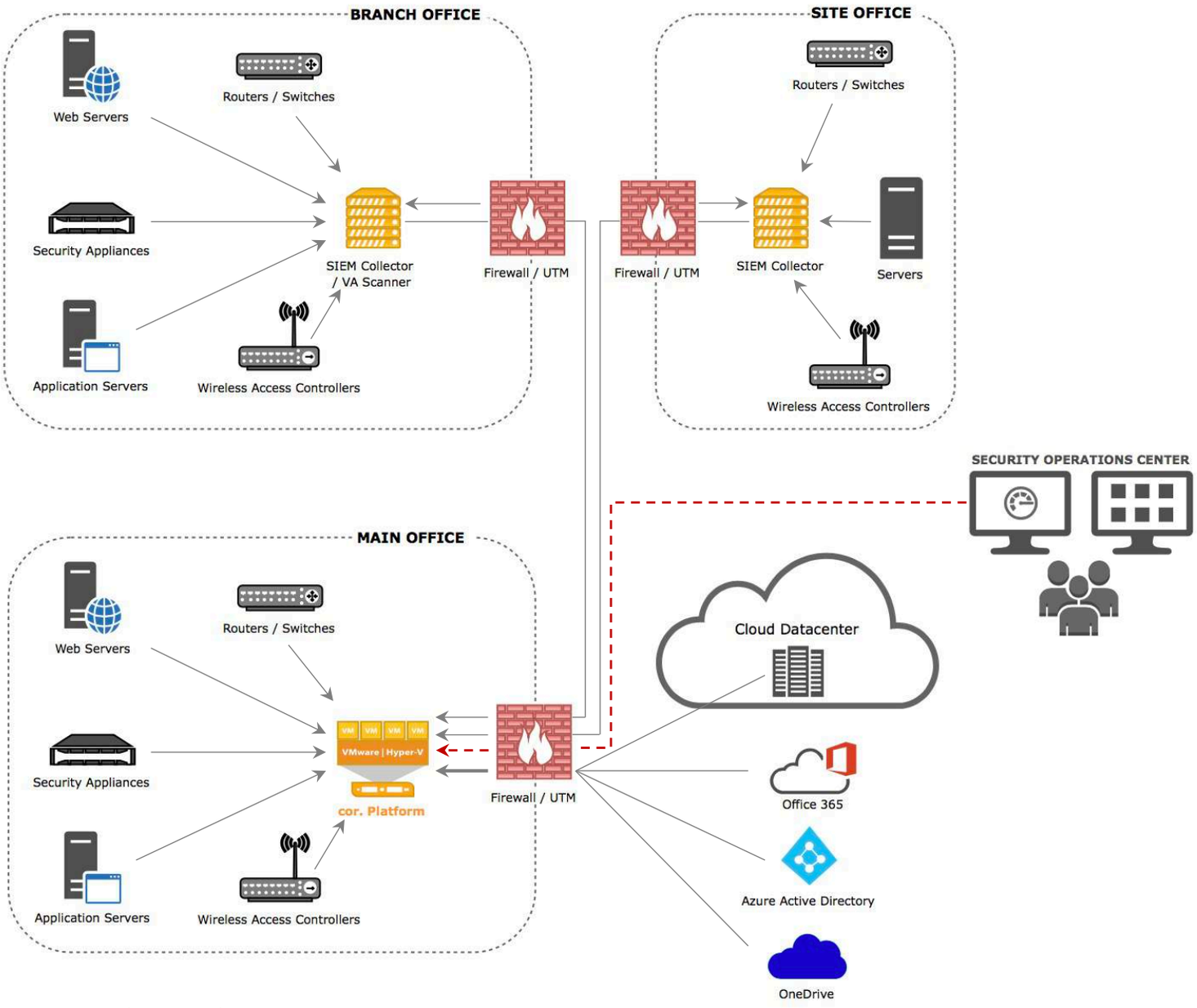


DEPLOYMENT NODES

In the case where Virtual Machines cannot be deployed in remote offices, logs can be sent directly to the main office platform.
In the event of connectivity loss between the remote sites/branches and the main office, logs won't be collected during that period and those specific events will be lost.

Collecting events at the branch-office through deployment of a VM will enable storing (Cashing) those logs if a connectivity issue occurs - When connectivity to the Head Office is restored, those logs are sent again to the cor. platform.

Sample Deployment Architecture



cor. Nodes Deployment

Main office	1 Log Collector (VM)
Branch office	1 Log Collector (VM) 1 Vulnerability Assessment Scanner (VM)
Site Office	1 Log Collector (VM)
Cloud Datacenter	1 Log Collector (VM)

The main cor. appliance is deployed at the main office and sized according to several parameters defined through joint technical workshops with the client.

- Number of Monitored Devices and their Types
- Estimated number of Events per Seconds (EPS)
- Number of Active PC/Laptop/Mobile users
- Number of Monitored Live IPs
- Data Logs Retention Period
- Client's infrastructure and Number of Remote offices/sites

DEPLOYMENT METHODOLOGY

01

PREPARATION PHASE

- Kick-Off Meeting
- Technical workshops
- Full data gathering
- Policies & Processes Customization
- cor. appliance delivery & installation

02

CONFIGURATION PHASE

- Network & Access configuration
- Technology Stack initial configuration
- Collector(s) deployment & configuration
- Devices configuration for log collection & SNMP
- Custom Parsing development
- Threat intelligence configuration
- Baseline Definition (User/Network Behavior)
- SIEM rules import/customization/finetuning
- CVAM & Scanning templates configuration
- Custom Policies implementation
- Ticketing system customization
- Advanced IR playbooks deployment
- Security automation deployment
- Reports & Dashboards customization

03

MANAGEMENT & FINETUNING PHASE

- Advanced finetuning
- Quality control checks
- Sharing Pre-Live security risks findings
- Finalizing SOC Documentation
- Handover customer documentation and access
- Go-Live date agreement
- Handover to IR team on D-Day

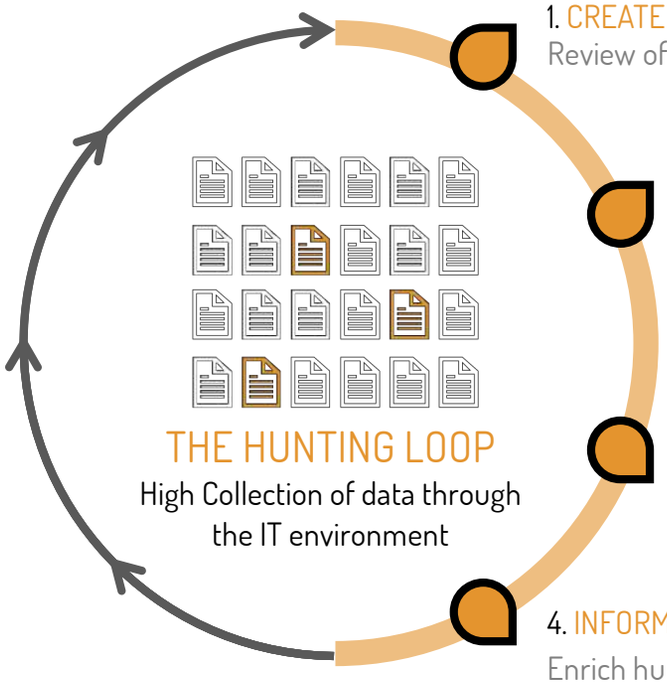
04

MONITORING PHASE

- 24x7x365 Monitoring, Detection, Response, Remediation
- Multi-channel support (Level 1, 2, 3)
- Remediation implementation support
- Continuous Compliance Review
- Scheduled Customer review visits and platform tuning

INCIDENT RESPONSE

PROACTIVE THREAT HUNTING



1. CREATE Hypotheses
Review of Threat Intelligence

2. INVESTIGATE Via Tools & Techniques
Leverage hunting procedures and collected data to detect adversary or IoC

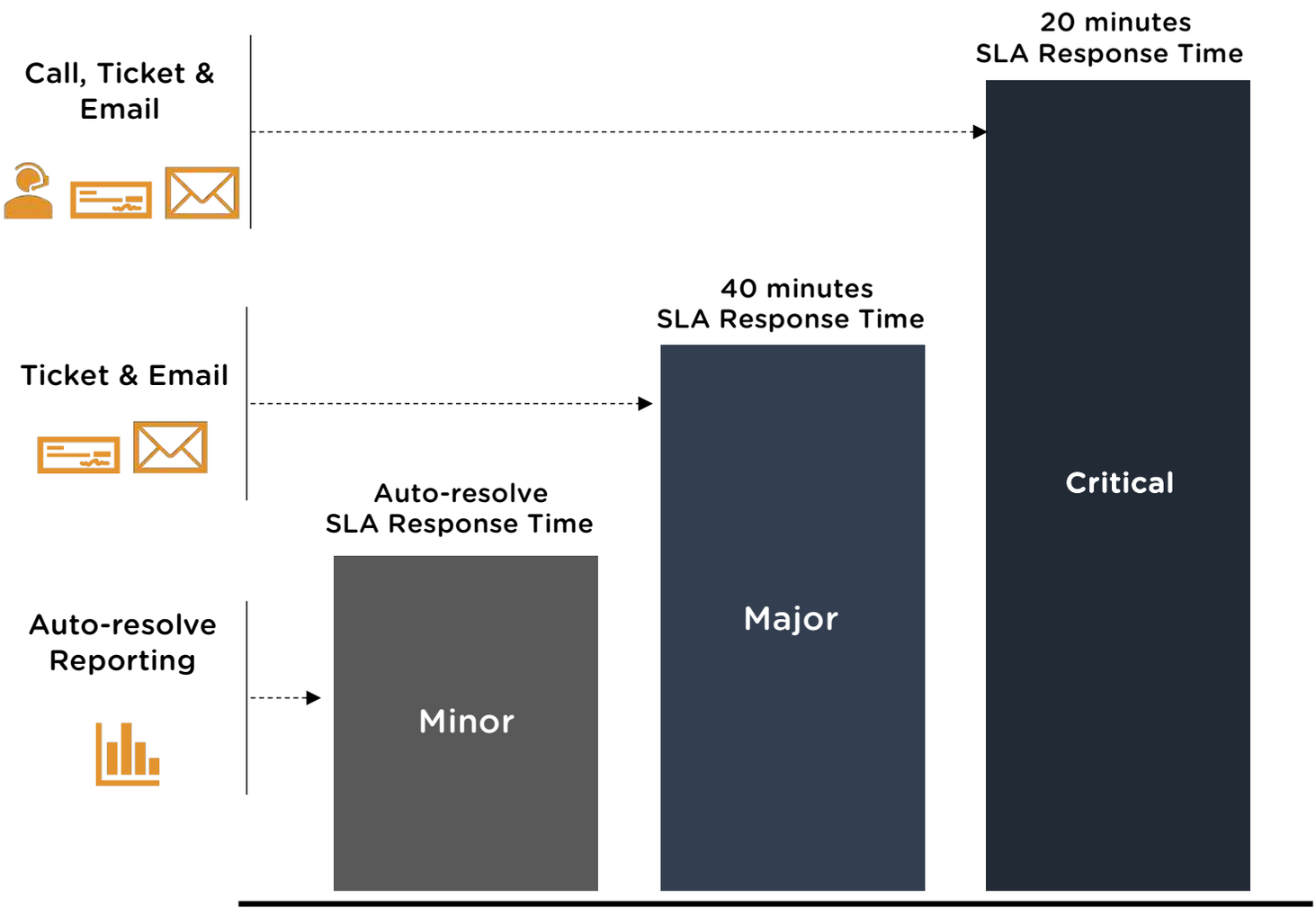
3. UNCOVER New Patterns, Tactics, Techniques and Procedures (TTP)
Complex TTP discovery and campaign tracking

4. INFORM & ENRICH Analytics
Enrich hunting procedures library, automate detection and update rules and policies

CORRELATION TUNING PROCESS

CHANGE REQUEST	Improvement, Threat Hunting, Analyst, Client, Infrastructure update, etc.
ANALYZE PLAUSIBILITY	False Positive Ratio Study and tuning to achieve acceptable rate of accuracy
BASELINE RULE	Rule baselined and studied – Case updated with analyst remarks
REVIEW	Review of the rule by a Sr. Analyst for approval.
LIVE	Activation of the rule and client specifics policies applied.

SERVICE LEVEL AGREEMENT



Fully Customizable through escalation policies
Automatically Implemented into correlation rules

Typical Attack Vectors by criticality

MINOR

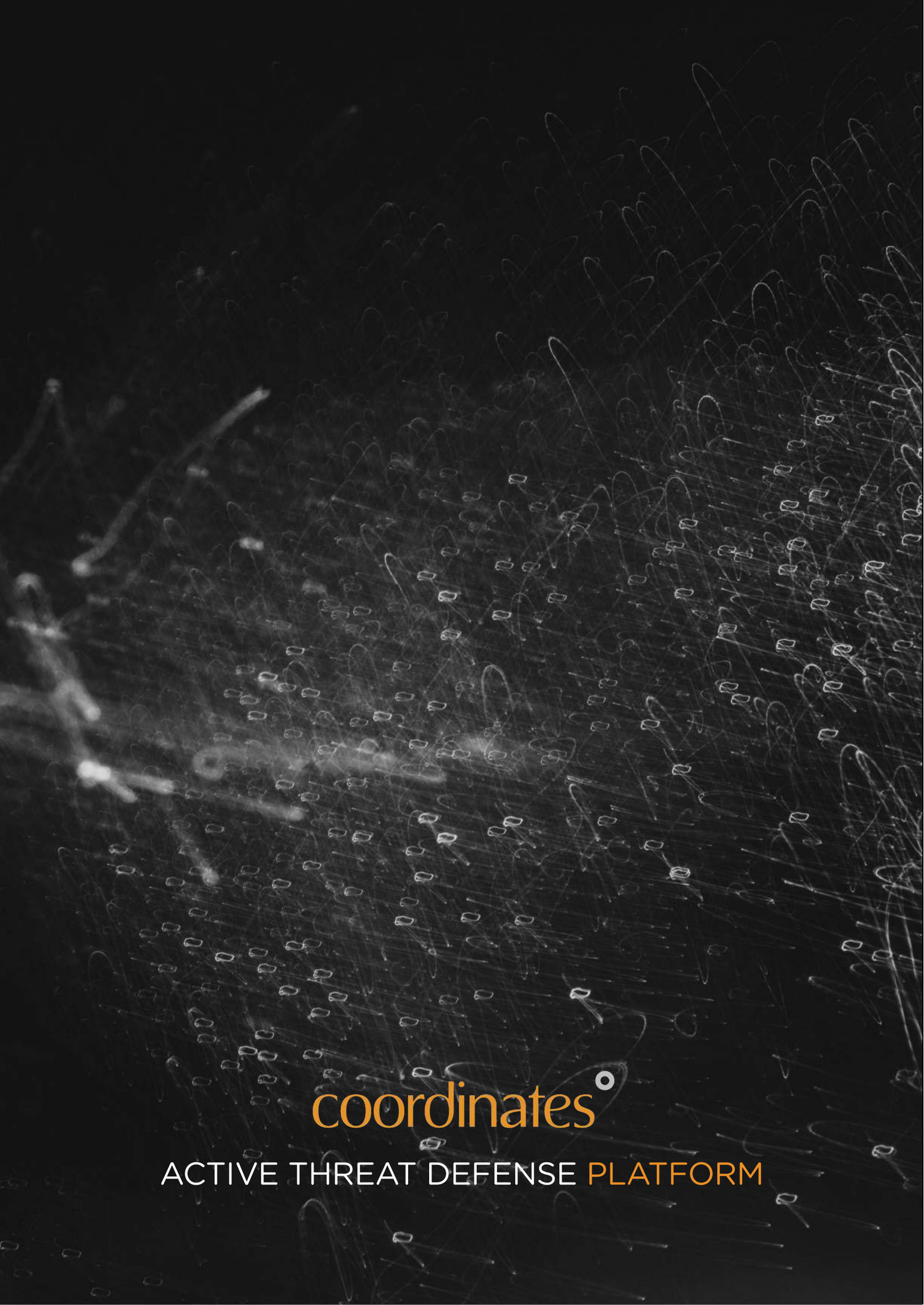
Inbound Web Attack
Exploit Kit - Malware
Adware/PUA/PUP
External/Inbound Port Scan
External/Inbound Vulnerability Scan
Malicious/Suspicious Email Attachments

MAJOR

External & Inbound Exploit
Internal/Outbound Port Scan
External & Inbound Vulnerability Scan
Policy Violation
Exploit Kit - Malware
Brute Force Attacks/ Multiple Login Failures
Inbound Web Attack
Scheduled Vulnerability Scan/Pen Test
Pre-Compromise Malware

CRITICAL

Command Execution
Credential Theft
Internal/Outbound Web Attack
Internal/Outbound Vulnerability Scan
DoS Internal/Inbound/Outbound
Internal Exploit


coordinates
ACTIVE THREAT DEFENSE PLATFORM