Building Great Customer Experiences

تقدم
TAQADOM
Specialized Solutions

Taqadom Specialized Solutions

Taqadom Specialized Solutions

2003

Established

Quick turn around time with Excellent Customer Experience (Achieving Goals)

Customer Services Company

6

Presence in 6 countries

7

Supporting 7 Languages

4

Worldwide NOC/SOC Centres

100

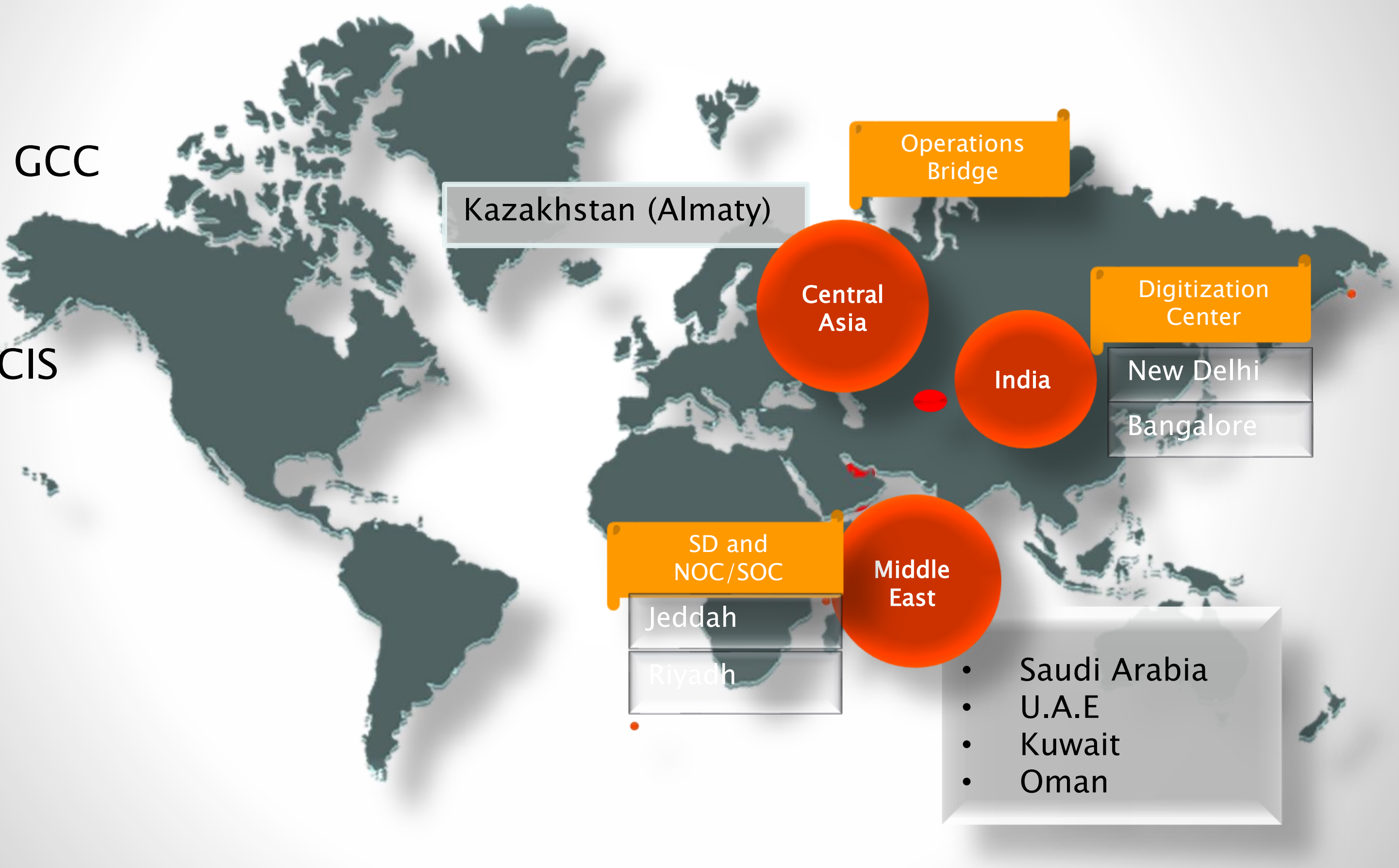
100’s of IT projects delivered

Global Presence and Delivery Centers

2009 Saudi Arabia & GCC

2016 Kazakhstan & CIS

2003 India & Apac



Kazakhstan (Almaty)

Operations Bridge

Central Asia

India

Digitization Center

- New Delhi
- Bangalore

SD and NOC/SOC

- Jeddah
- Riyadh

Middle East

- Saudi Arabia
- U.A.E
- Kuwait
- Oman

40% Cost Arbitrage

Skills Skilled Resources

20% Automation

Selected Customers (BFSI, Construction, Food, Telecom, IT, Manufacturing, Electronics)

IsDB
البنك الإسلامي للتنمية
Islamic Development Bank

KERRY
FOODS

indra

شركة الفهد

مصرف الهلال
al hilal bank

ferrovial

I CAD
المقاولون المبتكرون للمعايير المتطورة
INNOVATIVE CONTRACTORS for ADVANCED DIMENSIONS

T.G.I.
FRiDAY'S

الاتصالات المتكاملة
INTEGRATED TELECOM

AC
شركة المعدات المكملة للطائرات المحدودة
Aircraft Accessories & Components Co. Ltd.

WASATAH
CAPITAL
وساطة كابيتال

hp

itfc
International
Islamic Trade
Finance Corporation

AATCO

مجموعة شاهيني
SHAHINI GROUP

JEDجدة
مطار الملك عبدالعزيز الدولي
King Abdulaziz International Airport

الكترو
عالم الأجهزة المنزلية
Electro
World of Home Appliances

Spectrum of Skill Available

Applications	ORACLE APPLICATIONS Microsoft Dynamics TEMENOS THE BANKING SOFTWARE COMPANY MISYS FINANCIAL SOFTWARE SWIFT SAP Quest Lotus Notes
Middleware and Database	ORACLE FUSION MIDDLEWARE GOLDENGATE IBM WebSphere ORACLE Microsoft SQL Server ORACLE WEBLOGIC JBoss by Red Hat
Operating Systems and Virtualization	SOLARIS Windows vmware redhat openstack IBM AIX Microsoft Hyper-V ORACLE LINUX ORACLE VM suse A NOVELL COMPANY Red Hat
Hardware	hp invent DELL Sun microsystems EMC2 where information lives NetApp HITACHI Inspire the Next IBM radware Cisco Systems ORACLE Barracuda
Security	splunk> ManageEngine cisco FORTINET paloalto NETWORKS Symantec Trustwave Security begins with Trust F-Secure DeviceLock Proactive Endpoint Security ONDMARC KnowBe4 Human error. Conquered. Klassify ERICOM Be Connected. Be Secure senhasegura ilantus The Cloud Identity People CODETWO SECUDRIVE Data Protection beyond Encryption kaspersky KACE

What We Do

Summary

What We Do (Summary)

Automation Enabled Managed IT Services

- Automation for Monitoring and management software’s
- Platform support (Win,Linux, AIX)
- Network & Security management and automatio
- Data Centre support and automation
- Infrastructure support services (backup, system, networks, Databases, Virtualization (**OVM**, Vmware, VDI, HyperV)

1

End User Support Services- Automation

•State of art and **Automated** Service desk management (Auto Phone, ticket support)
•Proactive incident and problem management
•CMDB management and support (inventory control and vendor analysis)
•End user Device management (Lpt, mobile ,sensors)- Onsite/Offsite
•ITIL implementation

2

Automation, AI and IOT services

•Service catalogue automation
•Automation for routine tasks and activities
•Robotics Process Automation (implementation and support)
•Chatbot implementation
•Managing IOT sensors (entire lifecycle)
•BI

3

Security Services

•Incident detect and response SOC (Opex and Capex Model) - SIEM
•Risk assessment and mitigation
•ISO 27001 implementation
•Swift compliance and monitoring services
•Audit and Advisory Services

4

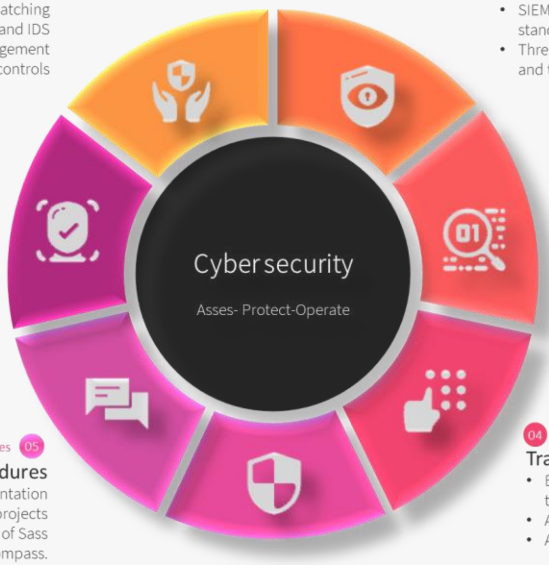
Development- Python, java, UI, C++

Managed Security Services

IT Security

Managed Security Services Benefits

- Complete end to end management of security
- Rapid Incident Response, Event Investigation and forensic 24*7
- 24*7 proactive incident security monitoring and reporting
- Huge cost advantage with Experienced security technical resources
- Effciently Manage organization Risk & Compliance through Experienced Auditors and technical implementors for ISO 27001



Across Platforms 01

Managed Security

- End point security
- OS hardening and patching
- Penetration testing and IDS
- Access management
- Security controls

02 24*7

SOC/SIEM

- 24*7 Incident detection and recording
- SIEM configurations and standardisation
- Threat correlations, segregation and trend analysis

03 Regulatory

Compliance and Audits

- ISO 27001 implementation
- Swift compliance implementation
- Audit and advisory

04 Training

Training and Awareness

- End user and Admin security trainings
- Awareness sessions and handouts
- Awareness compliance

Policies 05

Policies and Procedures

- ISO27001 implementation
- responsive web design projects that harnesses the power of Sass and Compass.

Risks 06

Risk Assessment

- Business and application risk
- Risk assessment and mitigation
- Vulnerability assessment

Security Services

Cyber security
Asses- Protect-Operate

Across Platforms 01

Managed Security

- End point security
- OS hardening and patching
- Penetration testing and IDS
- Access management
- Security controls

02 24*7

SOC/SIEM

- 24*7 Incident detection and recording
- SIEM configurations and standardisation
- Threat correlations, segregation and trend analysis

03 Regulatory

Compliance and Audits

- ISO 27001 implementation
- Swift compliance implementation
- Audit and advisory

04 Training

Training and Awareness

- End user and Admin security trainings
- Awareness sessions and handouts
- Awareness compliance

Policies 05

Policies and Procedures

- ISO27001 implementation
- responsive web design projects that harnesses the power of Sass and Compass.

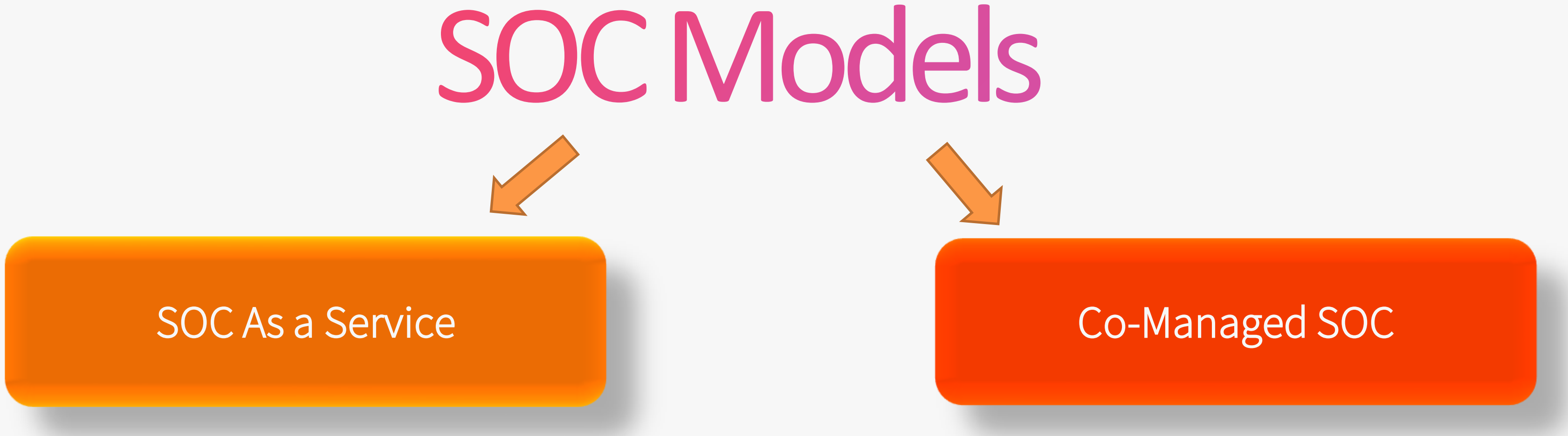
Risks 06

Risk Assessment

- Business and application risk
- Risk assessment and mitigation
- Vulnerability assessment

Security (SOC)

Our managed security operation service offers reliable security and flexibility to cater both operational and capex models.
Even having Flexibility of only opting for Off peak hours/single shift too



SOC Models

SOC As a Service

1. Go live within a week through SOC
2. Incident monitoring and response
3. Dedicated trained security experts
4. Save capital with our best-managed security solutions

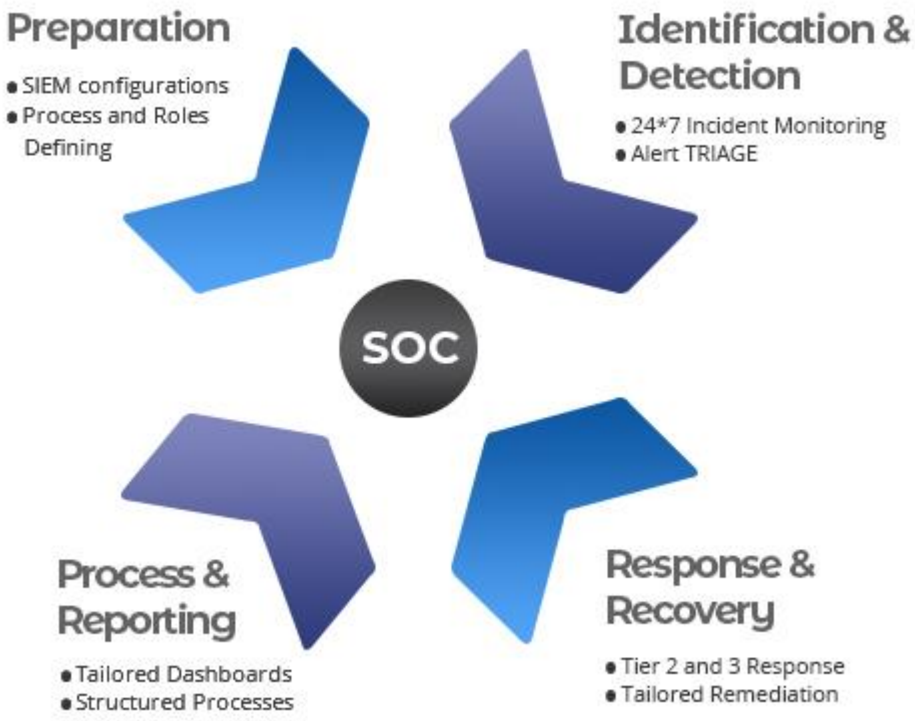
Co-Managed SOC

1. Maximize the value of SIEM
2. Customized and advance SOC proficiency
3. Enhanced operation effectiveness with our best-proven processes
4. Dedicated trained security experts

تقدم
TAQADOM
Specialized Solutions

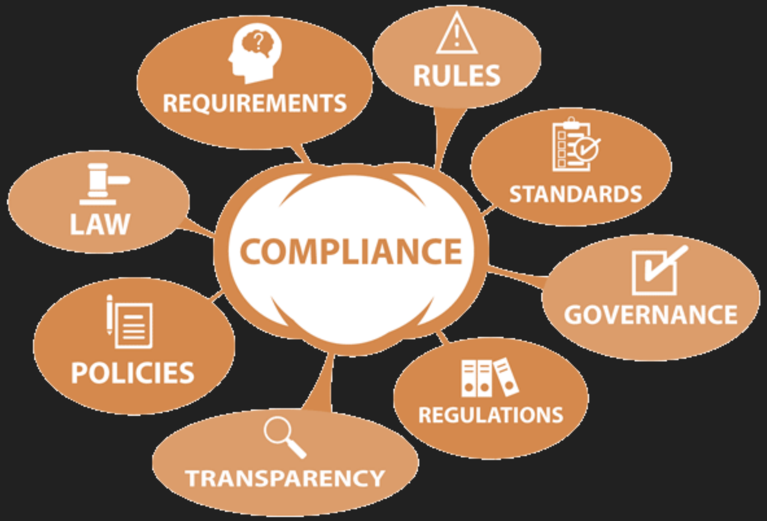
Security Monitoring

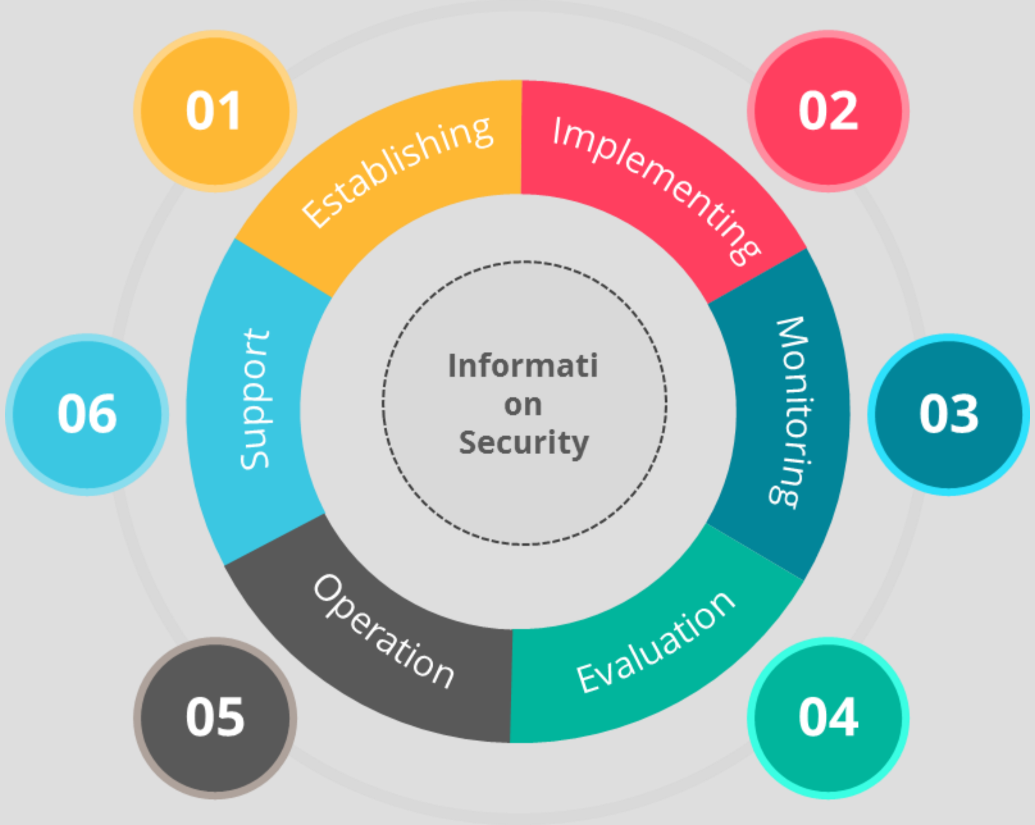
Limited access



Alerting · Escalation · Coordination · Analysis · Docs · Reports

1. 24*7 integrated monitoring of all components and global threats
2. Threat correlations, segregation and trend analysis
3. Well established and documented procedures
4. Reporting and Coordinating security vulnerability fixes
5. Live dashboard with threat metering


REQUIREMENTS
RULES
LAW
COMPLIANCE
STANDARDS
GOVERNANCE
POLICIES
REGULATIONS
TRANSPARENCY



تقدم
TAQADOM
Specialized Solutions

Security Compliance

PCI/SWIFT

- Analysing and Implementing swift compliance requirements
- Helping organizations to achieve compliance
- 24*7 Monitoring of PCI/swift environment
- Simplifying access management
- Providing quick technical fixes and suggestions

ISO 27001 and Trainings

ISO 27001

- Analyse business needs and establish ISMS framework
- Systematically implement ISMS processes
- Simplifying and reducing risks
- Measure security performance and audits
- Ensure continual improvement of ISMS
- Security Trainings (End users and Administrators)

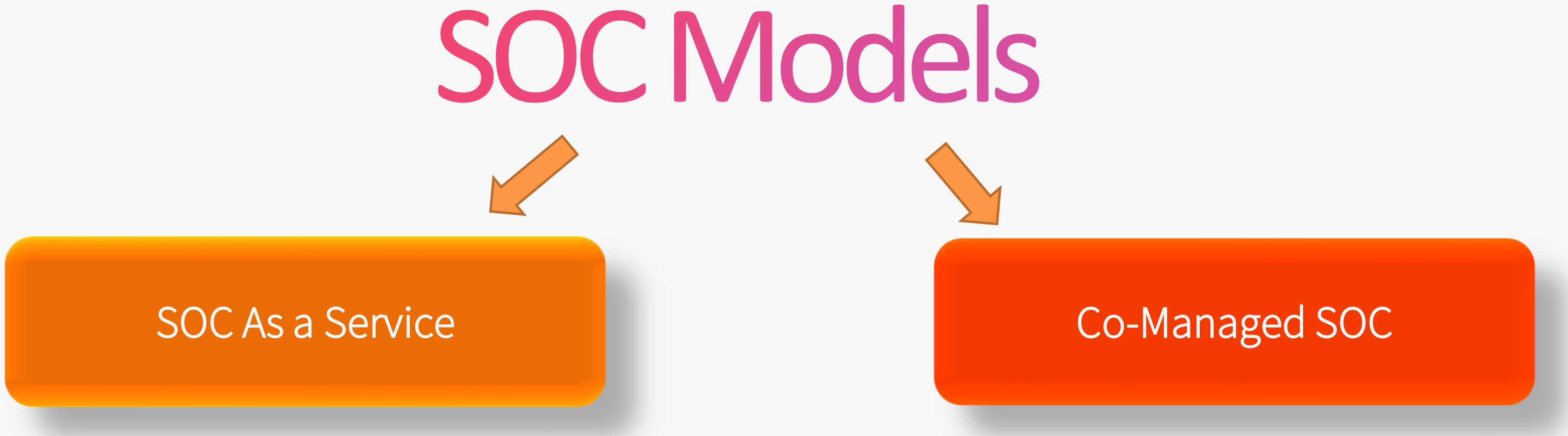
SOC Services

Challenges

- **Lack the in-house capabilities** required to keep pace with changing business demands, compliance mandates, and emerging threats for strategic implementation of new IT security solutions.
- **Tool capabilities or configuration-** Don’t have the capabilities to effectively monitor and manage the security infrastructure to ensure optimal utilization of **current assets**.
- Stringent **processes** are not in place if it is then not followed or audited
- In-house IT staffs spend far too much time on **day- to-day operational** security issues versus new strategic projects.
- **Reactive**, rather than proactive, approach to mitigating risk and minimizing data loss and downtime.
- Vulnerabilities and updates missing

What we offer

Our managed security operation service offers reliable security and flexibility to cater both operational and capex models.
Even having Flexibility of only opting for Off peak hours/single shift too



SOC As a Service

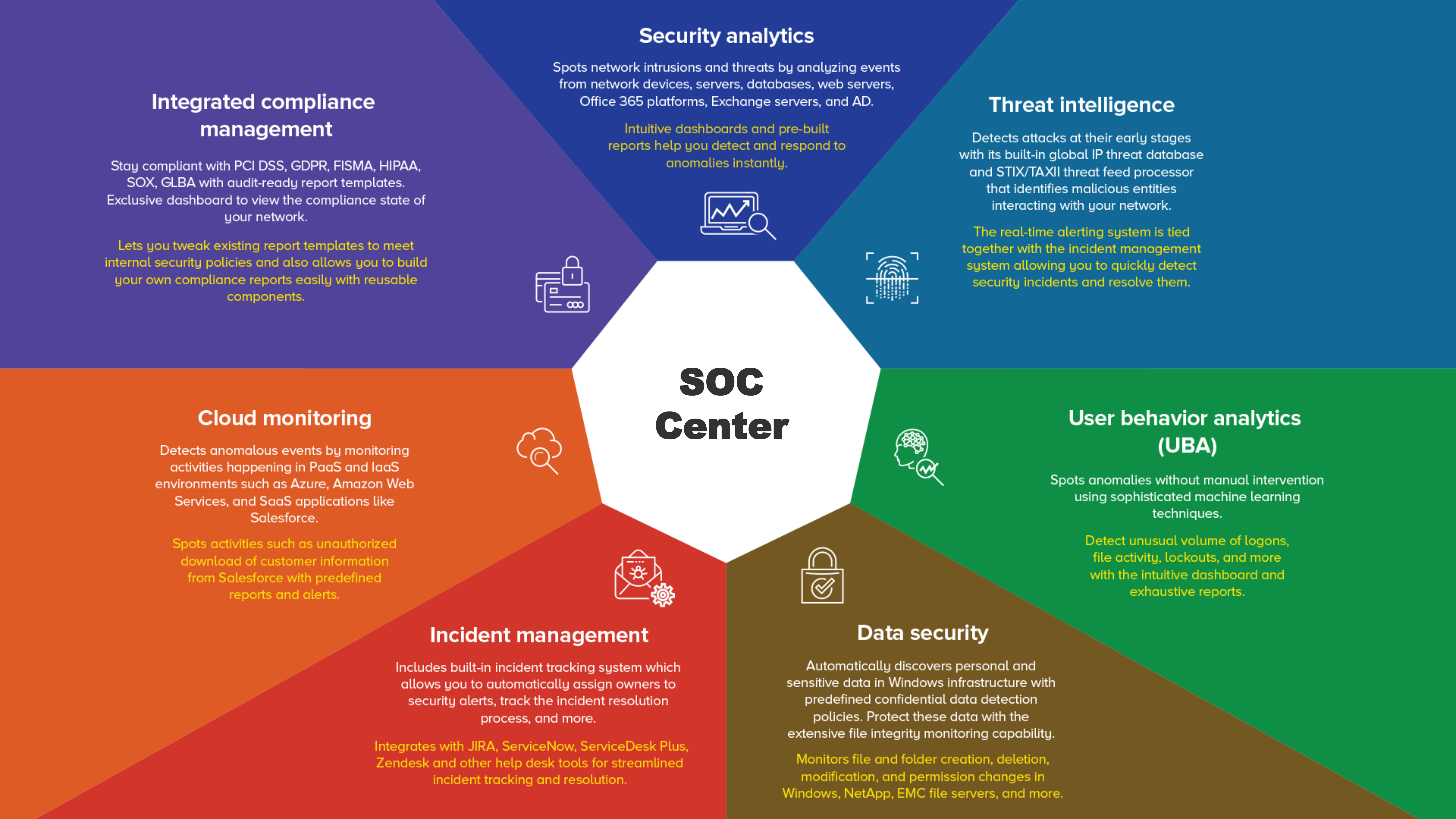
1. Go live within a week through SOC
2. SIEM bundled
3. Incident monitoring and response
4. Dedicated trained security experts
5. Processes

Co-Managed SOC

1. Maximize the value of SIEM
2. Customized and advance SOC proficiency
3. Enhanced operation effectiveness with our best-proven processes
4. Dedicated trained security experts

تقدم
TAQADOM
Specialized Solutions

What we do in SOC



SOC Center

Integrated compliance management

Stay compliant with PCI DSS, GDPR, FISMA, HIPAA, SOX, GLBA with audit-ready report templates. Exclusive dashboard to view the compliance state of your network.

Lets you tweak existing report templates to meet internal security policies and also allows you to build your own compliance reports easily with reusable components.

Security analytics

Spots network intrusions and threats by analyzing events from network devices, servers, databases, web servers, Office 365 platforms, Exchange servers, and AD.

Intuitive dashboards and pre-built reports help you detect and respond to anomalies instantly.

Threat intelligence

Detects attacks at their early stages with its built-in global IP threat database and STIX/TAXII threat feed processor that identifies malicious entities interacting with your network.

The real-time alerting system is tied together with the incident management system allowing you to quickly detect security incidents and resolve them.

Cloud monitoring

Detects anomalous events by monitoring activities happening in PaaS and IaaS environments such as Azure, Amazon Web Services, and SaaS applications like Salesforce.

Spots activities such as unauthorized download of customer information from Salesforce with predefined reports and alerts.

User behavior analytics (UBA)

Spots anomalies without manual intervention using sophisticated machine learning techniques.

Detect unusual volume of logons, file activity, lockouts, and more with the intuitive dashboard and exhaustive reports.

Incident management

Includes built-in incident tracking system which allows you to automatically assign owners to security alerts, track the incident resolution process, and more.

Integrates with JIRA, ServiceNow, ServiceDesk Plus, Zendesk and other help desk tools for streamlined incident tracking and resolution.

Data security

Automatically discovers personal and sensitive data in Windows infrastructure with predefined confidential data detection policies. Protect these data with the extensive file integrity monitoring capability.

Monitors file and folder creation, deletion, modification, and permission changes in Windows, NetApp, EMC file servers, and more.

Incident management Lifecycle

تقدم
TAQADOM
Specialized Solutions

1.Preparation

ONE

Benchmark and Bring speed

- SIEM configurations
- Process and Roles defining

TWO

Detect Incidents before it occurs

24*7 Proactive Incident monitoring and tracking

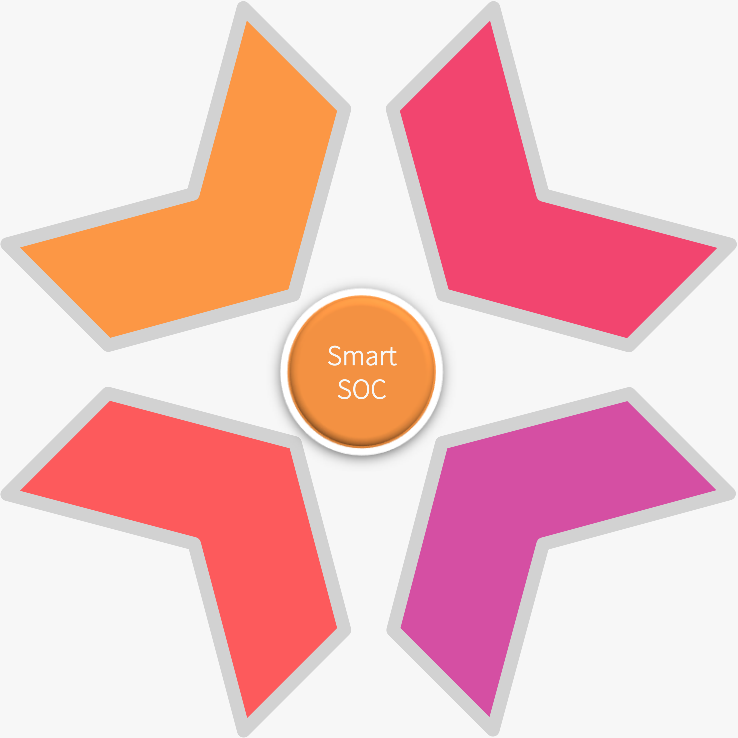
dentification & Detection

lifecycle

SEVEN

Global Threats

Threat hunting and providing recommended fixes



THREE

Filter Incidents

Incident correlations, categorizations and trend analysis

SIX

Tier 2 and 3 response

Incident response and resolution

FOUR

Act Quickly

Incident Detection and escalations

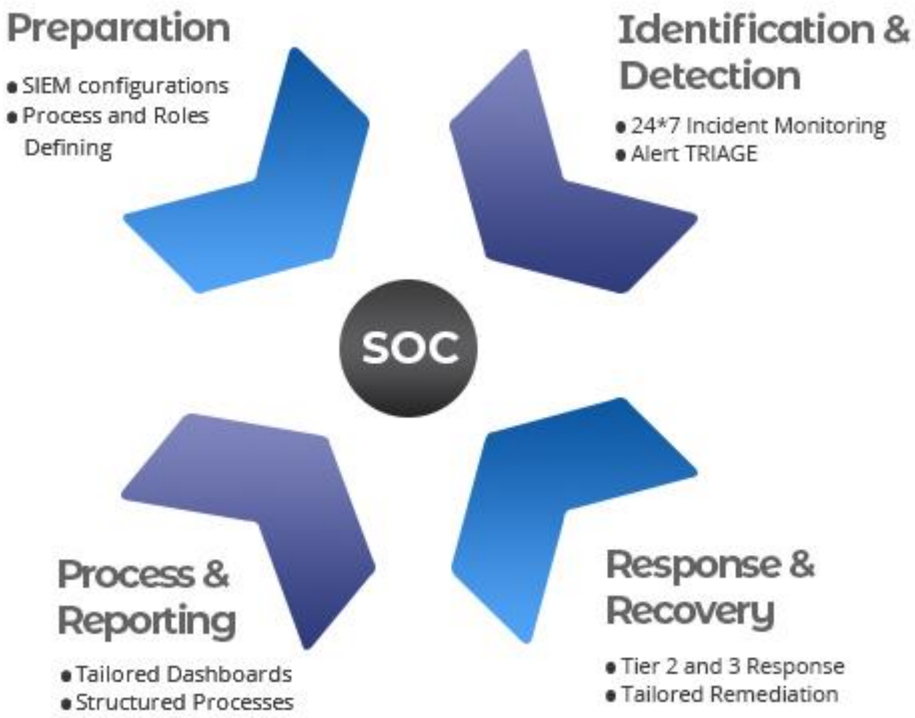
3.Response

FIVE

Live Dashboard

Reporting and Coordinating security vulnerability fixes

Incident Monitoring



Preparation

- SIEM configurations
- Process and Roles Defining

Identification & Detection

- 24*7 Incident Monitoring
- Alert TRIAGE

SOC

Process & Reporting

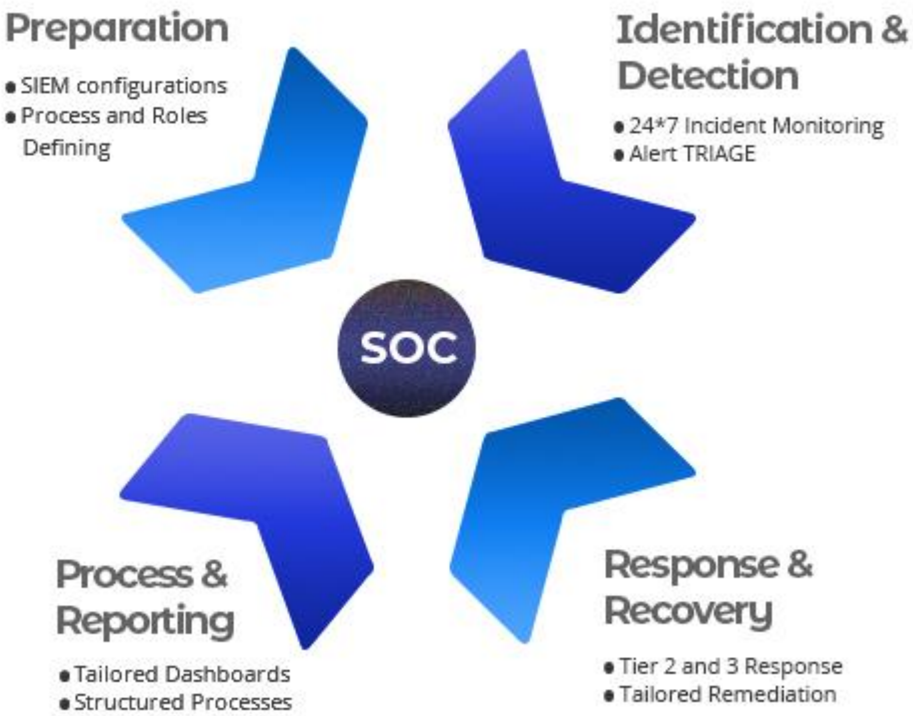
- Tailored Dashboards
- Structured Processes

Response & Recovery

- Tier 2 and 3 Response
- Tailored Remediation

Log Categorize Analyze Coordinate Escalate Reports

1. 24*7 integrated monitoring of all components and global threats
2. Threat correlations, segregation and trend analysis
3. Well established and documented procedures
4. Reporting and Coordinating security vulnerability fixes
5. Live dashboard with threat metering



Preparation

- SIEM configurations
- Process and Roles Defining

Identification & Detection

- 24*7 Incident Monitoring
- Alert TRIAGE

SOC

Process & Reporting

- Tailored Dashboards
- Structured Processes

Response & Recovery

- Tier 2 and 3 Response
- Tailored Remediation

Incident Response

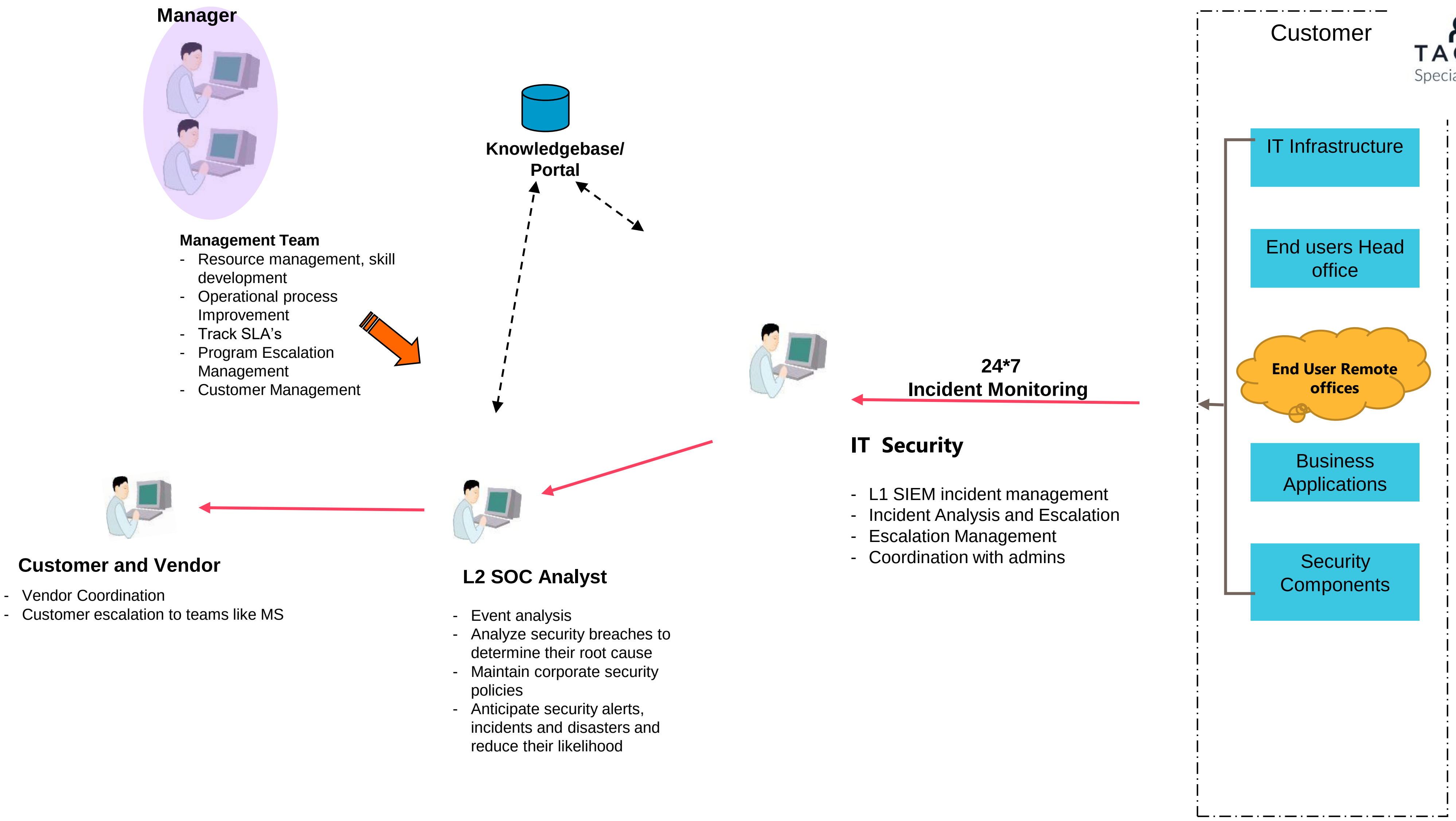
L2 and L3 Teams

Investigation · Analysis · Guidance · Hunting · Fixes · Review

1. Respond to security incidents as per the categorization and prioritization
2. Incident investigation and analysis
3. Active guidance on containment, eradication and remediation
4. Identifying vulnerabilities and fixing patches with recommended solution
5. Threat hunting and fixes
6. Review current security trends and incident response procedures
7. Prepare detailed root cause analysis wherever applicable along with remediation plan

Integrated Incident Management Flow

تقدم
TAQADOM
Specialized Solutions



Manager

Management Team
- Resource management, skill development
- Operational process Improvement
- Track SLA's
- Program Escalation Management
- Customer Management

Knowledgebase/ Portal

24*7 Incident Monitoring

IT Security
- L1 SIEM incident management
- Incident Analysis and Escalation
- Escalation Management
- Coordination with admins

L2 SOC Analyst
- Event analysis
- Analyze security breaches to determine their root cause
- Maintain corporate security policies
- Anticipate security alerts, incidents and disasters and reduce their likelihood

Customer and Vendor
- Vendor Coordination
- Customer escalation to teams like MS

Customer
- IT Infrastructure
- End users Head office
- **End User Remote offices**
- Business Applications
- Security Components

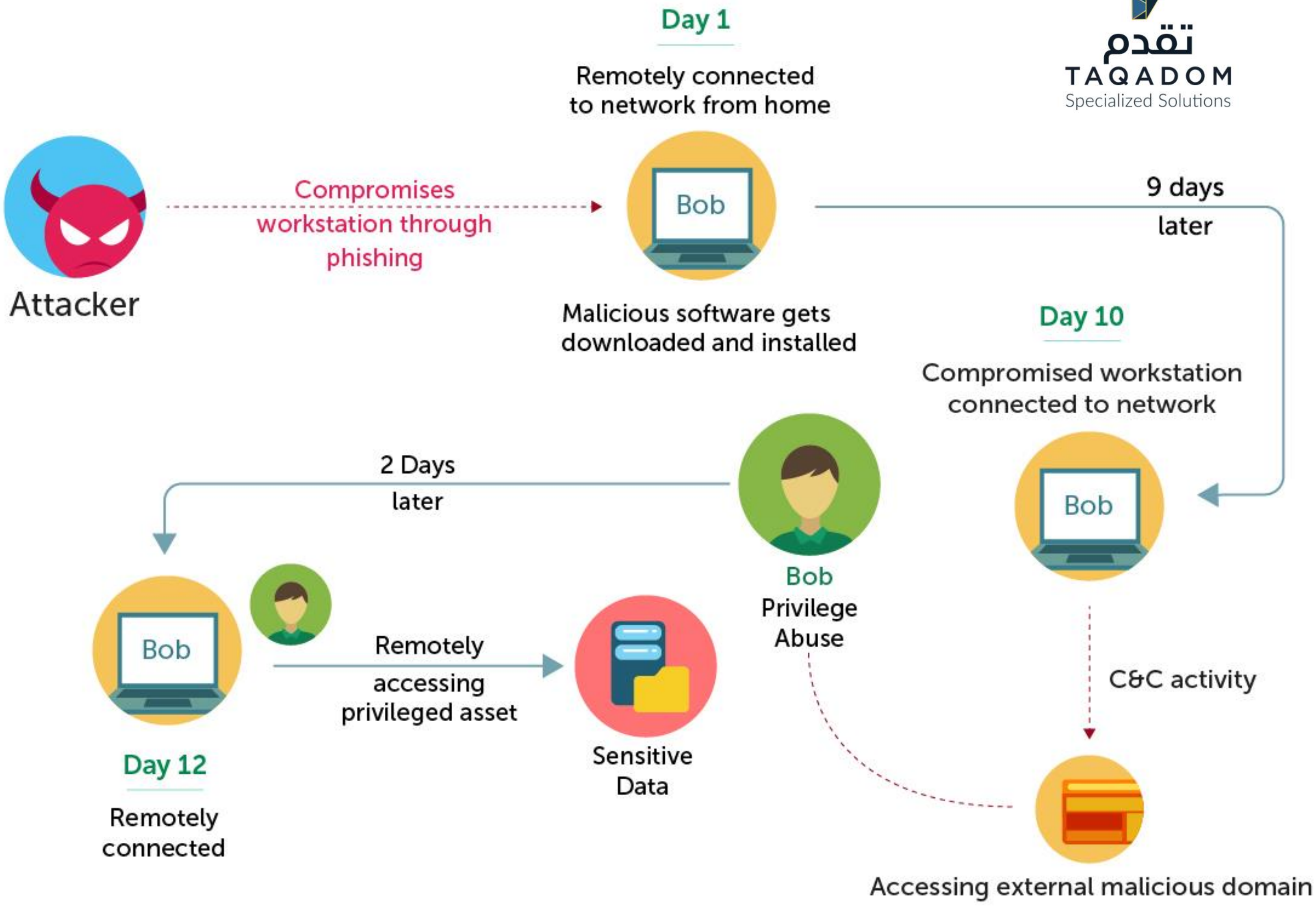
User and entity behavior analytics

User and entity behavior analytics

- Machine learning based anomaly detection
- **Anomalous behavior detection:** Based on time, pattern, or count
- **Risk score based threat prioritization:** Determine degree of risk posed by an identified threat
- Add high risk users and entities to a watchlist
- **Threat corroboration:** Identify indicators of common threats (account compromise, data exfiltration, and more)

Use case:

Compromised workstation & data exfiltration attempt


Attacker
Compromises workstation through phishing
Day 1
Remotely connected to network from home
Bob
Malicious software gets downloaded and installed
9 days later
Day 10
Compromised workstation connected to network
Bob
C&C activity
Accessing external malicious domain
Bob
Privilege Abuse
2 Days later
Bob
Day 12
Remotely connected
Remotely accessing privileged asset
Sensitive Data

How Do we Manage Logs

Warna - Multipurpose PowerPoint Template

تقدم
TAQADOM
Specialized Solutions

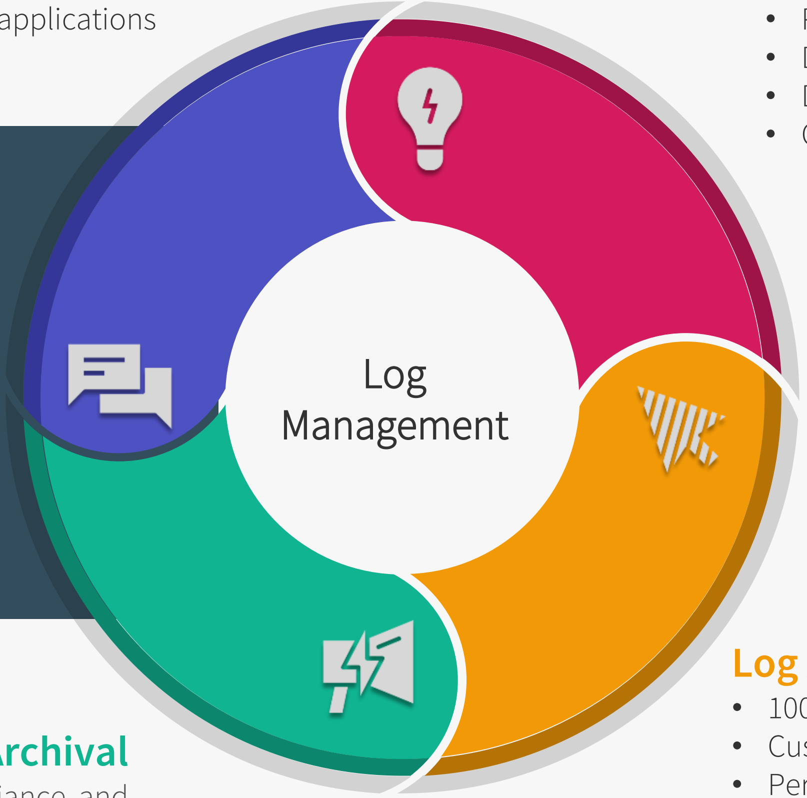
Log Collection

- agent-based and agentless methods of log collection
- 600+ log sources
- Logs from custom devices, in-house applications

Log Correlation

- Predefined correlation rules
- Detect attack patterns across devices.
- Detect anomalies such as suspicious software installations
- Create Custom correlation rule builder

Log Managem ent



Log Analysis and Reports

- 1000+ reports
- Custom Reports
- Perform in-depth log forensics and search through millions of log

Log Archival

- Encrypt logs for future forensic analysis, compliance, and
- internal audits
- Default Log archive files based on polices along with compression techniques

Comprehensive Auditing

Network Devices

- Monitor firewall configurations and rule changes.
- Identify unauthorized access attempts and privilege escalations on perimeter devices.
- Detect denied connections, threats, and other anomalous incidents on your routers, switches, firewalls, and IDS/IPS devices.

Critical Applications

- Automate the import of application log data:
- Secure IIS and Apache web servers:
- Audit Microsoft SQL Server and Oracle databases:
- Audit vulnerability scanners and threat intelligence solutions:

Multiple Environments

- Multiple different Environments

Threat Intelligence

تقدم
TAQADOM
Specialized Solutions

Threat Feeds

•Database of over 600 million malicious IPs, URLs, and domains, updated dynamically.
•Multiple open source and STIX/TAXII based threat feeds.
•Get real-time alerts when traffic is detected to or from suspicious IPs, URLs, and domains.

Incident Management

•Manage security incidents using the built-in incident management console.
•Automatically assign incident tickets to operators.
•Track incident tickets, use multiple views to filter tickets, and more.
•Alternatively, forward incident tickets to 3rd party SD tools

Provide Compliance Reporting

- Compliance reports for:
    - PCI DSS
    - GDPR
    - FISMA
    - HIPAA
    - GLBA
    - SOX
    - ISO 27001
- Modify existing reports or create new compliance reports to meet internal security policies.

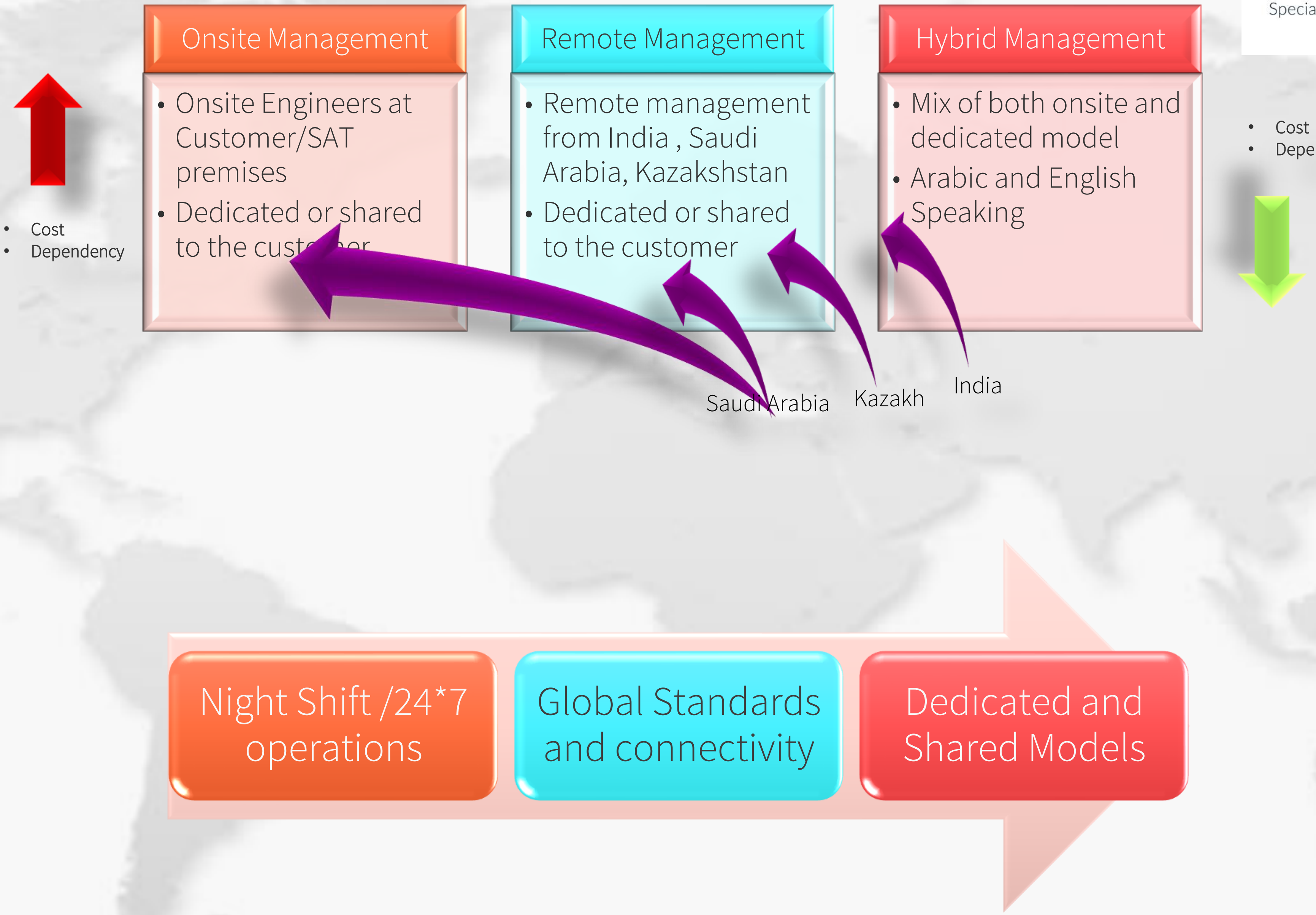
- Meet the forensic analysis and log archival requirement of most compliance policies with the powerful search feature and secure log archival capabilities.

Awards and recognitions

- ✓ Recognized in the Gartner Magic Quadrant for SIEM, for the fourth consecutive time.
- ✓ Gartner Peer Insights Customer Choice for SIEM, 2019.
- ✓ Placed as a leader in the Software Reviews Customer Experience Diamond for SIEM, 2019.

Delivery Models

تقدم
TAQADOM
Specialized Solutions



- Cost
- Dependency

Onsite Management

- Onsite Engineers at Customer/SAT premises
- Dedicated or shared to the customer

Remote Management

- Remote management from India , Saudi Arabia, Kazakhshstan
- Dedicated or shared to the customer

Hybrid Management

- Mix of both onsite and dedicated model
- Arabic and English Speaking

- Cost
- Dependency

Night Shift /24*7 operations

Global Standards and connectivity

Dedicated and Shared Models

Why SAT Microsystems

01 24* 7 Monitoring from 3 different geographies

02 Ready – SIEM, Processes and People

03 Talented resources and onsite presence

04 Low cost of operations due to offshore and shared delivery models

05 Modular based approach- Only monitoring or management or processes or tools

06 Advance Threat Intelligence

تقدم
TAQADOM
Specialized Solutions

Thank You

Achieving Customer Goals

Meeting Global standards

Automation and Robotics a key driver for cost and efficiency

01

KAZAKHSTAN

12th floor Block 3, 135 Zhybek Zholy
street Almaty 050004,
Kazakhstan
Phone– +7 727 311 2412

02

SAUDI ARABIA

Riyadh- 5, Mohamadia Building, KF Road
Jeddah – Level 7, Al Murjanah Tower, Sultan st
Phone- (+966) 12 601 7561
Mobile- +966 59 049 1974

03

U.A.E

Ras Al Khaimah, Economic Zone
United Arab Emirates
P.O.Box- 326526

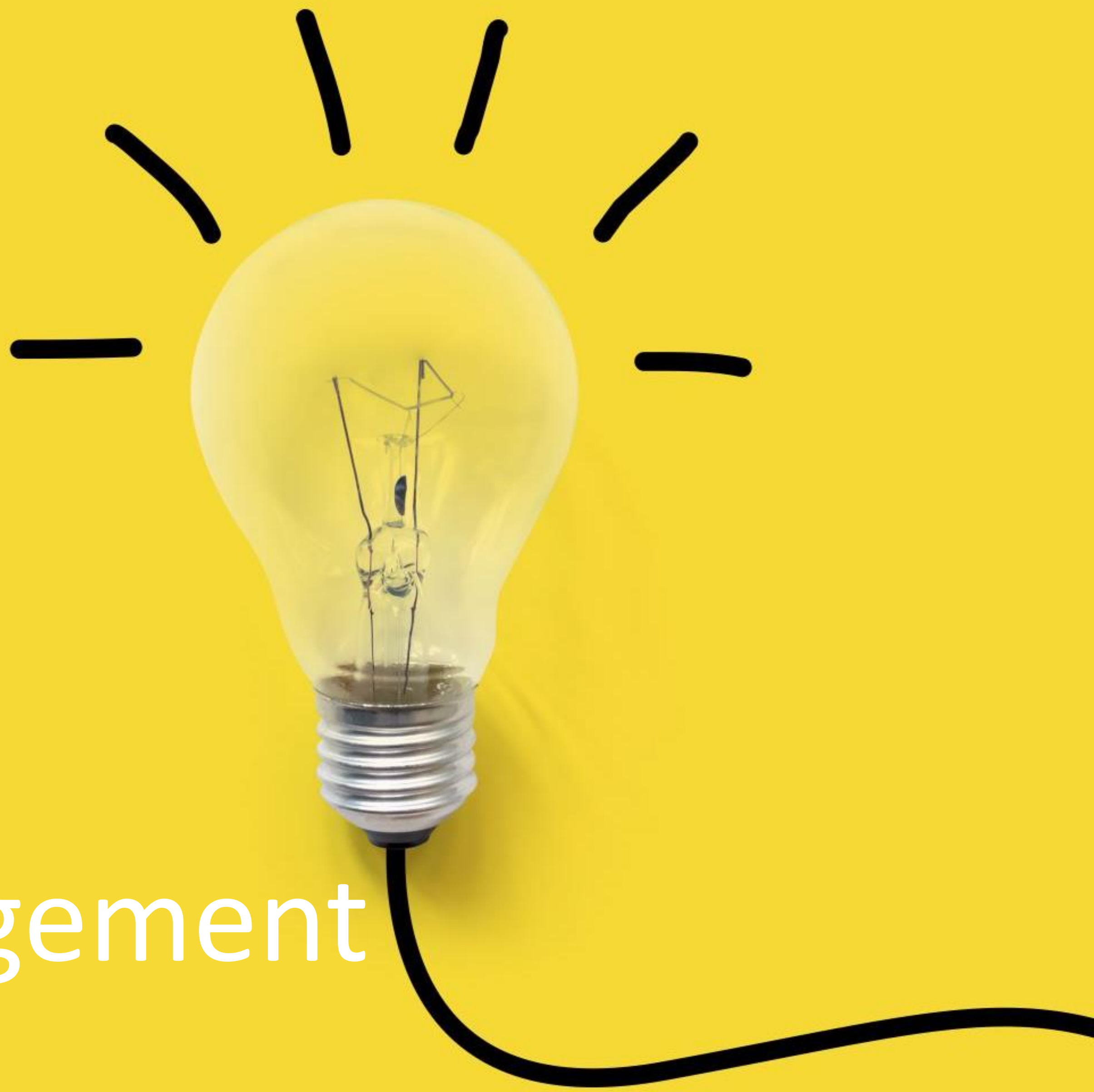
04

INDIA

5th Floor Ansal Chamber 2, Bhicaji
Cama Place
New Delhi -110029

Efficient Tool Management

- UBA
- Log Management
- Comprehensive Auditing
- Thereat Intelligence and IM
- Compliance Reporting



Cloud monitoring

Cloud environments

Get information on:

aws

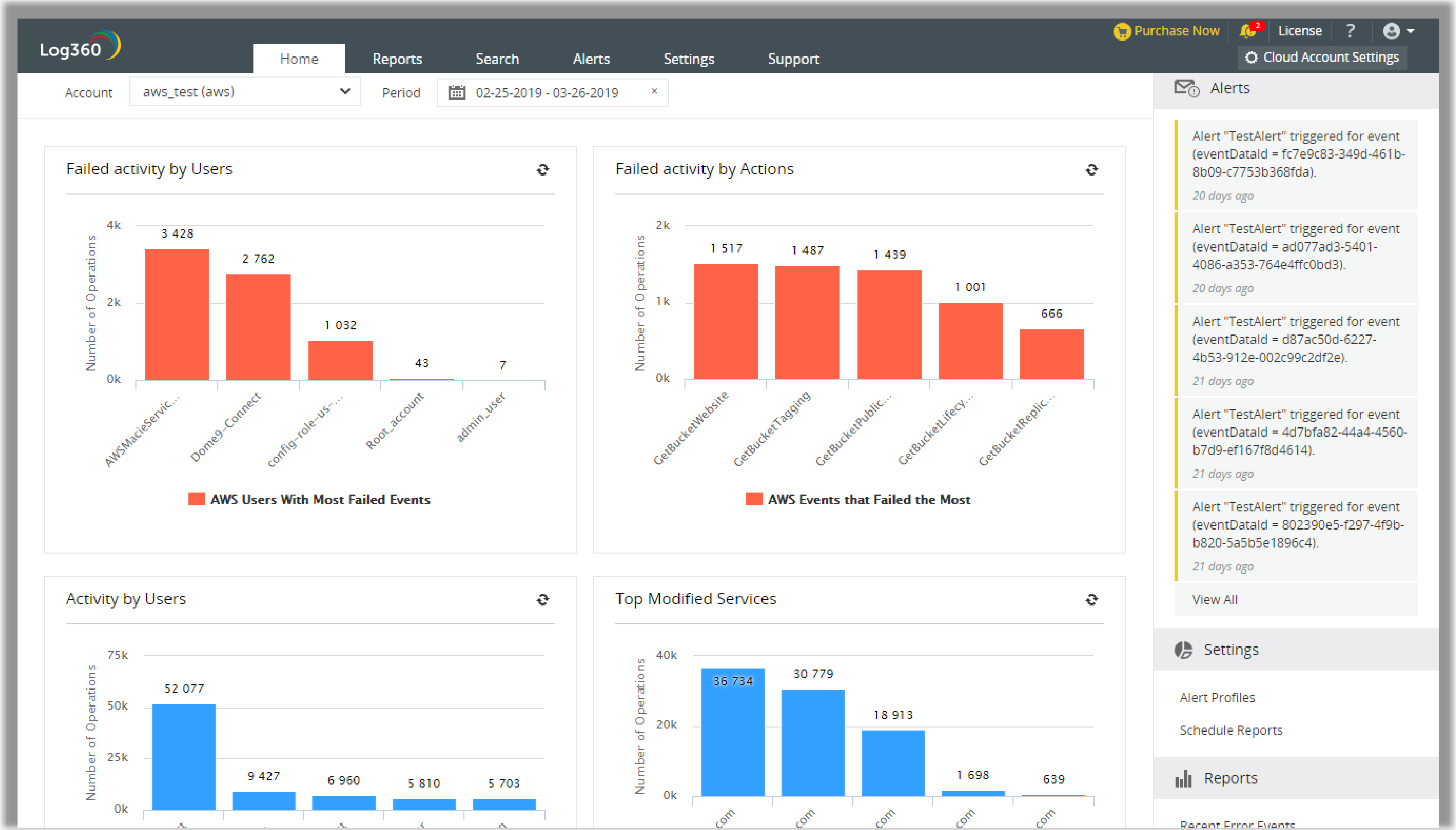
AWS: Amazon S3, Amazon EC2, Web Application Firewalls (WAF), Relational Database Service (RDS), and more

Microsoft Azure

Microsoft Azure: User activity, changes made to network security groups, virtual networks, DNS zones, databases, and more

salesforce

Salesforce: Login, report, content, and search activities



Account: aws_test (aws)

Period: 02-25-2019 - 03-26-2019

Alert "TestAlert" triggered for event (eventDataId = fc7e9c83-349d-461b-8b09-c7753b368fda).
20 days ago

Alert "TestAlert" triggered for event (eventDataId = ad077ad3-5401-4086-a353-764e4ffc0bd3).
20 days ago

Alert "TestAlert" triggered for event (eventDataId = d87ac50d-6227-4b53-912e-002c99c2df2e).
21 days ago

Alert "TestAlert" triggered for event (eventDataId = 4d7bfa82-44a4-4560-b7d9-ef167f8d4614).
21 days ago

Alert "TestAlert" triggered for event (eventDataId = 802390e5-f297-4f9b-b820-5a5b5e1896c4).
21 days ago