XcellSecure

SIEM-As-a-Service

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

www.xcellhost.cloud
+91-22-67111555
@xcellcloud

Identifies Your Assets

Protects Your assets

Detects Incidents

Responds With a plan

Recovers Normal Operations

www.xcellhost.cloud sales@xcellhost.cloud +91-8657414121

XcellSecure

What is SIEM?

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

Security Information and Event Management (SIEM) solutions use rules and statistical correlations to turn log entries, and events from security systems, into actionable information.

Detect Threats in Real Time

Manage Incident Response

Perform Forensic Investigation

Audits for Compliance Purposes

What are SIEMs Used For....?

Security Monitoring

Advanced Threat Detection

Forensics and Incident Response

Compliance Reporting and Auditing

How SIEM Works....?

Data Collection

Data Storage

Policies and Rules

Data Consolidation and Correlation

www.xcellhost.cloud sales@xcellhost.cloud +91-8657414121

XcellSecure

aiSIEM: Security Threats Vectors

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

CLOUD SECURITY

Security Monitoring of Cloud Platform and Cloud Applications

CYBER THREAT

Organizations face several threats directed towards their IT infrastructure

INSIDER THREAT

Turn-key Insider Threat Detection and Management Platform

DATA EXFILTRATION

Proactive Data Loss Prevention

FRAUD PREVENTION

Uncovering Fraud Using Security Analytics Approach

APPLICATION SECURITY

Threat and Risk Monitoring of Key Enterprise Applications

IDENTITY ACCESS

Bringing Focus and Effectiveness to IAM

PRIVILEGED ACCOUNTS

Monitoring the Keys to the Kingdom

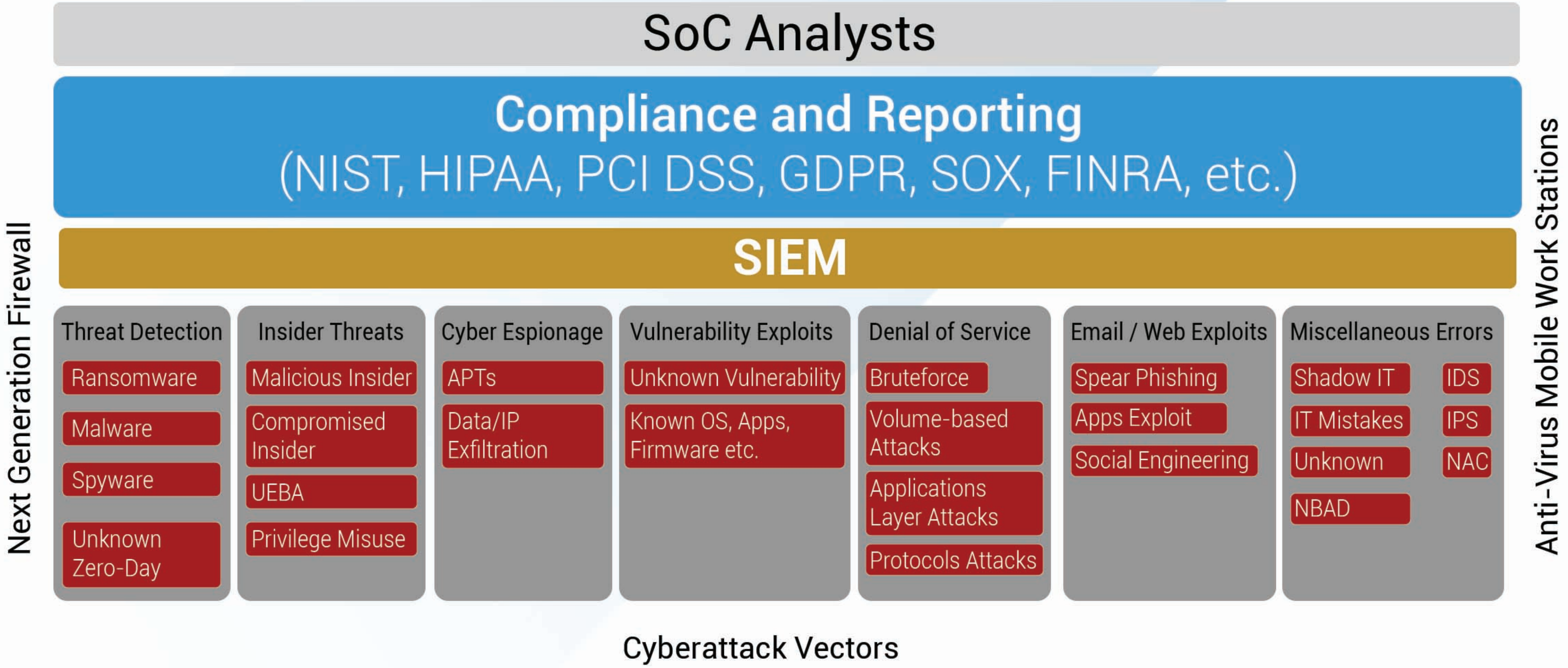
XcellSecure

aiSIEM: Security Landscape

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: seceon

Easily manage network security complexity with aiSIEM™.



SoC Analysts

Compliance and Reporting
(NIST, HIPAA, PCI DSS, GDPR, SOX, FINRA, etc.)

SIEM

Next Generation Firewall

Anti-Virus Mobile Work Stations

Threat Detection
- Ransomware
- Malware
- Spyware
- Unknown Zero-Day

Insider Threats
- Malicious Insider
- Compromised Insider
- UEBA
- Privilege Misuse

Cyber Espionage
- APTs
- Data/IP Exfiltration

Vulnerability Exploits
- Unknown Vulnerability
- Known OS, Apps, Firmware etc.

Denial of Service
- Bruteforce
- Volume-based Attacks
- Applications Layer Attacks
- Protocols Attacks

Email / Web Exploits
- Spear Phishing
- Apps Exploit
- Social Engineering

Miscellaneous Errors
- Shadow IT
- IDS
- IT Mistakes
- IPS
- Unknown
- NAC
- NBAD

Cyberattack Vectors

XcellSecure

aiSIEM: Current SIEM Market

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

Log Management

- TIBCO The Power of Now™
- BALABIT
- KeyW
- tripwire
- splunk>

SIEM

- hp eIQ networks®
- Attachmate
- solarwinds
- BlackStratus
- AlienVault
- RSA
- LogRhythm® The Security Intelligence Company
- Netsurion EventTracker Actionable Security Intelligence
- Symantec.™
- IBM®
- NetIQ®
- Trustwave®
- CLICK SECURITY
- McAfee™
- tenable network security

SAAS Logging

- sumologic
- papertrail
- logentries
- Torch
- eGestalt Analyze • Secure • Transform
- splunk>storm
- ALERTLOGIC
- loggly

XcellSecure

aiSIEM: OpenThreat Management Platform

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

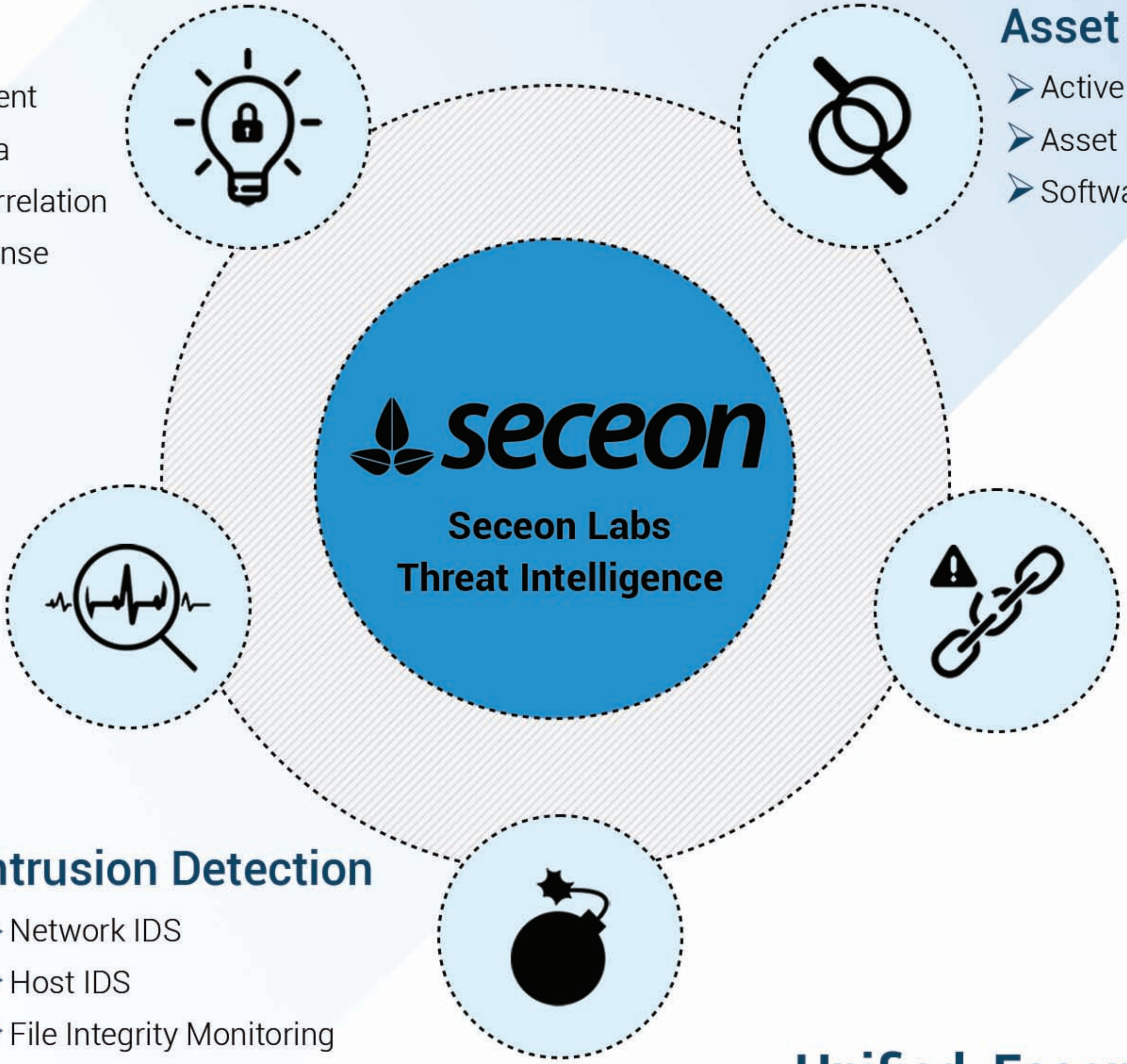
Powered by: seceon

SIEM

- Log Management
- OTX threat data
- SIEM Event Correlation
- Incident Response

Asset Discovery

- Active & Passive Network Scanning
- Asset Inventory
- Software Inventory



Network Behavioral Monitoring

- Netflow Analysis
- Service Availability Monitoring

Vulnerability Assessment

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning
- Remediation Verification

Intrusion Detection

- Network IDS
- Host IDS
- File Integrity Monitoring

Unified, Essential Security Controls

www.xcellhost.cloud   sales@xcellhost.cloud   +91-8657414121

Get the SIEM You Always Wanted

Unlimited Storage. Advanced Analytics. Automated Response.

Unified Security Management (USM) Platform

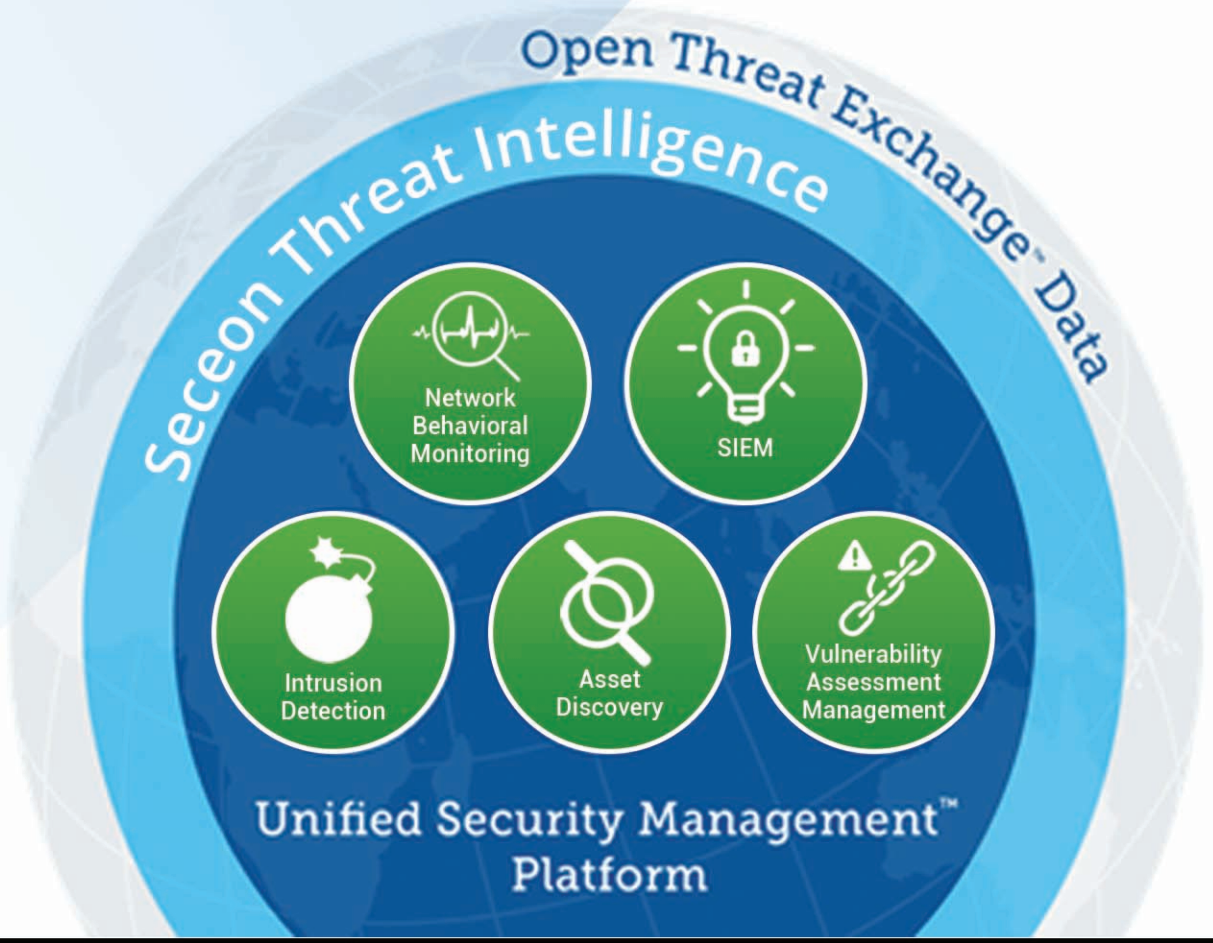
A single platform for simplified, accelerated threat detection, incident response & policy compliance

Seceon Labs Threat Intelligence

Actionable information about malicious actors, their tools, infrastructure and methods, automatically updated into the USM platform

Open Threat Exchange

The world's largest repository of threat data provides a continuous view of real time malicious activity


Open Threat Exchange™ Data
Seceon Threat Intelligence
Network Behavioral Monitoring
SIEM
Intrusion Detection
Asset Discovery
Vulnerability Assessment Management
Unified Security Management™ Platform

XcellSecure

aiSIEM: Actionable Threat Intelligence

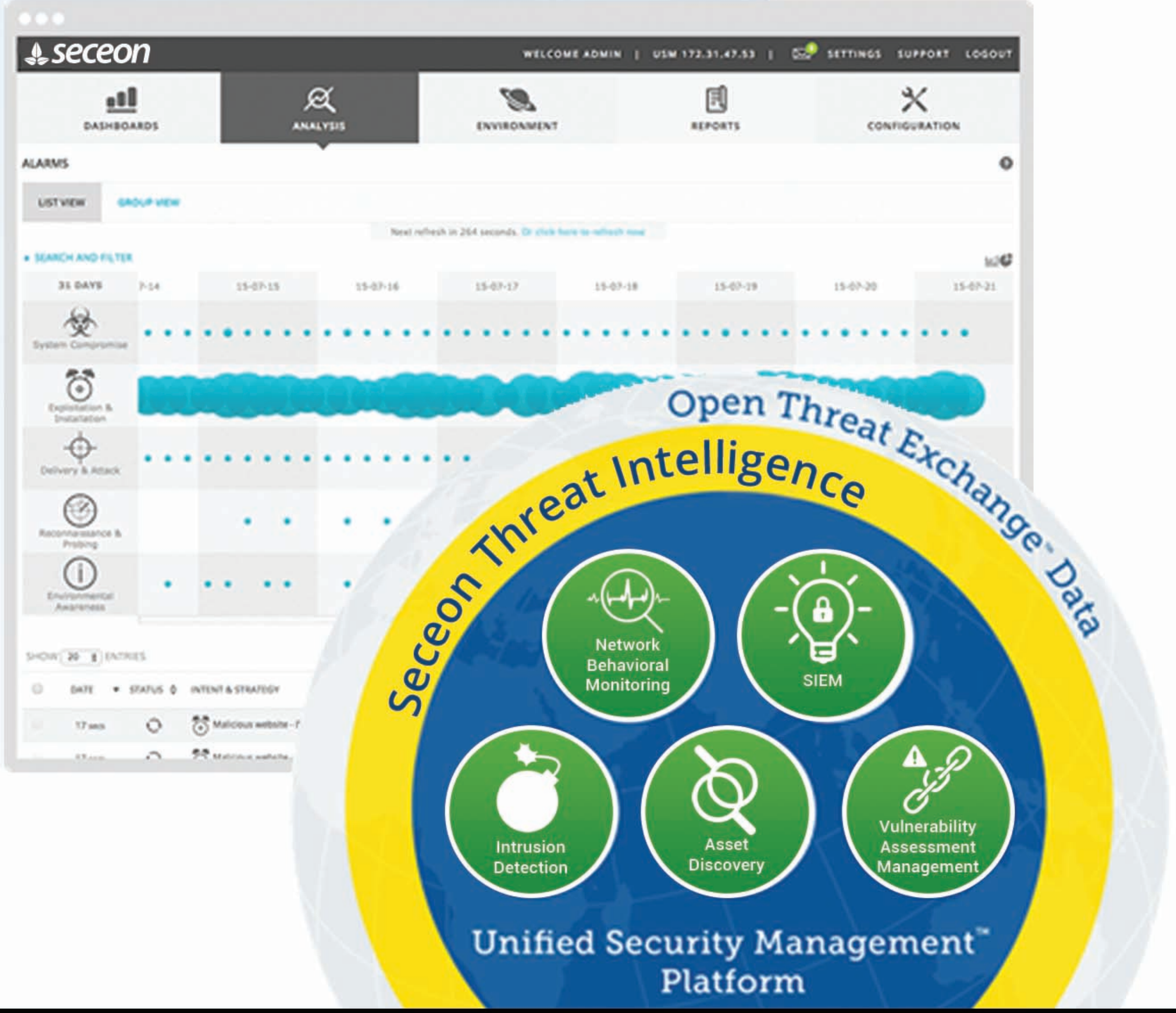
Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

Spend Your Time Responding to Threats, not Researching Them.

Automatically Detect and Prioritize Threats Through:

- Correlation Directives
- Network IDS Signatures
- Host IDS Signatures
- Asset Discovery Signatures
- Vulnerability Assessment Signatures
- Reporting Modules
- Incident Response Templates
- Data Source Plug-Ins



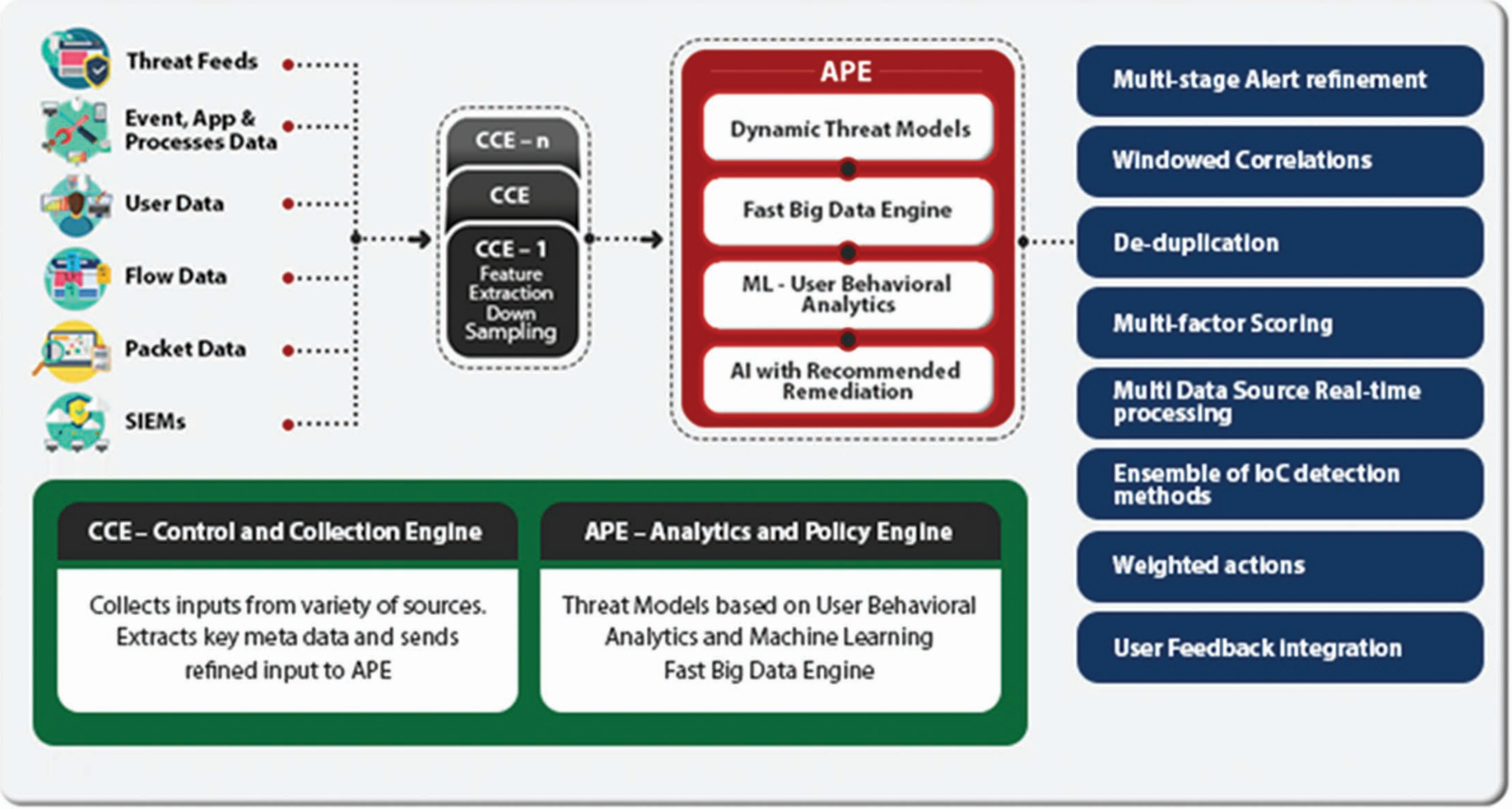
www.xcellhost.cloud
sales@xcellhost.cloud
+91-8657414121

XcellSecure

aiSIEM: Detecting “Threats That Matter”

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon



Threat Feeds

Event, App & Processes Data

User Data

Flow Data

Packet Data

SIEMs

CCE – n

CCE

CCE – 1 Feature Extraction Down Sampling

APE

Dynamic Threat Models

Fast Big Data Engine

ML - User Behavioral Analytics

AI with Recommended Remediation

Multi-stage Alert refinement

Windowed Correlations

De-duplication

Multi-factor Scoring

Multi Data Source Real-time processing

Ensemble of IoC detection methods

Weighted actions

User Feedback Integration

CCE – Control and Collection Engine

Collects inputs from variety of sources. Extracts key meta data and sends refined input to APE

APE – Analytics and Policy Engine

Threat Models based on User Behavioral Analytics and Machine Learning Fast Big Data Engine

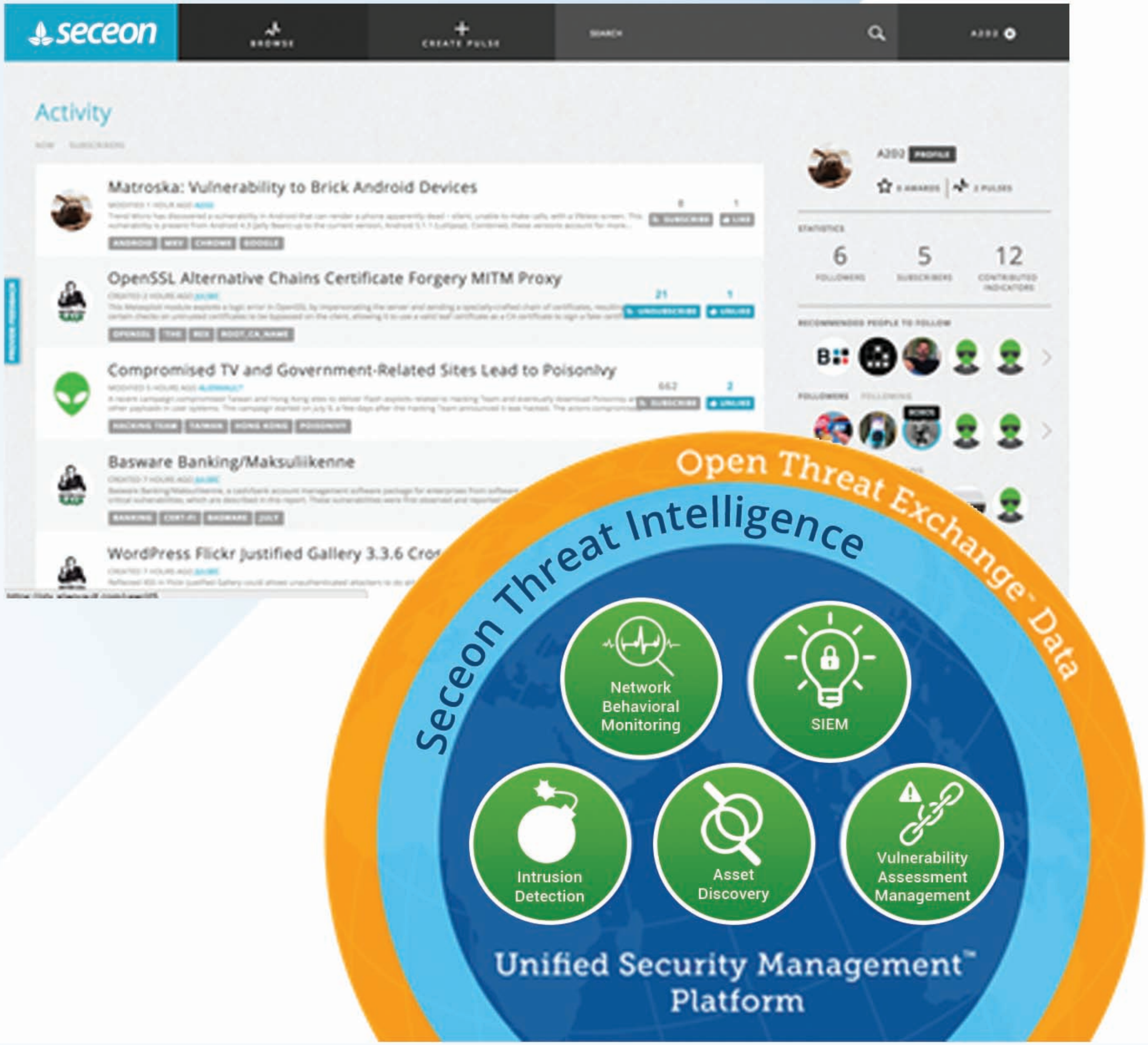
XcellSecure

aiSIEM: Open Threat Feed (OTX)

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

- ➤ The world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data
- ➤ With more than 37,000 participants in 140+ countries
- ➤ And more than 3 million threat indicators contributed daily
- ➤ Enables security professionals to share threat data and benefit from data shared by others
- ➤ Integrated with the USM platform to alert you when known bad actors are communicating with your systems


Activity

Matroska: Vulnerability to Brick Android Devices

OpenSSL Alternative Chains Certificate Forgery MITM Proxy

Compromised TV and Government-Related Sites Lead to PoisonIvy

Basware Banking/Maksuliikenne

WordPress Flickr Justified Gallery 3.3.6 Cros

seceon
BROWSE
CREATE PULSE
SEARCH
A202
PROFILE
6
FOLLOWERS
5
SUBSCRIBERS
12
CONTRIBUTED INDICATORS
RECOMMENDED PEOPLE TO FOLLOW
Open Threat Exchange- Data
Seceon Threat Intelligence
Network Behavioral Monitoring
SIEM
Intrusion Detection
Asset Discovery
Vulnerability Assessment Management
Unified Security Management™ Platform

XcellSecure

aiSIEM: Open Threat Management Benefits

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

Improve Your Security Posture With aiSIEM™

Open Threat Management Benefits

- Near Real Time Protection
- Integrate Remediation with FW/AD
- Stop Breaches in Minutes
- KB stays with OTM not with L0-L3, SMEs
- Data Visualization OOTB
- No Customization Required
- Actionable Alerts
- No Additional Special Skills Required
- Learning Curve is Small
- Reduce Training OpEx
- SaaS Model, Subscription Based Pricing
- Resilient Architecture, Scale Horizontally
- Reduced Upfront Capex
- Protect Private/ Hybrid Clouds

www.xcellhost.cloud sales@xcellhost.cloud +91-8657414121

XcellSecure

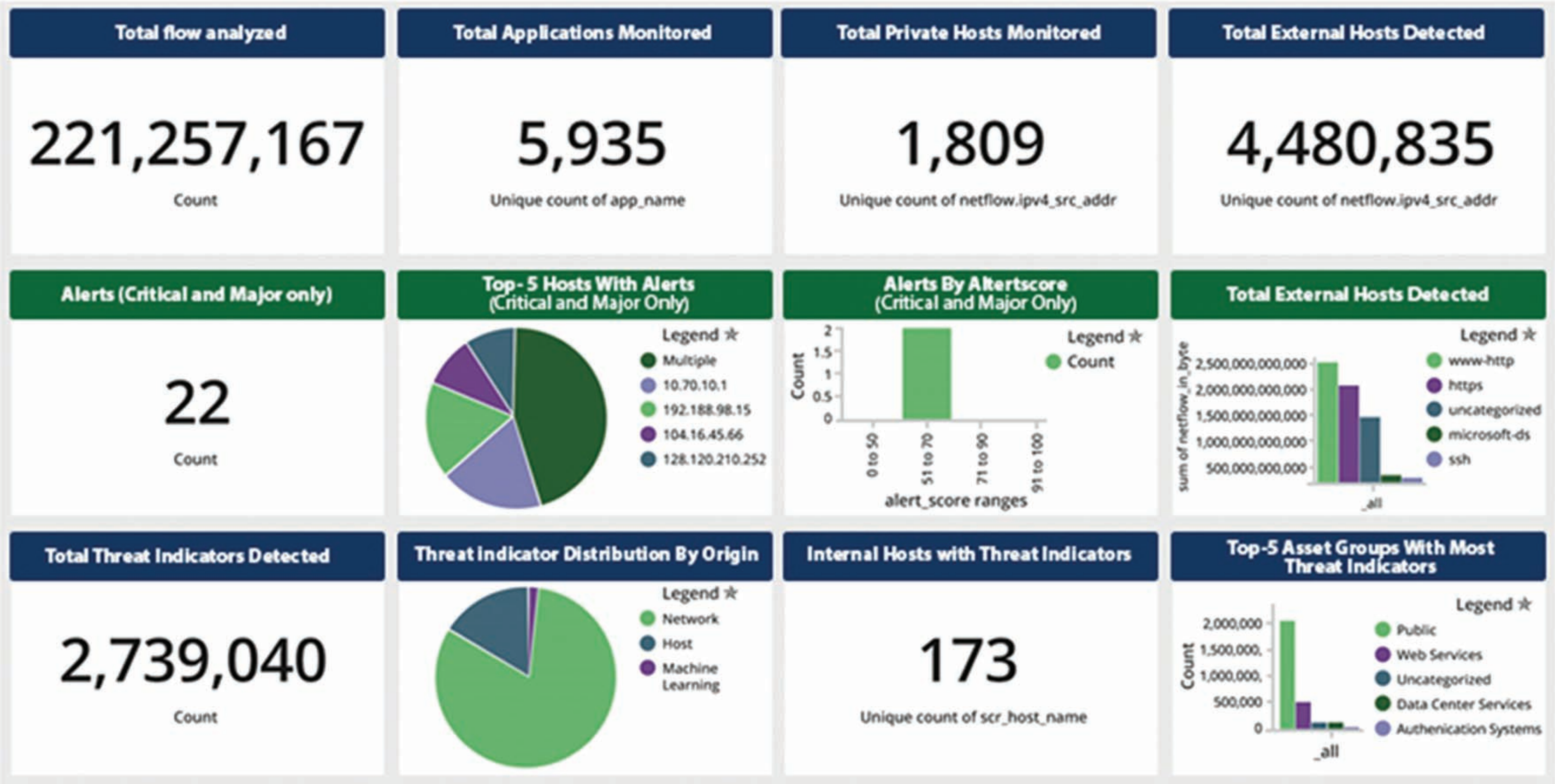
aiSIEM: Sample Dashboard

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: seceon

aiSIEM Alerts

Typical #of SIEM Alerts



Total flow analyzed
221,257,167
Count

Total Applications Monitored
5,935
Unique count of app_name

Total Private Hosts Monitored
1,809
Unique count of netflow.ipv4_src_addr

Total External Hosts Detected
4,480,835
Unique count of netflow.ipv4_src_addr

Alerts (Critical and Major only)
22
Count

Top- 5 Hosts With Alerts (Critical and Major Only)

Alerts By Altertscore (Critical and Major Only)

Total External Hosts Detected

Total Threat Indicators Detected
2,739,040
Count

Threat indicator Distribution By Origin

Internal Hosts with Threat Indicators
173
Unique count of scr_host_name

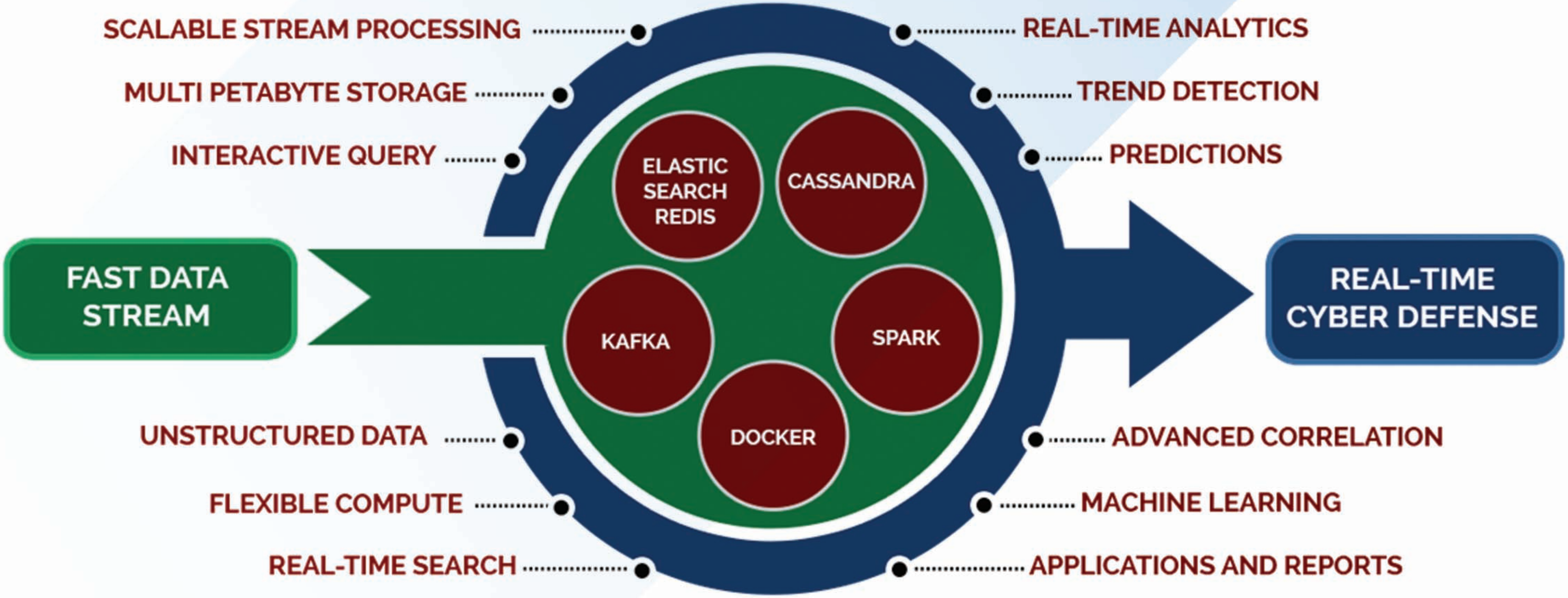
Top-5 Asset Groups With Most Threat Indicators

XcellSecure

aiSIEM: A High Level View

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: seceon



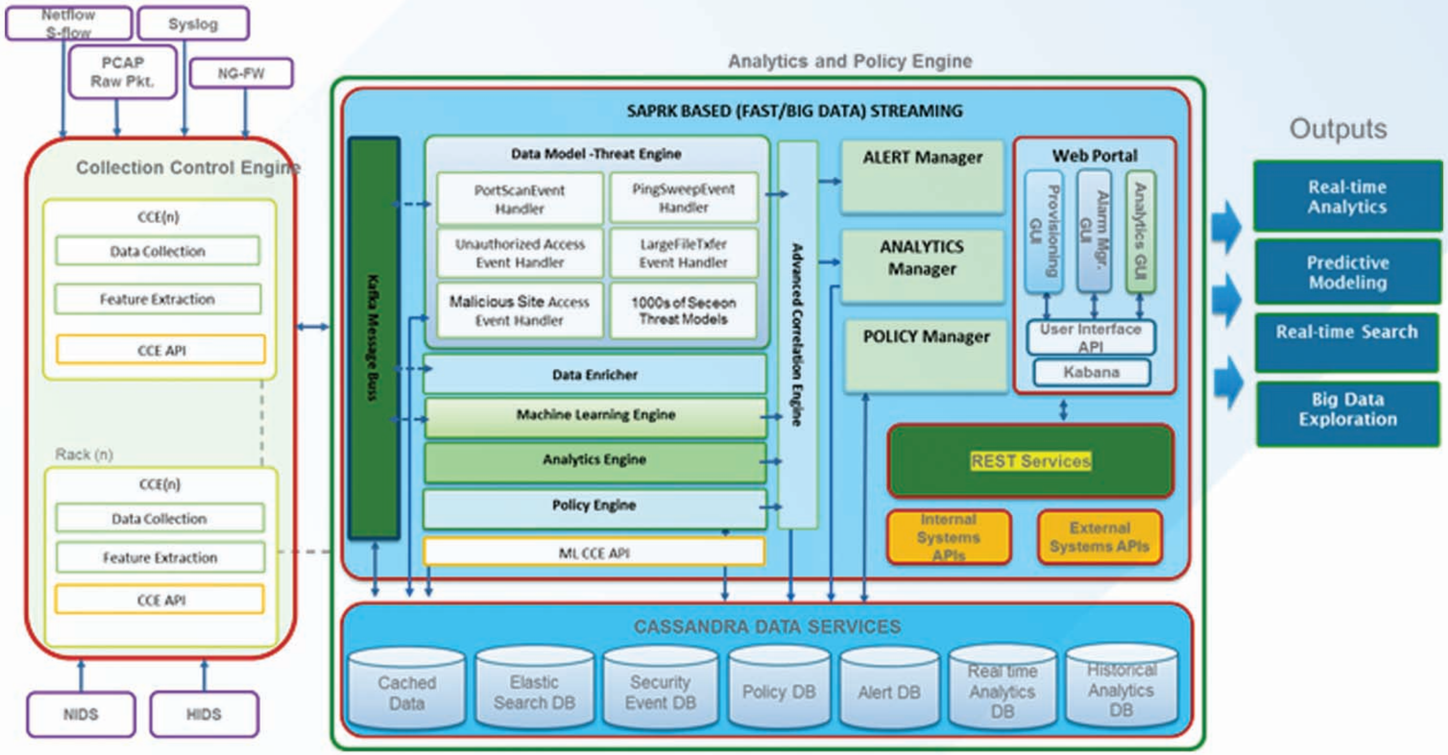
XcellSecure

aiSIEM: Core Architecture

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

Platform



Benefits

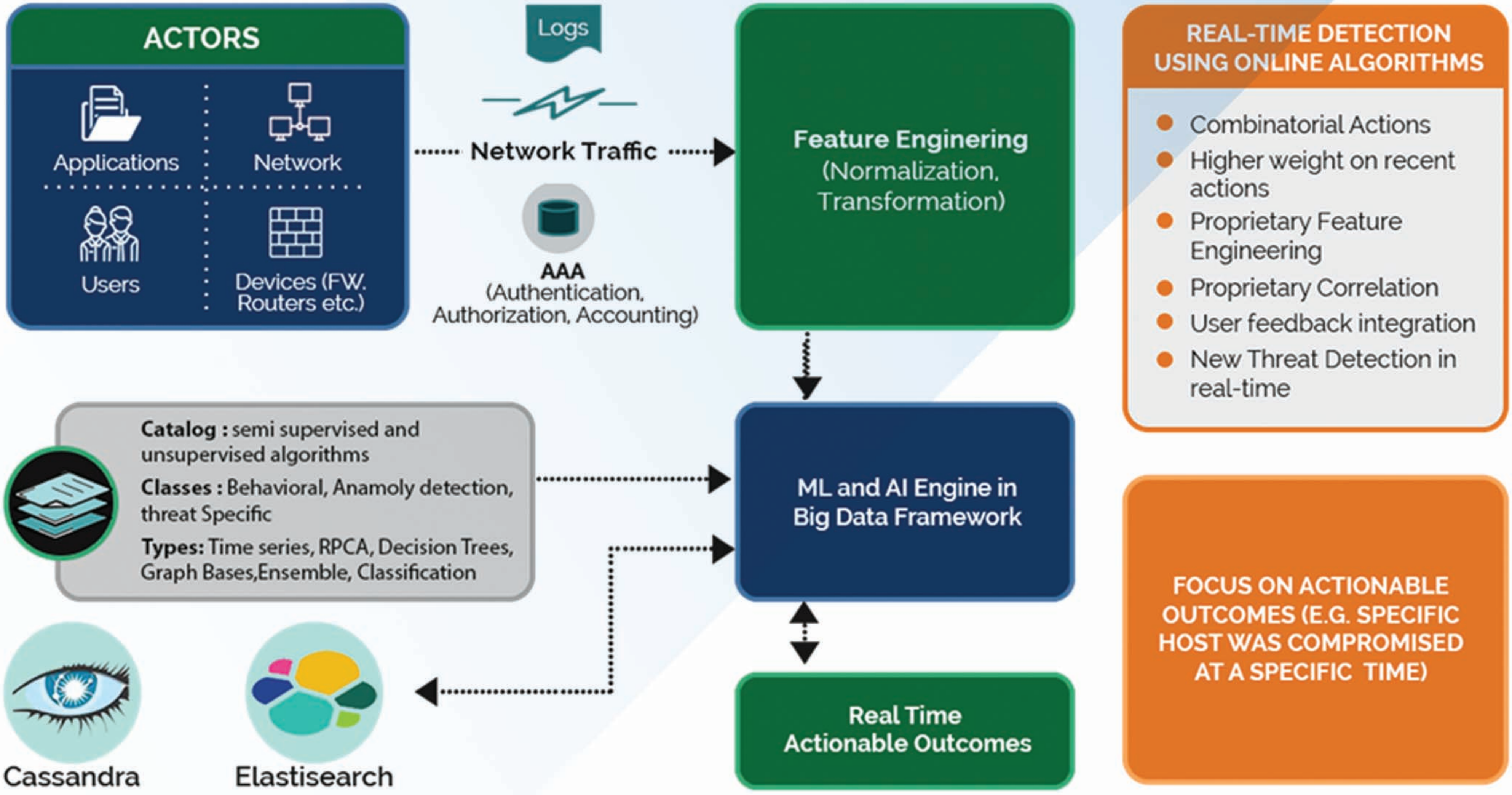
- Designed for MSSP
- Supports Multi-Tenants
- Adaptive Machine Language
- Behavior Analytics
- Threat Models (>25)
- Dynamic Thresholds
- Scale out architecture
- Support for multi-cloud environment
- Wrap-around solution

XcellSecure

aiSIEM: Machine Learning Execution

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon



ACTORS

Applications

Network

Users

Devices (FW. Routers etc.)

Logs

Network Traffic

AAA
(Authentication,
Authorization, Accounting)

Feature Enginering
(Normalization,
Transformation)

ML and AI Engine in
Big Data Framework

Real Time
Actionable Outcomes

Catalog : semi supervised and unsupervised algorithms

Classes : Behavioral, Anamoly detection, threat Specific

Types: Time series, RPCA, Decision Trees, Graph Bases,Ensemble, Classification

Cassandra

Elastisearch

REAL-TIME DETECTION USING ONLINE ALGORITHMS

- Combinatorial Actions
- Higher weight on recent actions
- Proprietary Feature Engineering
- Proprietary Correlation
- User feedback integration
- New Threat Detection in real-time

FOCUS ON ACTIONABLE OUTCOMES (E.G. SPECIFIC HOST WAS COMPROMISED AT A SPECIFIC TIME)

XcellSecure

aiSIEM: How Breach Detection work?

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: seceon

Cyber Intelligence in a Box

Detect and respond to attacks quickly without an army of analysts

Threat Detect Respond

3 reasons why you want to Integrate Breach Detection into a SIEM solution

Intelligence - Recogzine Threat Patterns

- Malware Intelligence Labs
- Engine-detecting New - Unseen Threats
- Reducing costs in Technical Support
- Plug-and-Play

Suspicious Network Trafic

- Non-Intrusive
- OS Independent
- Integrate with Existing Security Systems
- Data Retention - Analyse Traffic

Monitoring and Alerting Mechanism

- GDPR Regulations
- Network Egress Monitoring
- Security of Employee - Owned Devices
- STIX/TAXII Support

XcellSecure

Managed Security Services

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Reliably Protect Your Data And Your Business

- 24/7 Monitoring and Management of F-Secure Environment Activity
- Real time incident remediation Day or Night
- Guaranteed service levels, backup success and critical restore response time
- Updates, upgrades, and plans for expansion/ capacity growth in your IT environment

Save Time & Money

Remove the burden of backup operations

Minimize staffing issues

Focus IT on strategic business priorities

What We Manage

Firewall

IPsec VPN

Intrusion Prevention (IPS)

Antivirus

Anti-Spam

URL Filtering

Auto Logging & Reporting

Security Updates

Services

We are the Leader for Managed Security Services

Advanced Threat Services

Security Management & Orchestration

Security Monitoring

Vulnerability Management

www.xcellhost.cloud

sales@xcellhost.cloud

+91-8657414121

XcellSecure | Managed Security Services

Our Services

Extend Your Team with Cyber Security Experts

Leverage the power of XcellHost Managed Security Services for continual threat monitoring and customized guidance 24x7.

Flexible Coverage at a Predictable Cost

XcellHost Managed Security Services offers a predictable subscription-based cost structure to provide continual, real-time monitoring across your security environment.

Accelerate Detection and Response

Threat visibility across your environment and benefit from XcellHost global infrastructure, big data analytics, and integrated threat intelligence services.

Minimize Business Risk

XcellHost Managed Security Services helps to determine which events are most dangerous and critical to your organization

Our Solutions

Security Leadership

We are the
Leaders for 20+
consecutive years

Global Presence & Delivery

Global SOC's worldwide
industry leading SLA's-30
minute escalation

Scalability

Analyze 30+ million logs daily
escalate 400+ severe security
incidents daily

Expertise

Designated teams 100% GIAC
Certified Intrusion Analysts
customized service

Version 01/2018/ME/CP/MS

XcellSecure

aiSIEM: Out of Box Intregrations

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
seceon

Firewalls (Auto Remediation)

FORTINET SONICWALL™ paloalto NETWORKS Check Point® SOFTWARE TECHNOLOGIES LTD. SOPHOS CISCO™ WatchGuard™

Email Security

mimecast® Partner Office 365

End Point Security

F-Secure® CROWDSTRIKE

WAF

IMPERVA INCAPSULA CLOUDFLARE®

DLP

FORCEPOINT Symantec™

PROXY

zscaler

UEBA

Data Resolve

Public Cloud

Microsoft Azure amazon web services Alibaba Cloud

Other Security Tools

McAfee™ Together is power. RAPID7 SECLORE gemalto security to be free TREND MICRO™ okta

and many more....

www.xcellhost.cloud sales@xcellhost.cloud +91-8657414121

XcellSecure

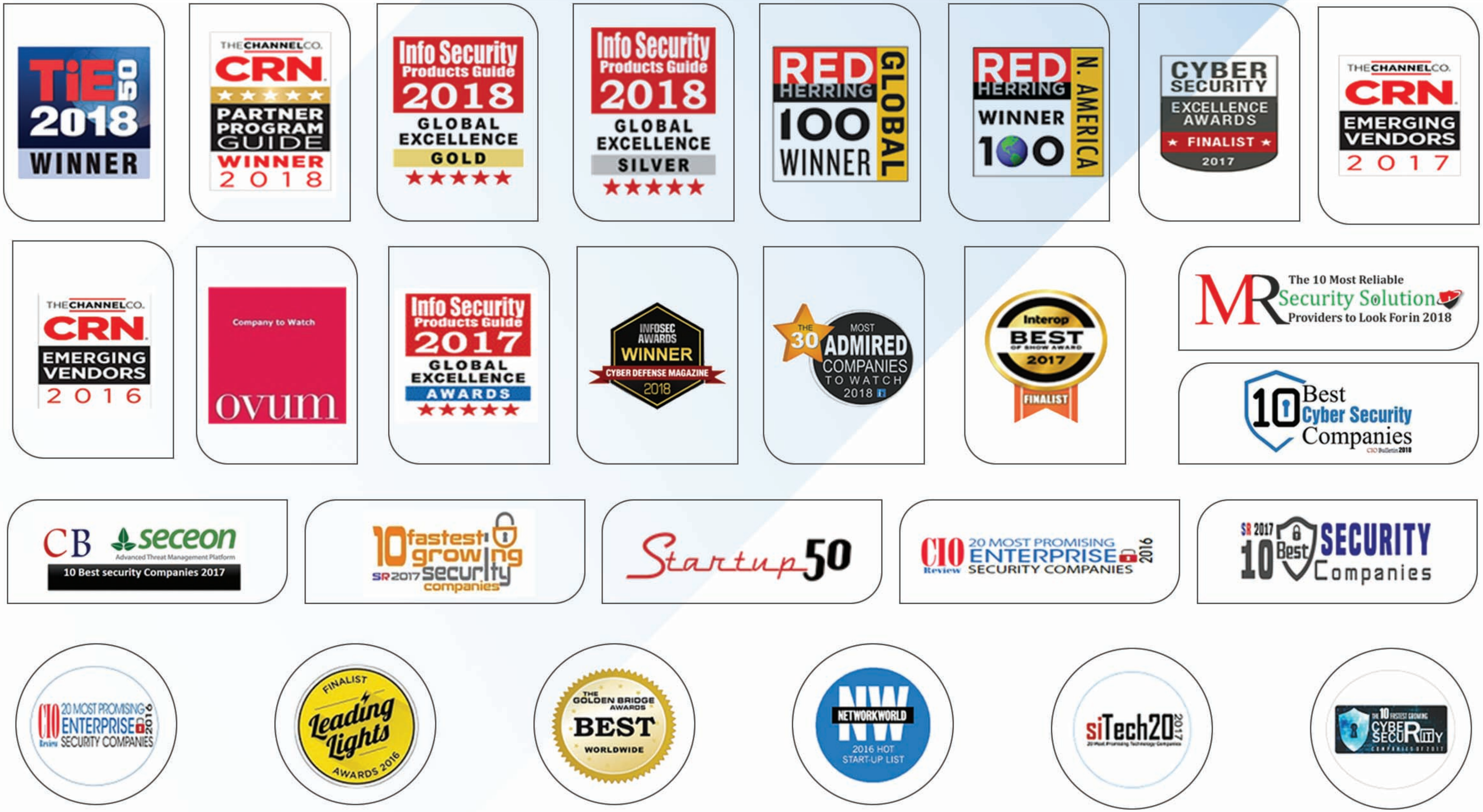
aiSIEM: Industry Awards and Recognition

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:

seceon



www.xcellhost.cloud

sales@xcellhost.cloud

+91-8657414121

XcellHost™

Global Reach - Personal Touch

ISO/IEC 27001 Information Security Management

ISO/IEC 20000-1 Information Technology Service Management

ISO 9001 Quality Management

• INDIA • DUBAI • SINGAPORE

209, Laxmi Plaza, Bldg. No. 9
Laxmi Industrial Estate,
Andheri (W), Mumbai - 400053
MAHARASHTRA, INDIA

+91-22-67111555

www.xcellhost.cloud sales@xcellhost.cloud +91-8657414121