

# 24/7/365 SOC

**DETECT | TRIAGE | DEFEAT**

Security Operation Center (SOC) works for you 24x7 – attackers never sleep and neither do we. We leverage Next-gen SIEM, AI, UBA and Threat Intel combined with an expert cyber security team to protect your business 24x7 at a starting price less than what it would take you to hire a single security analyst.

## 24X7 SOC MONITOR AND TRIAGE

- User Behavior Analytics (UBA)
- MITRE ATT&CK Framework
- Command & Control & Botnets
- Malware/Ransomware
- Phishing/Spear Phishing Attacks
- Indicators of Compromise
- Privileged Access Monitoring
- Privilege Escalation
- Lateral Movement Attacks
- Impossible Travel
- Unauthorized Access
- Brute Force Attacks
- VPN Access Anomalies
- Policy Violation & Misconfigs
- Suspicious Activities
- Defense Evasion
- Data Exfiltration
- DoS/DDoS

## SUPPORTED LOG SOURCES

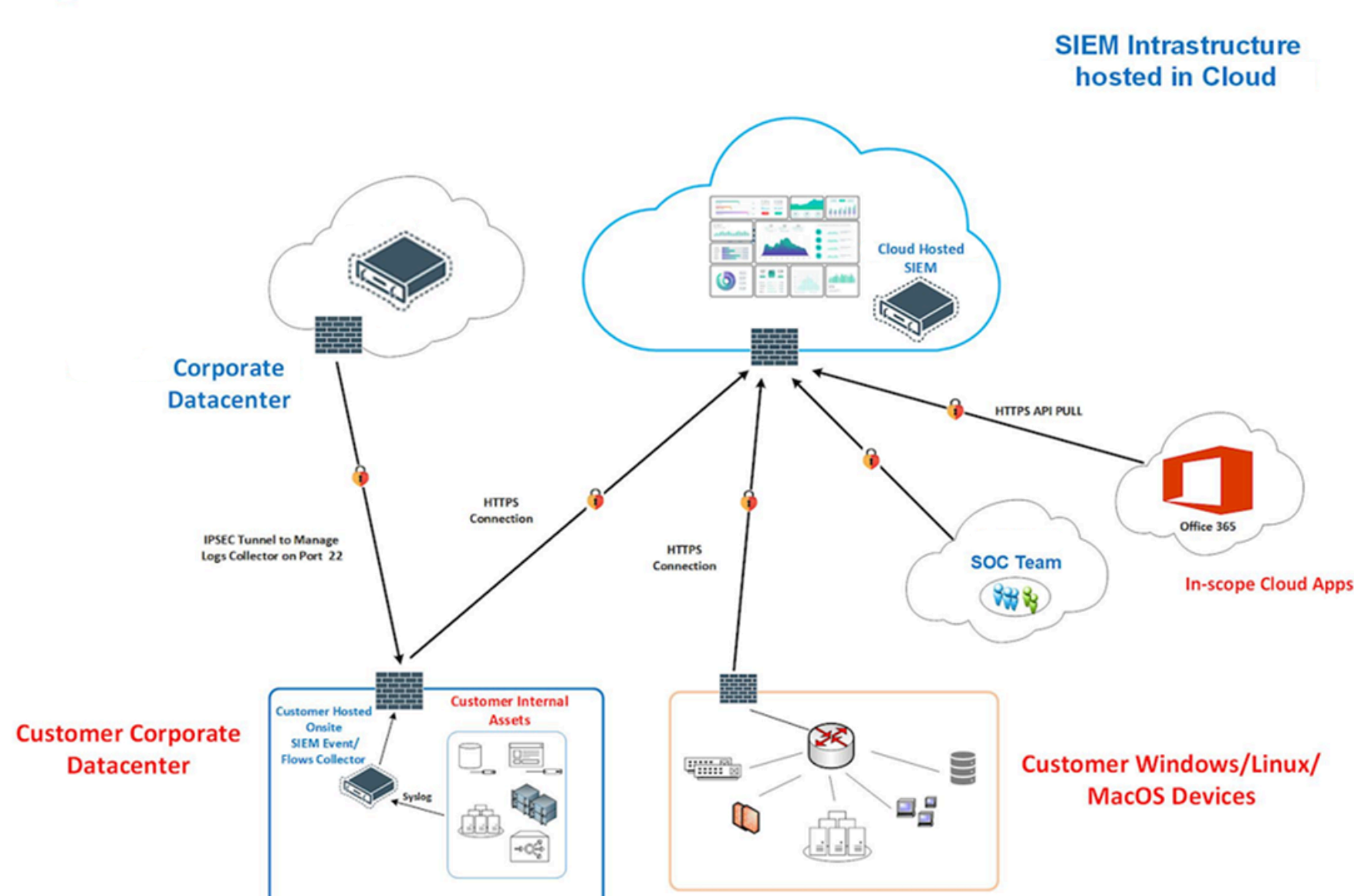
- Server Infrastructure
- Workstations/Laptops/WFH and Firewall/IDS
- Domain Controllers
- Email Solutions
- Web Proxies
- Antivirus/EDR
- Cloud Applications
- Enterprise Applications
- Custom Legacy Applications
- Routers/Switches
- DevOps

## WHY US

- **A SOC 2 Type II and ISO 27K1 Certified SOC**
- **Industry Beating Priced Premium Quality Service**
- **1000+ customers across 20+ countries**
- **Global SOC Locations**
- **Fully-Managed Turnkey/Co-Managed Options**
- **15-Min Gold SLA**
- **GDPR and Local Privacy Laws Compliant**

## SOC SERVICE ARCHITECTURE

Customer Hosted Rapid7 InsightIDR  
Log Collector Network Architecture



### Virtual Collector Specifications

CPU	RAM	HDD
4VCPU	8 GB	150 GB



## WHAT YOU CAN EXPECT

- 24x7 Threat Detection, Analysis & Alert Triage
- Weekly/Monthly SOC Reports
- Recurring SOC Governance Calls
- Access to Customer Data
- 750+ Custom Security Rules
- Assigned Named SOC Analysts
- SOC Ticketing Portal Access
- Automation & Incident Response
- Customized SOC Escalations
- 30-min GOLD SLA
- 90-days to 1-year log Retention
- Dedicated local 1800-SOC number

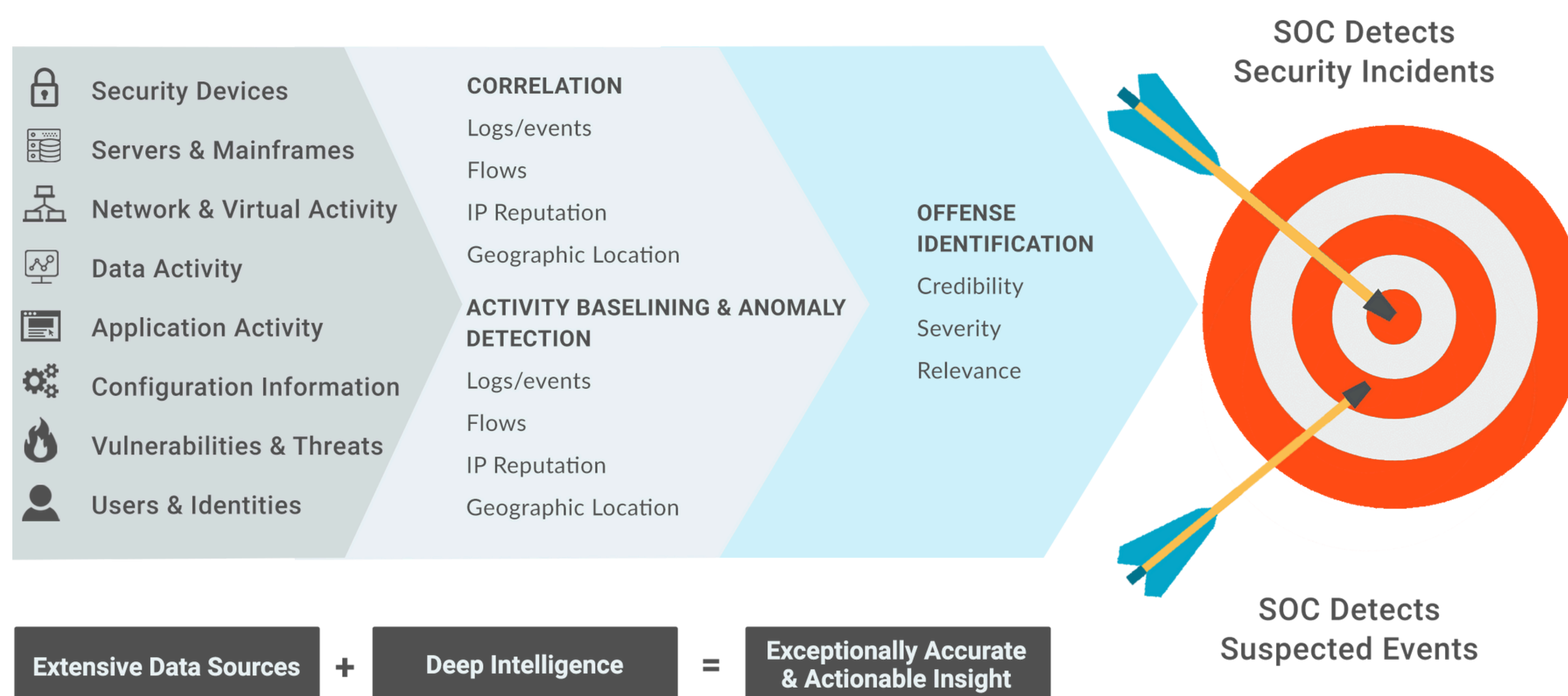
## SOC SERVICE BENEFITS

### Actionable & Noise Suppression Alerts

- Customer's network is monitored 24x7 by dedicated named SOC analysts.
- Every detected alert is triaged, and custom incident report tickets manually created.
- Noise is suppressed & only True Positives are escalated - Customers don't have to deal with overwhelming alerts and false positives.

### 24x7 Access to SOC and Customer Data

- Customer gets full access to search SIEM ingested log data
- Customer gets access to SOC Ticketing Portal
- 24x7 Real-time Incident Alerting & Triage by SOC
- SOC Analysts available to jump on Incident
- Containment Bridge Calls (No extra charges)
- 24x7 access to expert Named SOC analysts



## SUPPORTED SIEM PRODUCTS



## CONTACT US

## CONTACT US NOW!