# F7 SOC-AS-A-SERVICE

DETECT | TRIAGE | DEFEAT

F7Digital

F7's 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 F7 MONITOR & TRIAGE

> User Behaviour 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

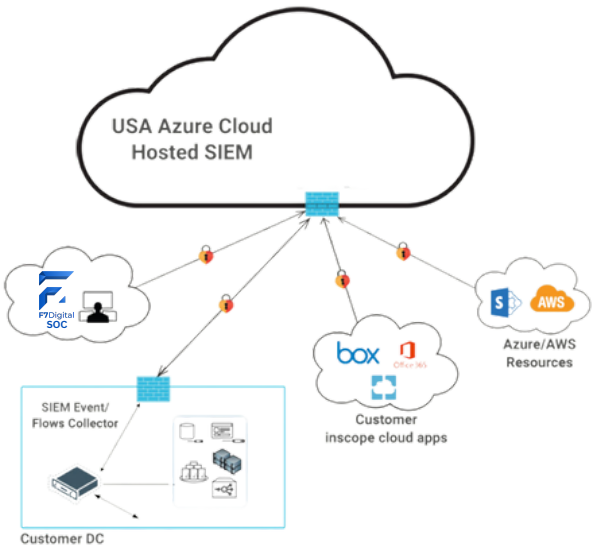
> Data Exfiltration

> DoS/DDoS

## WHY F7?

- ▸ A SOC 2 TYPE II AND ISO 27K CERTIFIED SOC
- ▸ INDUSTRY BEATING PRICED PREMIUM QUALITY MDR SERVICE
- ▸ 300+ CUSTOMERS ACROSS 10+ COUNTRIES
- ▸ GLOBAL MDR SOC LOCATIONS
- ▸ EDR SOLUTION AGNOSTIC SERVICE
- ▸ MONTH-TO-MONTH SUBSCRIPTION
- ▸ FIXED MONTHLY FEE (NO NICKEL-&-DIME!)
- ▸ NO EXTRA CHARGES FOR DEPLOYMENT AND ONBOARDING
- ▸ FULLY-MANAGED TURNKEY/CO-MANAGED OPTIONS
- ▸ GDPR AND LOCAL PRIVACY LAWS COMPLIANT

## SOC-AS-A-SERVICE ARCHITECTURE




| Virtual Collector Specifications | CPU | RAM | HDD |
|---|---|---|---|
| | 4 vCPU | 8 GB | 150 GB |

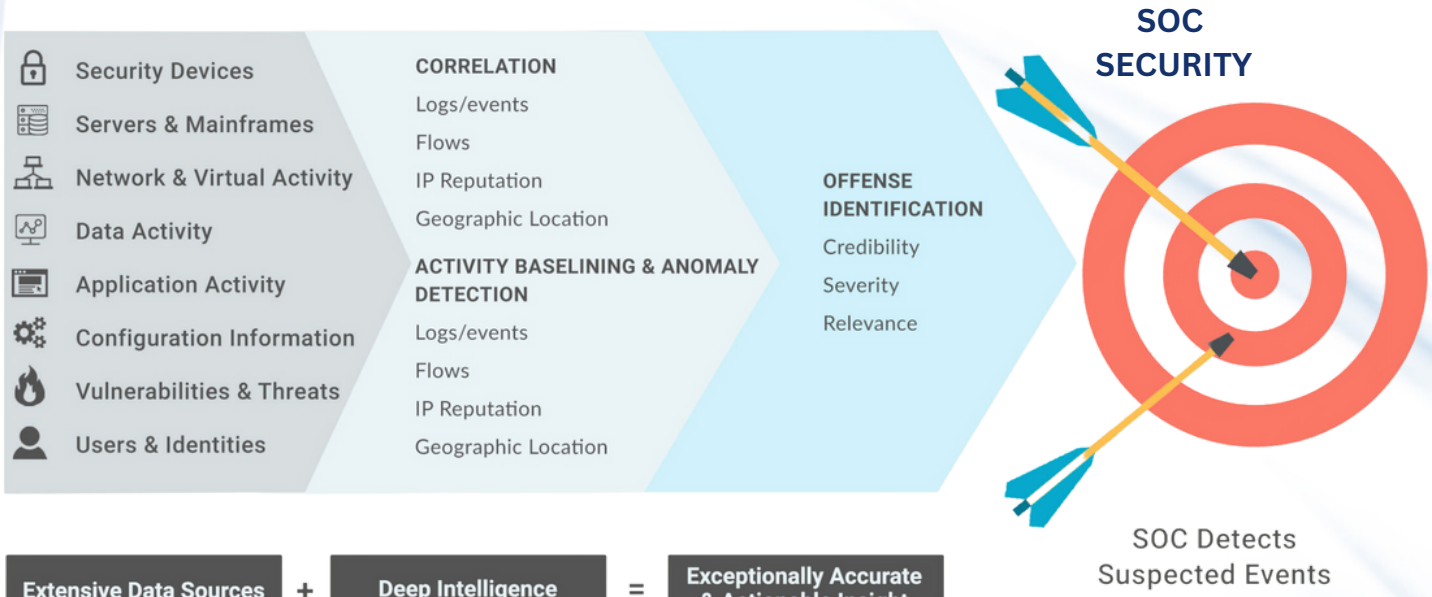
# BENEFITS OF SOC-AS-A-SERVICE

**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

**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

**Predictable Monthly Costs & No Contracts**
> Month-to-Month Subscription Contracts
> Customers have a predictable FIXED cost for their security operations
> Reduced operational complexity
> Reduced operational cost

# HOW SOC DETECTION WORKS




Extensive Data Sources + Deep Intelligence = Exceptionally Accurate & Actionable Insight

## F7 SOC-AS-A-SERVICE GLOBAL LOCATIONS