



LIGHTCREST

# Cybersecurity & Threat Mitigation

Your customers mandate a secure cloud. Get one.

## SOC-as-a-Service Services

- Dedicated Security Expertise
- Vulnerability Assessment
- Managed Threat Detection
- Security Incident Response
- 24/7 Network Monitoring
- Compliance Reporting

## Overcome Major Challenges & Threats

- Ransomware
- Phishing
- Data breach
- Alert fatigue
- Account hijacking

## Power Your Cybersecurity with SOC-as-a-Service

Cybercrime is more sophisticated than ever before, and companies are exposed to a wide range of new threats: ransomware attacks, phishing scams, data breaches, and more. The best practice for fighting this wave of cybercrime is to build a Security Operations Center (SOC). In a SOC, a dedicated team of security experts monitors threats throughout the organization, and uses cutting edge technology to detect and respond to attacks in real time. Only a SOC can handle the growing complexity of today's cyber threats.

However, SOC's are expensive, complicated and far beyond the reach of all but the largest enterprises. Many businesses attempt to fill the gap with point solutions, but this approach leaves them exposed and hackers are ready to exploit any vulnerability.

SOC-as-a-Service, powered by Lightcrest, meets this urgent business need. It is a dynamic combination of world class security experts and advanced machine learning, working together to provide actionable intelligence. With CyberSOC, businesses can achieve industry-leading threat detection and response, with unlimited scale and affordable cost.

## The SOC-as-a-Service Difference

### Dedicated Security Expertise

IT managers, facing limited budgets, can be tempted to assign cybersecurity responsibilities to general IT staff. But security is its own specialization, and simple technical expertise does not qualify an engineer to protect your organization. With CyberSOC, every company is supported by a trained and qualified security engineer, working exclusively to keep companies like yours safe.

- Industry-certified experts
- Dedicated to monitoring, testing, and remediation
- Strategic security recommendations





## Monthly External Vulnerability Assessments

Maintaining good security posture requires proactive measurement of unpatched vulnerabilities. With CyberSOC, you'll receive monthly vulnerability assessments, highlighting actionable steps you can take to eliminate known attacks that exploit those vulnerabilities.

- Regular analysis of cyber risk and security posture
- Improve effectiveness of your patch lifecycle

## Managed Threat Detection

The key to thwarting a cyberattack is prompt detection and effective response. CyberSOC uses a proprietary SOC, machine learning technology, and human expertise to detect threats as they occur, and direct your organization in effective response.

- Hybrid AI - human-assisted machine learning
- Behavioral analytics and threat intelligence
- Log management and analysis
- Unlimited policy customization

## Security Incident Response & Crisis Support

Most of the time and money in security goes into incident detection and response. With dedicated security expertise and security optimized CyberSOC we provide:

- Remote analysis of security incidents
- Prioritization and recommendation of remediation actions

## 24/7 Network Monitoring

Only round-the-clock network monitoring can detect anomalous activity and protect your company from cyberattacks. The CyberSOC includes network sensors that monitor network flows and collects log data to identify zero-day threats.

- 24/7 network monitoring
- Real-time alerting

## Compliance Reporting

We speed up compliance by producing the compliance reports required by each regulation and standard, reducing time and cost of audit preparation.

- Customized reports for PCI, HIPPA, SOX and more
- Instrumented for cybersecurity data science
- Immediately operational with zero setup time



LIGHTCREST

Lightcrest YPEs

SOC as a Service

Security Outcomes



MSP Security Program	Solution Examples
SOC-as-a-Service/Live Monitoring	Managed Detection & Response (24x7 monitoring, SIEM, IDS, Log Aggregations/Correlation, Threat Management, Behavior Analytics)
Vulnerability Assessment	Pentest, Continuous Vulnerability Scans, Asset/Patch Management
Security Assessment	Compliance Gap Analysis
Educate	Phishing Training/Campaigns
Remediate	Hands on Keyboards-Customer Action





# LIGHTCREST

## Lightcrest Cyber-SOC

### Industry's Most Fierce SOC-as-a-Service

A Security Operation Center (SOC) is the most essential element of modern security. But SOC's are expensive, complicated and far beyond the reach of most small enterprises. So many take the easy route and invest in products, but investment in new security products is no guarantee of security.

Lightcrest CyberSOC™ differs from traditional managed security services. It is a dynamic combination of world-class Concierge Security Engineers (CSE), advanced machine learning, and action-able security intelligence. Your CSE conducts both routine and emergency tasks to protect you from known and unknown threats

## Lightcrest CyberSOC Service Capabilities



**Dedicated  
Security Expert**



**Managed  
Detection &  
Response**



**SIEM  
Replacement**



**Regulatory  
Compliance**



**Behavioral  
Analytics**



**Real-Time  
Alerting**

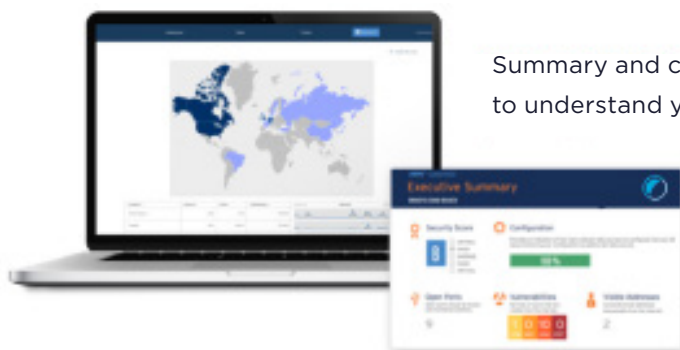


**Log Analysis  
with Machine  
Learning**



**Vulnerability  
Scans**

## Lightcrest CyberSOC Service Capabilities



Summary and customized reports  
to understand your security posture

## Turnkey SOC In Minutes

### Concierge Security Engineers

- Customer-dedicated primary point of contact
- Proactively hunts for hidden threats and remote forensic analysis

### Managed Detection and Response

- Machine learning with adaptive tuning for efficiency and scale
- Actionable remediation recommendations

### Security Incident and Crisis Support

- Assessment of the severity of an incident or crisis
- Prioritization of remediation and required steps

### Compliance

- Monitoring user behavior and managing security incidents
- Reducing time and costs of audit preparation

### Simple, Predictable Pricing

- Fixed price for the duration of your contract
- Unlimited data or event collection





# LIGHTCREST

## The Lightcrest Difference

### Concierge Security Engineer

The Concierge Security Engineer (CSE) is your single point of contact for your Lightcrest SOC-as-a-Service. Your CSE is your trusted security advisor and an extension of your internal team.

- Conduct daily triage and forensics
- Customizes service to your needs
- Provide actionable remediation recommendations

### CRule Intentions

CRule Intentions provide unlimited flexibility to tailor our services to the exact needs of every customer. They allow the CSE to apply your exact security and operational policies and update them as needed to align with your changing business needs expeditiously.

- Unlimited security policy customization
- Unlimited rules granularity or generalization
- Unlimited situational rules customization

### Hybrid AI

Hybrid AI demonstrably identifies attacks, reduces false positives and speeds up the time between detection and response. It merges a security engineer's intelligence and intuition with the efficiency and productivity of artificial intelligence.

- 10X better threat detection
- Human intelligence and intuition
- Machine scale and efficiency

### Security Optimized Data Architecture (SODA)

SODA unifies the ingestion, parsing and analysis of network traffic and log data. It provides the foundation for the security analytics that give our security engineers deep pervasive visibility into your security posture.

- On demand access to the relevant security data for incident investigation
- Instrumented for cybersecurity data science
- Immediately operational with zero setup time

