SOC IN A BOX

Successful cyber attacks are increasingly showing up in headlines, leaving a wake of financial loss, data loss, negative brand impact and organizational disruption. As a result, industry regulations continue to develop and enforce standards that must best be adhered to.

To meet those demands while moving at the speed of business, a security solution needs to be quick to deploy, affordable, effective and functional.

CyFlare has created The SOC In A Box that provides an AI Driven Breach detection, vulnerability scanning monitored 24x7x365 by a Top 100 Global MSSP

Flexible Deployment Options

100 Series Appliance

- Mini PC Form Factor
- 4-1gbps Copper Ports
- Comes Pre-Configured
- Includes Updates & Maintenance
- Next Day Replacement Included
- Load support for up to 500 devices

200 Series Appliance

- 1U Rackmount
- 6-1gbps Copper Ports, Fan Cooled
- Comes Pre-Configured
- Includes Updates & Maintenance
- Next Day Replacement Included
- Load support for up to 500 devices

Virtual Appliances are Also Available for Deployments in

vmware KVM docker amazon web services Microsoft Azure x86 Microsoft Hyper-V

A Security Platform

The SOC In A Box is s so much more than an appliance with a security tool. The SOC In A Box has been engineered from the ground up to enable multiple security tools, all pre-configured and maintained around the clock.

CYFLARE

The Solution Line-Up

Breach Detection System	Vulnerability Scanning	CyFlare Pulse – 24x7 SOC
AI Driven Security Platform	Internal and External Network scanning	100% USA Based
SIEM Replacement	Simple Risk Scoring	Dedicated Customer Success Manager
Zero Day File Sandboxing	Vulnerability details	Constant Security Analyst Monitoring
Exploit Kit Detection	Simple To Read Reporting	Unlimited Incident Response
26 Supervised Machine Learning Use Cases	Simple or Credential Based Scanning	Defined SLA
Automated Threat Hunting	Agentless	
Customizable Dashboards and Reports		
IDS		
Application ID Engine		

More Solutions Coming Soon including DLP, IoT and Firewall.

Breach Detection System (BDS) Overview

This is not your grandfathers SIEM tool. The BDS elegantly integrates best-of-breed threat intelligence feeds, cloud sandboxing, IDS, additional security engines and supervised Machine Learning.

Though the platform is built to enable rapid identification of anomalous behaviour it still offers SIEM functionality providing clients with transparency via a full-featured web portal allowing event searching and drill-down capabilities.

Pervasive Visibility

The cornerstone of an effective security monitoring and detection solution is visibility into your entire infrastructure whether that includes on-premises servers, virtual machines, workstations, containers, cloud VM's or cloud services.

The BDS monitors or accesses the following data:

- Passively monitor all network activity via a mirror or TAP
- Windows or Linux Server event log forwarding
- OKTA API Integration
- Office 365 / Azure AD API Integration
- AWS Cloudtrail API Integration
- Nessus log ingestion

Firewall Integrations

The BDS provides API integrations into major firewall vendors to enable automatic or integrated white and blacklist management, a common activity for remediation.

The following firewalls are currently supported:

- Palo Alto Networks
- Fortigate
- Checkpoint
- AWS Firewall
- Hillston

CYFLARE

Compliance Enablement

The BDS serves as compliance enablement tool providing SIEM capabilities for pre-defined reporting and customizable reporting.

Compliance requirements such as PCI DSS, HIPAA and NIST-CSF require evidence to be provided of various events that have taken place.

The following are just some of the reports that the BDS can provide:

- Audit Failures by User
- Audit Failures by Host
- Suspicious Activity by User
- Suspicious Activity by Host
- Suspicious Users
- Top Targeted Hosts
- Top Targeted Applications
- Access Granted/Revoked by User
- Access Granted/Revoked by Host
- Access Granted/Revoked by Application
- Disabled/Removed Account Summary
- Disabled/Removed Accounts by Host
- Disabled/Removed Accounts by Application
- Successful/Failed File Access by User
- Successful/Failed Host Access by User
- Successful/Failed Application Access by User
- Privilege Escalations on Windows / Linux systems
- File Integrity Monitoring
- Audit Trail History

Hyper-Paranoid Security For Any Organization In Any Vertical

The following capabilities have been built in and ALL included within your subscription:

Environment Support

- AWS
- Azure
- Google Cloud Platform
- VMWare
- KVM
- Hyper-v

Operating Systems (Agent)

- Ubuntu
- Debian
- Red Hat
- Centos
- Docker & other containers
- Windows Server 2008 or later

Data Capture Methods

- Port Mirroring
- Physical Network Tapping
- Virtual Network Tapping
- Syslog
- API Integrations
- Nessus Log Ingestion

Features

- Machine Learning (Supervised & Unsupervised)
- Real Time Kill Chain Breach Detection
- Asset Discovery
- Historical Forensic Investigation
- Network Traffic Analysis
- Application Performanc Monitoring
- Centralized Management
- Malware Sandbox
- Next Generation Intrussion Detection System
- Anti-Virus
- SIEM (Syslog, IPFIX, Aella Flow)
- Deep Packet Inspection (3,000+ applications)
- Application Identifcation & Metadata extraction
- Service Visualization
- User visibility & tracking (Auth Log, AD, Kerberos, Radius)
- Digitial Certificate Visibility
- Geo Location Feeds
- Threat Intelligence Feeds
- Threat Intelligence Sharing
- Firewall Enforcement Integration (Palo Alto Networks, Fortinet, AWS)
- SIEM Integration (Splunk, Elasticsearch)
- Orchestration Integration (Phantom)
- Alerting
- Reporting
- Data Processor / Data Lake Clustering & High Availability
- Multi-tenancy support
- Multi-tenant machine learning
- Multi-site ML

CYFLARE

Detections

Reconn

- Port scan & IP address sweeping
- Brute force login failures (SSH, AD, SQL)
- Brute force login success (SSH, AD, SQL)
- Login location anomaly detection
- Web directory scan detection
- Malcious user agent detection
- Phishing detection
- Malcious reputation detection

Delivery

- Zero day malware detection
- Known malware detection
- Lateral malware movement detection
- Ransomware detection
- Spyware detection
- Trojan detection
- Virus detection

Exploitation

- Known exploit detection (80,000+)
- Zero day exploit detection
- Process anomaly detection

Installation

- File creation detection
- File modification detection

Command & Control

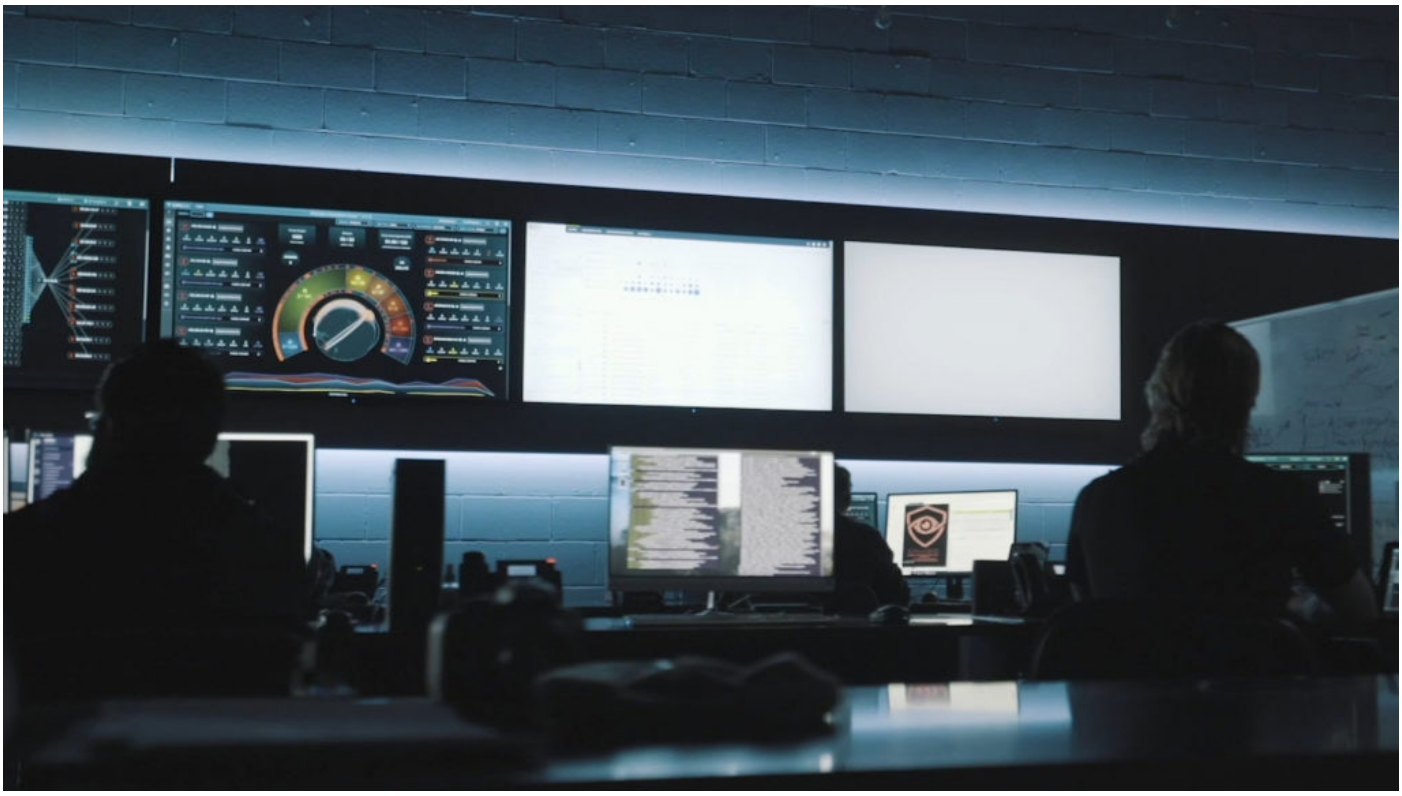
- C&C server reputation (50,000+)
- Resolvable DGA detection
- Command execution anomaly detection
- SQL command line execution detection

Exfilitration & Actions

- DNS tunneling detection
- Denial of service detection (Syn Flood)
- Anomalous outbound traffic detection
- Bitcoin mining detection

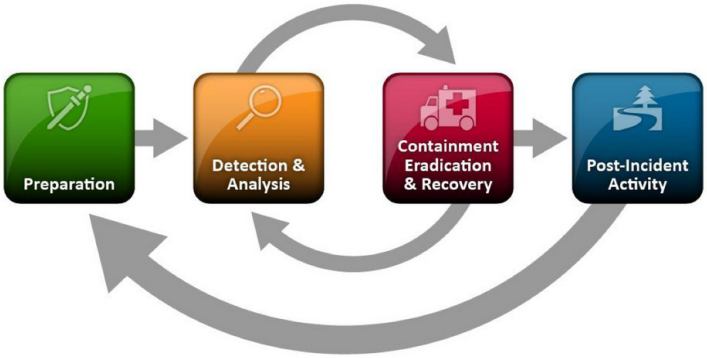
Network Traffic

- Geographic anomaly detection
- Session duration anomaly detection
- Anomalous inbound traffic detection
- Abnormal smb traffic detection



CYFLARE

SOC Methodology



Preparation

- Gap Analysis of the Customer Environment
- Network Discovery Questionnaire
- Remote access for SIEM sensor install
- Recommendation of Technology Defining of SLA's

Detection & Analysis

- Network Discovery Collection of host and network based security logs
- Identification of Critical Systems and Privileged Users
- Refinement and tuning of correlation rules according to company policy and needs
- Compliance and Vulnerability Report scheduling
- Availability Monitoring and Alerting
- File Integrity Monitoring

Containment, Eradicatio & Recovery

- Stop the bleeding by automated action or client recommendation
- Client recommendation for remediation within defined SLA's (Critical, High, Medium, and Low)
- Playbook Execuition (manual and automated)
- Automated security orchestration (block, lookup, quarantine w/o customer interaction

Post-Incident Activity

- Refinement of correlation rules to detect or monitor for other current or future compromises across the network
- Continual recommendations for long term security program and roadmap improvement
- Additional threat-hunting services availableTechnology Defining of SLA's

Analyst Roles

Resources are managed by the SOC Director who will also serve as an escalation point along with other level 3 engineers we employ.

Role	Meta-Data	Memory	Disk Storage
Tier 1 Security Analyst	Triago Specialist (Separating the wheat from the chaff)	Sysadmin skills (Linux/Mac/Windows); Programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more; security skills (CISSP, GCIA GCIH GCFA, GCFE, etc.)	Reviews the latest alert to determine relevancy and urgency. Creates new trouble tickets for alerts that signal an incident and require Tier 2 / Incident Response review. Runs vulnerability scans and reviews vulnerability assessement reports. Manages and configures security monitoring tools (netflows, IDS, correlation rules, etc).
Tier 2 Security Analyst	Incident Responder (IT's version of the first responder)	All of the above + natural ability. dogged curiosity to get to the root cause, and the ability to remain calm under pressure. Being a former white hat hacker is also a big plus.	Reviews trouble tickets generated by Tier 1 Analyst (s). Leverages emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and scope of the attack. Reviews and collects asset data (config, running processes, etc.) on these systems for further investigation. Determines and directs remediation and recovery efforts,