CYFLARE

PULSE - BREACH DETECTION SERVICE

Technical Capabilities Overview

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

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

Environment Support

- AWS
- Azure
- Google Cloud Platform
- VMWare
- KVM
- HyperV

Operating Systems (Agent)

- Ubuntu
- Debian
- Red Hat
- Centos
- Docker
- Windows

Data Capture Methods

- Port mirroring
- Physical Network tapping
- Virtual Network tapping
- Agent
- VXLAN
- GRE
- Logs
- Netflow / IPFIX