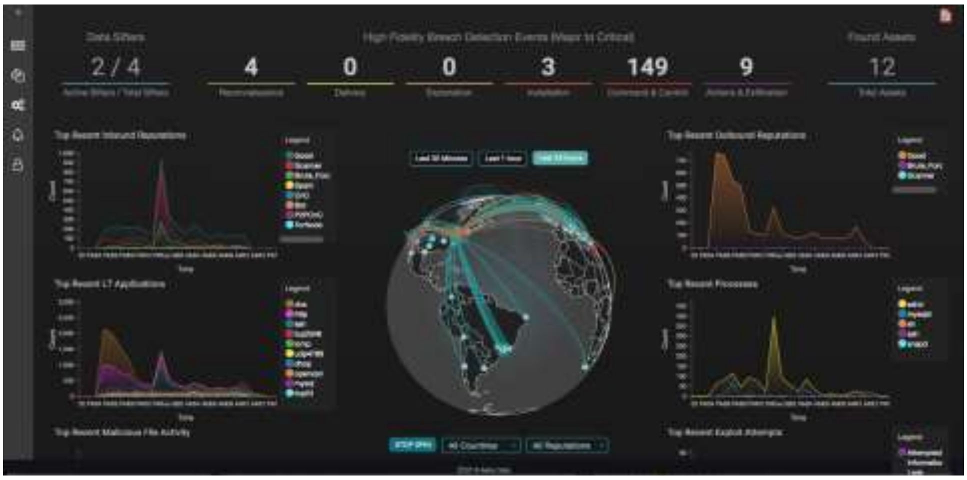
www.guardianhit.com : 1-800-607-9890

GUARDIAN INFOSEC SOLUTIONSPULSE SOC-AS-A-SUBSCRIPTION


Data Sifters
High Fidelity Breach Detection Events (Major to Critical)
Found Assets
2 / 4
Active Sifters / Total Sifters
4
Reconnaissance
0
Delivery
0
Exploitation
3
Installation
149
Command & Control
9
Actions & Exfiltration
12
Total Assets
Top Recent Inbound Reputations
Top Recent Outbound Reputations
Top Recent L7 Applications
Top Recent Processes
Top Recent Malicious File Activity
Top Recent Exploit Attempts

A Security Operations Center (SOC) is a cornerstone to an effective security strategy. Building a SOC requires the right tools, right people and most important the right procedures to bring it all together. The alternate to an outsourced SOC is to go through extensive evaluations of available security tools, evaluate staffing needs, complete extensive tool training, professional services for tool deployment and building of processes to consistently investigate important alarms. This process is incredibly time consuming, expensive and takes months, if not years depending on the size of the organization. Guardian InfoSec Solutions can be deployed rapidly providing a SOC within minutes.

Guardian InfoSec Solutions provides a packaged solution to bring an innovative breach detection platform and expert security resources together in a SOC-as-a-Subscription.

Key Benefits

- **Enterprise Grade Breach Detection Platform**
- **Turn a SOC on in days not months**
- **Analyst created monthly executive security briefing report**
- **Deployment Included**
- **Enables Compliance (PCI, HIPAA, NIST)**
- **All-Inclusive Monthly Subscription**
- **Month to Month commitment**
- **We do not nickel and dime for new devices, servers etc.**
- **Dedicated Technical Account Manager**
- **24x7x365 Constant Monitoring and Response**

Customized Monthly Executive Security Briefing Report

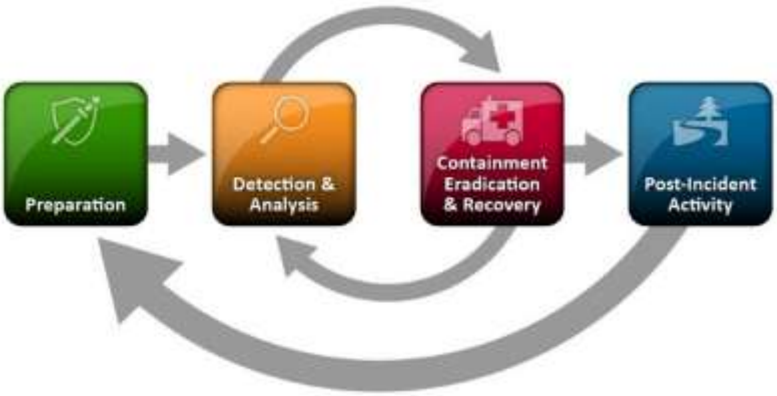
Your dedicated Technical Account Manager will compile an executive report that includes:

- **Key Alarms that occurred within the month with disposition**
- **Top system vulnerabilities and recommendations to remediate**
- **New industry specific threats**
- **Other security recommendations**
- **Additional custom data points as required by the client**

Guardian InfoSec Solutions Pulse Platform Key Security Features

- **Machine Learning**
- **Pervasive Visibility for Small to Very Large Companies**
- **SIEM Replacement**
- **Network Intrusion Detection System**
- **File Sandboxing (Detects ransomware, trojans and viruses.)**
- **DNS Tunnel Detection**
- **Best of breed integrated threat intelligence**
- **Automatic Domain Generation Detection**
- **Authentication Detection**
- **Malware Detection**
- **Exploit Detection**
- **Command and Control Detection**
- **Ex-Filtration and Personally Identifiable Information Detection**
- **Port Scan / Syn Flood Detection**
- **Anomalous Application Detection**
- **Anomalous Traffic Detection**
- **Anomalous Command Detection**
- **Anomalous Process Detection**
- **Anomalous File Access Detection**

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 AND 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, ERADICATION & RECOVERY

- ● Stop the bleeding by automated action or client recommendation
- ● Client recommendation for remediation within defined SLA's (Critical, High, Medium, and Low)
- ● Playbook Execution (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 available-Technology 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	Triage 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,

Flexible Deployment Options

- ☐ Lightweight Virtual Appliance
- ☐ Pre-Configured Hardware Appliance
- ☐ Server Agent

100 series