PBS PHANTOMWATCH

I Fear Not The Man Who Has Practiced 10,000 Kicks Once, But I Fear The Man Who Has Practiced One Kick 10,000 Times."
- Bruce Lee

SOC-as-a-Service

Cyber security is what we do. All day. Everyday. Our solution provides an easy, yet formidable and a reliable method to meet your cyber security needs. From network traffic flows, log ingestion, and compliance - our solution is engineered from the ground up to enable multiple security tools, all pre-configured and maintained around the clock.

Cyber security and bad actors are moving far too quick for businesses to appropriately and proactively protect and respond to threats as they happen. There are simply too many tools, too many events, and too many constraints to effectively manage it all.To meet those demands while moving at the speed of business, a security solution needs to be quick to deploy, affordable, effective, and functional.

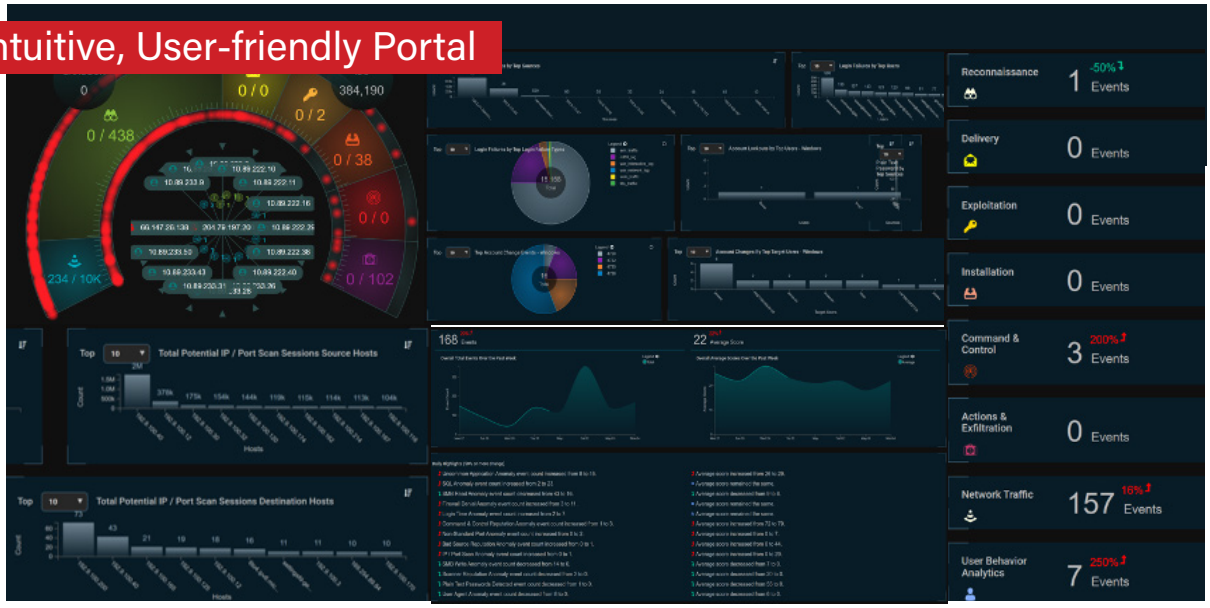
PBS PhantomWatch offers SOC-as-a-Service that provides human and AI Driven Breach detection, vulnerability scanning, and much more monitored 24x7x365.

SOC-as-a-Service Overview

IDS Installation and Tuning	Included
IDS 24x7x365 Monitoring	Included
IDS Regular Attack Signature Updates	Included
Monthly Mgmt. & Event Summary Report	Included
SIEM Configuration and Tuning	Included
SIEM 24x7x365 Data Capture	Included
SIEM Regular Analysis	24x7x365
SIEM Regular Attack Signature Update	Included
Vulnerability Scanning	Internal & External
SIEM Report Generation	Scheduled & On-Demand
Remote Incident Response Assistance	Included
Log Management	24x7x365 Included

Asset Discovery	Included
Comprehensive Threat Intelligence	Included
Automated Response for Integrated Security Platform	Included
File Sandboxing (Detects Ransomware, trojans, and viruses)	Included
Anomalous Application, Traffic, Commands, Processes	Included
File Access Detection	Included
Malicious Command & Process Detection	Included
Concierge Security Engineer	Included
Monthly Security Report and Briefing	Included
24x7x365 Manned Security Ops Center	Included

Intuitive, User-friendly Portal



the benefits:

SOLUTION HIGHLIGHTS

AI Driven Breach Detection
Our solution provides enterprise grade cyber security monitoring, analytics and detection which incorporates features and capabilities that a typical SIEM solution does not. The solution not only includes typical features of a SIEM that includes ingesting logs, correlation and reporting, it also includes deep machine learning to accurately and efficiently detect zero day threats from 3,250 different data points.

Rapid Detection Time
With over 40 threat intelligence feeds, threat engines, and machine learning detections our solution quickly identifies emerging, active, and dormant threats with an intuitive interface that will be made available to you at all times. We provide full transparency to the UI and all detections made. Our staff utilizes multiple tooks for monitoring and analyzing your environment.

Compliance Enablement
By default, all server logs including privileged account access, network device syslogs and network flow logs are stored for a 1-year period which enables compliance for the following regulations:

- HIPPA
- PCI
- NIST
- DFARS
- ISO27001
- GLBA
- SOX

> *"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."*
>
> - FBI

how it works:

SOC METHODOLOGY

SOC Intakes Data:

- Network Security Firewall
- Endpoint Security (PC/VDI)
- Model Security
- SPAM and Email Security
- Data Loss Prevention (DLP)
- SaaS Application Security
- Identity Access Mgmt (IAM)
- Multi-Factor Authentification (MFA)
- Server, Network, & Application Logs
- Network Flows and Packet Data
- Cloud Access Security Broker (CASB)
- Internet of Things (IoT)

SOC Provides:

- Automated Response Capability to Address Security Incidents
- Remediation Guidance / Incident Response
- Security Tuning and Improvement Recommendations
- Regular Security Status and Compliance Reporting
- Monthly Security Briefings

Implement Improvements Utilizing:

- Solution Tuning
- Process Improvements
- Technology Changes
- User Training
- Other Actions

ADDITIONAL SERVICE OFFERINGS

- Compliance Management
- Digital Asset Discover
- Incident Response
- Risk Management
- Security Compliance Management
- Security Solution Management (endpoint, firewall, cloud)