As organisation needs continue to evolve in Network Operations (NOC), Security Operations (SOC) along with Governance, Risk and Compliance (GRC) there are now more ways to monitor and visualize system data than ever before. With new solutions and approaches arriving in the market every day all claiming to be a silver bullet for an organisation's security and monitoring needs, prioritization of monitoring and visualization technologies continues to grow more complex. As a result of this increasingly complex landscape, Pervade Software has created the Hierarchy of Monitoring Needs to act as a measure of maturity for organisations to understand current and future needs.

Whilst the below hierarchy offers a benchmark for maturity against monitoring needs, how an organisation achieves each layer is not detailed within this document. It is recommended that a unified system allowing complete correlation of data between all layers along with automated analysis, reporting and alerting such as the Pervade Software suite of products, is the ideal strategy to achieve complete security monitoring. Unified systems allow for your monitoring to grow with your needs meaning that there are no cracks between systems from different vendors and no reconfiguration is needed for previously achieved layers as you grow.

Hierarchy of Monitoring Needs

Advanced Visibility	Intelligence Gathering (Dark Web & Threat Feeds)	ce internal monitoring has been configured, acquisition of external data should be used to assist with security rules and better understand potential risks to the organisations IT estate as well as employees, reputation and brand
	Traffic Flow and User Behavior Analysis	Traffic flow and user behaviour analysis allow for further visualisation of 'normal' activity on systems, allowing for the detection of events outside this 'normal' to be sent to the security team to investigate using data from the below layers
Advanced	File Integrity	With lower levels designed to monitor the confidentiality and availability of data and systems, it is time to look at the integrity of data within the systems helping to limit access control issues and illegal tampering
	Vulnerability Scanning & Penetration Testing	As security needs mature, testing becomes key to any monitoring strategy with regular vulnerability scanning and penetration tests creating the cornerstone of this advanced strategy
Basic Security	Config & Asset Auditing	This layer is used to augment SIEM Data. SIEM data will alert that an event occurred, Config and Asset Auditing will detail what happened. This layer also assists with technical GRC
	SIEM	Introducing security & event monitoring via log analysis is essential when trying to monitor activity, giving an insight into changes and anomalies on a network
Basic Visibility	Performance	Understanding performance of all devices within an estate allows for understanding of problems and future needs such as capacity planning
	Health and Availability	At the heart of all monitoring strategies should be the visibility of all assets including status and health issues

About Pervade Software

Pervade Software has been named one of the most innovative cyber security companies in the UK and is the creator of OpViewTM, OpIndexTM and OpAuditTM.

Thanks to award-winning new architecture, OpViewTM can collect, correlate and display every data type, OpIndexTM can search and index Dark Nets with the highest degree of accuracy & detail and OpAuditTM can capture both technical and manual compliance evidence. All of this functionality is enabled from a single configurable portal-based system.

The products are used by a wide range of private and public sector clients across all verticals operating in more than 80 countries.



Pervade Software has been recognised as "one of the Most Innovative Cyber Security Companies in the UK". We are an independent software vendor with strong roots in the capital of Wales and our award-winning software is used by Law Enforcement, Public Services and Businesses in more than 80 countries

Security Monitoring

OpView[™] is the most flexible security monitoring system on the market which leverages a completely new database architecture to collect, correlate and report on all data types so you can successfully monitor security (SIEM), vulnerability, configuration & availability (SOC), performance, asset & flow (NOC) all in a single configurable system.

- ✓ Collect any data, from any device on any network
- Cross-datatype correlation
- ✓ Create and edit tabs, dashboards and charts.
- ✓ Built-in incident management system
- √ Forensic analysis at lightning speeds
- ◆ Design and run comprehensive reports















Compliance Tracking

OpAudit[™], the platform behind Cyber Essentials, is a brand new kind of compliance tracking solution which gathers & manages all compliance evidence in a single system to track answers & evidence from contributors (Attestations), technical data from devices (Audit) and questionnaires from staff/supply chain (Assessments) for external & internal policies and audits.

- √ Attestations answer questions upload evidence
- √ Assessments questionnaires to staff & suppliers
- ✓ Auditing data from devices for technical controls
- ✓ Policy Builder build your own assessments
- √ Unified Control Framework answer questions once
- ✓ Custom Fields gather rich business intelligence















Dark Web Intelligence Gathering

OpIndex[™] is the most accurate and comprehensive Dark Web Intelligence solution on the market with unique Spider software custom-built to circumvent anonymisation measures and circumnavigate routing relays in order to Search and/or Index content with Reporting and Alerting to disrupt threat actors who operate in the Dark Web.

- ✓ Search Content for Key Words, Metadata & Images
- ✓ Target by URL, IP or use Recursive Searching.
- √ Scan Dataleaks and Hacker Message Boards
- ▼ Threat Hunting and Counter Intelligence
- ✓ Real-time Alerting with Configurable Rules
- ✓ Auto-Report to Action Fraud and Service Providers













