primend

Primend Shield

Cyber Incident Monitoring and Management Service

- **Keep your data secure!**
- **Make cybercriminals and malicious employees accountable!**
- **Achieve compliance with cybersecurity legislation!**

Primend Shield managed cybersecurity service integrates centralized security logging, responding to cyber threats, and cybersecurity consultations.

Average breach lifecycle is 287 days (Blumira and IBM, 2021). The reasons for breach may be a zero-day bug or an unpatched system, but often a breach is caused by an uninformed user or malicious actions of an authorized user. Bug related breaches or direct attacks can be detected rapidly and contained with automated countermeasures. The malicious type of breaches are hard to detect and require evidence for legal action.

What is Primend Shield?

Primend Shield's centralized Security Information and Event Management (SIEM) system collects security event evidence from servers, computers, firewalls, and other networked devices. Collected logs are stored for at least one year for pattern recognition, intelligence training, and as legal evidence.

Automated response system that has been trained on recognized patterns, will instantly respond to discovered malicious activity and initiates predefined mitigation scenarios. SIEM system enables integration with any networked system.

Primend Shield Team audits security event logs and maintenance logs daily to discover new attack patterns, possible breaches of systems not discovered by pattern recognition, and systems that have dropped connectivity to SIEM system. New patterns and responses are defined as they are discovered, and mitigation scenarios approved.

Microsoft Sentinel SIEM that Primend Shield service uses for collecting and analysing security events has been named by Forrester research as a leader in Security Analytics platforms with innovation roadmap, product security, case management, and architecture as the best in industry.

According to a 2021 report by Blumira and IBM, the average breach lifecycle takes 287 days, with organizations taking 212 days to initially detect a breach and 75 days to contain it.

Examples of events that Primend Shield SIEM system is trained to detect:

- User is copying abnormal number of files from a file server (malicious employee)
- New privileged account has been created
- Firewall is being scanned for vulnerabilities
- A virus has been detected in multiple computers
- Organization has been targeted by a phishing attack
- Access to company's sensitive documents at unusual times
- User authentications and data access from unusual locations

System & Services

Servers | Database | Microsoft 365 | Firewalls & Switches | Computers & Phones

Cloud Platform

Event Monitoring | Log Storage | Pattern Detection | Automated Actions

Certified Specialist

Event Monitoring | Rapid Response | Audit & Analysis | Reporting & Consulting

Contact

Joosep Truu | Sales manager

joosep.truu@primend.com

primend

bm certification

ISO 9001
ISO 27001
System certification