Cyber Spear
PRECISE THREAT DETECTION

Cyber Spear **Persistence**

Benefits

- **Clean operation** - Confidence in the integrity 'cleanliness' of the IT environment
- **Detect APTs** - Detection of attacks that bypassed existing security prevention layers
- **Avoid IT Flooding** - Minimal number of ambiguous cases
- **Zero Impact** - On privacy, availability and performance
- **Agentless Solution** - No agent installation required

Cyber Spear Persistence is an agentless solution that accurately detects sophisticated cyber-attacks such as Advanced Persistent Threat (APT), without flooding the IT department with inconclusive 'gray' findings.

The Cyber Spear Persistence process begins by collecting indicators from workstations, servers and the network. It then persistently mines the collected data in order to detect the presence of malicious activity, by using a comprehensive set of Automated Analysis Processes. Then, in order to minimize the number of ambiguous cases, suspicious activities and items are investigated by analysts at the Cyber Spear Security Operation Center (SOC).

The Cyber Spear Persistence solution can be installed within hours, and requires virtually no IT resources for operation and maintenance. In ongoing operation, the agentless solution does not impact data/user privacy, availability or performance. It ensures that your environment remains 'clean' and provides the most effective and comprehensive attack detection.

1 Collect Indicators

From workstations, servers and the network

2 Automated Analysis Process

Baseline comparisons, anomaly correlation rules, behavior analysis, reputation & signature checks

3 Expert Human Analysis

Done in Cyber Spear's Security Operation Center (SOC)

The Result: **Precise Threat Detection**

- The threats are detected
- The network is cleansed
- Minimal ambiguous warnings