When Minutes Count

Fight advanced threats with real-time SIEM and eight key indicators of attack.

Time Is Crucial

Companies with early attack detection skills are faring best against targeted attacks.

57% Experienced **10 or fewer** targeted attacks last year.

12% Of agile organizations investigated **more than 50 incidents** last year.

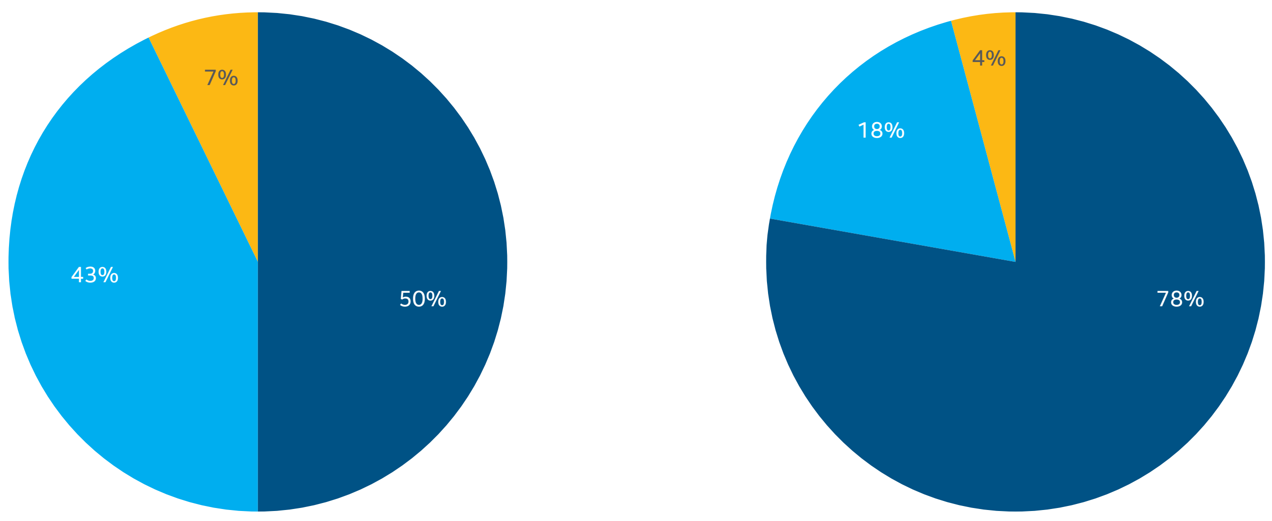
5 Out of 8 Most useful indicators of attack **rely on time.**

52% Of companies that are least concerned about attacks **have a real-time SIEM.**

McAfee, part of Intel Security, commissioned Evalueserve to perform a health check on organizational abilities to deal with advanced and targeted attacks.

Is Your SIEM Real Time?

Current security efforts and checkbox compliance are not sufficient for data protection.



50% of the organizations surveyed **have no SIEM** or inadequate SIEM solution.

78% of those able to detect **attacks in minutes** have a real-time, proactive SIEM.

- 🟦 Real-time SIEM
- 🟦 Inadequate SIEM
- 🟨 No SIEM

Today's SIEM is a security intelligence solution that can analyze security events, flow, and log data in real time, correlating this information with contextual data. It is a focal point for internal and external threat management and can collect, store, analyze, and report on log data for regulatory compliance and forensics.

Why Every Minute Counts

Using IoAs provides a way to shift from reactive cleanup/recovery to a proactive mode.

1. **Off-hour** malware detection.

2. Internal hosts **scanning multiple other** internal hosts in a short time-frame.

3. Multiple alarm events from a single host or **duplicate events across multiple machines** in the same subnet over a 24-hour period.

4. A freshly cleaned system is **re-infected with malware** within 5 minutes.

5. User account **trying to login** to multiple resources within 10 minutes from/to different regions.

Indicators of Attack (IoAs) are events that could reveal an active attack before indicators of compromise become visible, allowing for earlier and more definitive action to disrupt attacks.

Visit www.mcafee.com/siem

intel Security