McAfee Investigator

Transform analysts into expert investigators

McAfee® Investigator helps analysts close more cases faster with higher confidence that they've determined root cause. Triaged alerts trigger expert-led exploration of relevant SIEM and real-time endpoint data. Security operations centers (SOCs) can efficiently investigate malware, network threats, and indicators of compromise (IoCs) using automation, expertise, and artificial intelligence.

SOC Challenges

Huge event volumes and data shelf-life issues make it hard to accurately assess the importance and extent of an alert. Analysts often ignore alerts because they lack the context or knowledge to decide if it should be treated as a formal incident.

Investigations of any selected incidents can then take a long time and substantial expertise across threat vectors to dig to the core of the problem. These trends mean the need for skilled SOC analysts is growing, while the available talent pool is not.

New Investigative Analytics

Mature SOCS are tackling this problem with automation and sophisticated analytics to facilitate rapid time to close while identifying root cause, according to McAfee research.[1]

McAfee Investigator places advanced automation and analytics in reach of every SOC. As a SaaS offering, expert systems and endpoint capture tools integrate with existing data sources and security management systems for rapid time to value and minimal effort.

These interactive analytics provide automation, knowledge, and continuously updated guidance to empower incident responders to fully investigate malware, network threats, and IoCs in less time and with increased accuracy.

Triage accurately and quickly

Investigator improves triage immediately by permitting security operations to automate prioritization of certain situations for immediate attention. For these alarms, as well as other alerts an analyst wants to explore, McAfee Investigator collects, organizes, summarizes, and visualizes the alerts, activity, evidence, and intelligence gathered on a suspected attack.

Key Benefits

- **Reduce dwell time:** Thorough exploration of case data increases root cause detection rather than remediating a symptom.
- **Shift from alerts to cases:** Reduce time spent on manual and low-priority investigations.
- **Focus on the unknown:** Zero in on the unique artifacts and insights that need human interpretation and decisions.
- **Improve triage:** Process more cases more quickly with higher quality.
- **Reduce analyst burnout:** Make the best use of finite time, energy, and cognitive capacity.
- **Build analyst skills:** Guidebooks and relevant insights educate analysts about the right questions and hypotheses within the workflow.
- **Extend value of current systems:** Existing data sources and analytics are enhanced to increase focus and accuracy.

Relevant data is collected in the background and includes only the insights important to a specific threat investigation that will trigger a decision. Data from security information and event management (SIEM) solutions can be augmented with data from endpoints, without requiring endpoint detection and response (EDR) agents at every node. This model replaces silos with contextual visibility into IoCs, tactics, techniques, procedures, and relationships.

A data analytics and machine learning engine compares evidence data against known baselines and threat intelligence sources. It processes artifacts and elevates key suspicious insights.

By collecting and prioritizing the right data automatically, McAfee Investigator reduces the effort and increases the speed with which analysts can determine the risk and urgency of the incident. Analysts can make accurate triage decisions faster and focus on the most significant threats.

At an organizational level, the benefits multiply. By up levelling triage from alert reviews to contextual cases, each analyst can be more efficient, more cases are dispositioned by Tier 1 analysts, and analyst time is spent on the highest value activities.

When an incident is chosen for a detailed investigation, analysts leverage interactive guidebooks that focus analysts on what is important as they scope and assess. Investigative guidebooks are not script-based or static. The system mimics the human brain, exploring many hypotheses in parallel for maximum speed and accuracy.

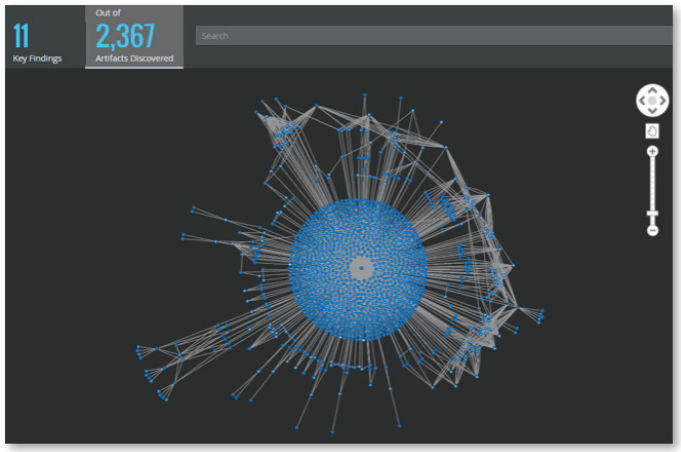

Figure 1. McAfee Investigator collects thousands of pieces of evidence.

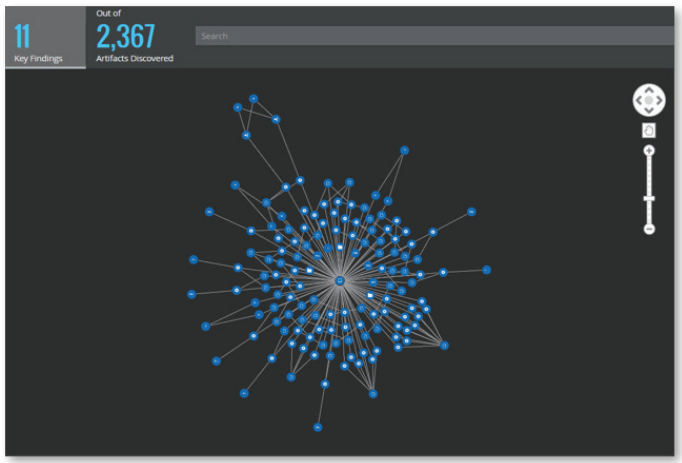

Figure 2. McAfee Investigator then applies expert analytics and guidance to present the findings that matter.

Key Features:

- Precise on-demand data collection
- Dissoluble endpoint collection agent
- Interpretation of gathered data based on expert guidance and artificial intelligence
- Interactive visualizations
- Multivector hypotheses to explore likely data
- Baselines for institutional intelligence
- Case management specifically for investigations

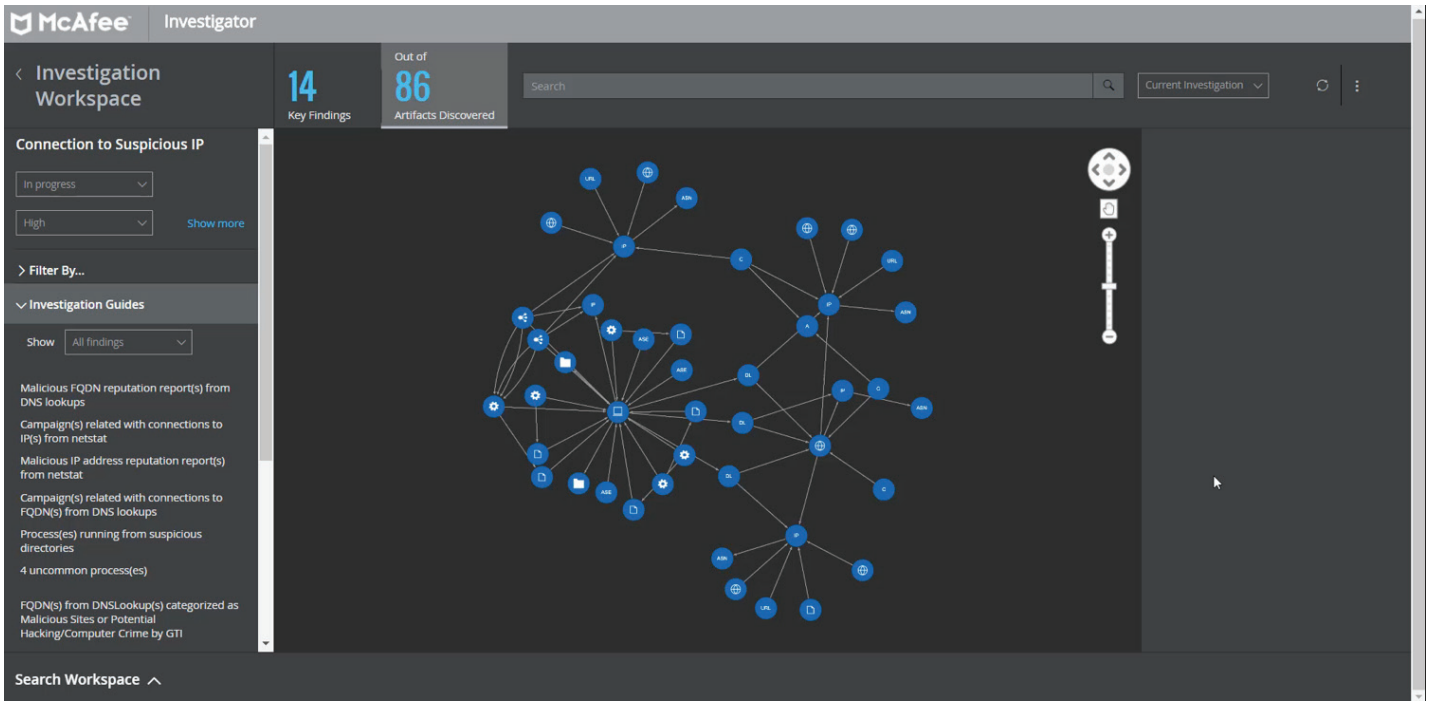

Figure 3. The workspace makes key findings obvious and easy to explore.

The human-readable guidebooks were built with a combination of Foundstone® researcher expertise and artificial intelligence. This is one way McAfee Investigator embodies human-machine teaming.

The workspace structures case insights and findings to help analysts pose the right questions. This focused, multivector exploration yields efficient, accurate case closure with high confidence that analysts have identified root cause.

Enhance skill and collaboration

McAfee Investigator's interactive workspace continues McAfee innovation in user interface. It prompts workflows and navigation through data within a single cognitive environment. This model reduces the information strain generated from the multitude of alert types and eliminates the need to review multiple screens.

The workspace coaches novice and intermediate analysts to implement the thought processes of advanced analysts, building skills without separate training. The workspace also activates case workflows to simplify access, recording, sharing, and updating of cases across teams. Consistent sharing of data is especially important with the tiers and distributed teams that characterize security operations centers.

Build on existing tools and data

McAfee Investigator works with a SIEM and McAfee® ePolicy Orchestrator® software to add advanced analytics to existing data sources, baselines, correlations, and alerts. A dissoluble agent collects fresh endpoint data that is especially crucial to accurate interpretation of subtle evidence. Professional services expedite onboarding and successful activation.

Learn More

With McAfee Investigator, once you have a suspicion, you don't need to spend hours collecting data and even more time interpreting the data. The advanced analytics engine behind McAfee Investigator inspects and triages threat alerts within a context-driven interface to scale security operations. McAfee Investigator automates use of expert knowledge in SOC investigations, allowing your analysts to work smarter, faster, and with greater accuracy.

This is human-machine teaming.

Visit **mcafee.com/investigator** to learn more.

1. https://www.mcafee.com/us/resources/reports/restricted/rp-disrupting-disruptors.pdf

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com