SOLUTION NOTE

SOC INSIGHTS

Apply AI-driven analytics to turn vast amounts of event, network, ecosystem and DNS intelligence data into actionable insights to elevate SecOps efficiency

BARRIERS TO SECOPS EFFICIENCY

As with other functions of business or government organizations today, the modern security operations center (SOC) struggles to do more with available resources. According to the SANS 2023 SOC Survey,[1] 80 percent of the top 10 SOC barriers to making full use of SOC capabilities fall into three areas:

- Understanding and dealing with alerts
- Integrating or automating tools
- Performing key tasks with available staff and skills

But the most truly tragic statistic may be that all these barriers have been challenging the SOC for over a decade. The incremental improvements from simply auto-prioritizing incidents based on malware rankings and other basic filters have not been able to keep pace with the growth of alerts and other events that may need SOC analyst attention. So, things have only become worse.

AI-DRIVEN SOC INSIGHTS

Modern persistent threats depend on flexible attacker infrastructure and dynamic command-and-control (C2) systems to host and deploy the numerous pen-test, exploit, encryption and other tools involved in even a single attack. This makes them extremely dependent on DNS and highlights a key weakness that defenders can exploit to detect and disrupt these threats.

DNS sees legitimate and malicious activity regardless of protocol, platform, OS, application or even location. With this unique visibility, a pilot program under the director of the Cybersecurity Directorate at the National Security Agency (NSA) revealed that securing DNS can reduce malware attacks by 92 percent.[2]

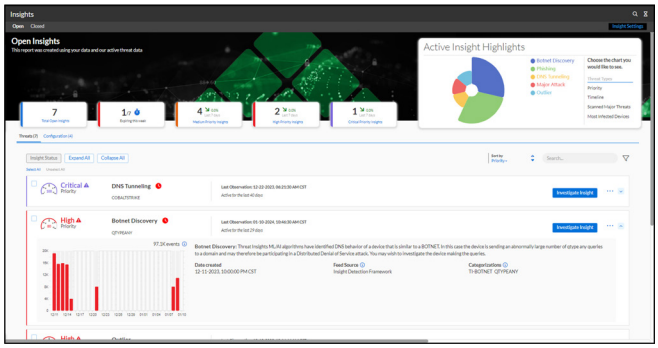


Figure 1. The SOC Insights Summary page provides analysts with one-click access to what matters most

FACTS & FIGURES

- 60% of SOC analysts say their workloads are growing and 65% are likely to change jobs in the next year.[4]
- 55% of survey respondents say that critical alerts are being missed often on a weekly and even daily basis.[5]
- 64% of analysts say manual work eats up more than half of their time.[4]
- Misconfiguration is one of the top three factors in error-related breaches.[3]
- Eight of the top 10 barriers preventing full SOC utilization involve alerts, tool integration and skill shortages.[1]
- 77% of CEOs are worried about the availability of key skills.[6]
- 92% of malware and C2 activity can be controlled at the DNS layer with the right DNS intelligence and visibility.[2]

SOC Insights works with Infoblox's Protective DNS solution, Infoblox Threat Defense™, to offer unique AI-driven analytics to detect unknown threat activity that other tools miss, raise SOC efficiency and improve the overall return on investment (ROI) of current security investments.

SOLVING MULTIPLE PROBLEMS WITH A RANGE OF INSIGHTS

Post-incident or -breach investigations often reveal that early indicators of malicious activity were missed due to misconfigurations, security tool integration challenges or simple alert overload. SOC Insights applies AI-driven analytics to a vast amount of data to help address these risks.

Security Insights

The Security add-on for SOC Insights is available for Infoblox Threat Defense Business Cloud or Advanced, uses AI to distill vast amounts of event, network, ecosystem and DNS visibility, and intelligence into a manageable set of actionable, security insights.

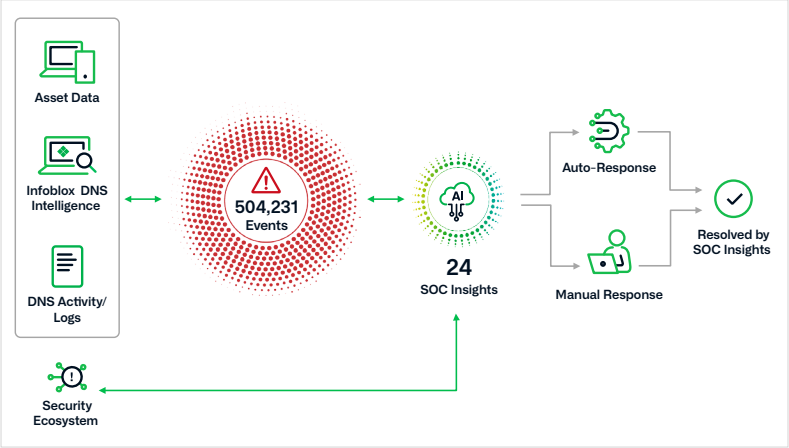


Figure 2. Let SOC Insights eliminate alert overload, distilling mountains of events into a more manageable set of meaningful, actionable insights

- Zero Day DNS™
- Persistent Threat
- Active Threat Spreading
- Major Attack
- Botnet Discovery
- Outlier Communication
- Phishing
- Malware
- Open DNS Resolver
- DNS Tunneling
- Data Loss Activity
- Targeted Attack
- Excessive DNS Errors
- Monitored Lookalike Domain

Configuration Insights

The Configuration feature of SOC Insights is included with Infoblox Threat Defense Business Cloud and Advanced to help users ensure they are taking full advantage of current best practices and avoiding common mistakes. Follow videos and other guides to help address mistakes and weaknesses, or deactivate unnecessary warnings for allowed exceptions.

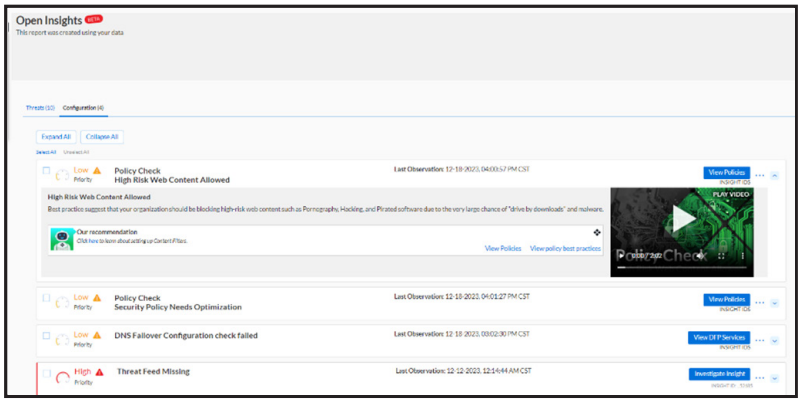


Figure 3. Proactively identify weak or dangerous configuration errors to ensure optimal defense, investigation and response capabilities

- DNS Threat Feed Missing
- VirusTotal Free Key Missing
- Security Policy Needs Optimizing
- DNS Failover Check Failure
- Feed Action Mismatch
- DFP Hiding Asset Details
- Security Policy in Logging Mode
- Web Content Filters OFF
- High-Risk Web Content Allowed

A POSITIVE FINANCIAL, OPERATIONAL AND BUSINESS IMPACT

While most security tools can promise little more than "ease of use" and "fewer breaches," SOC Insights can do much more, ranging from reducing analyst stress and turnover to reducing many security concerns from expansion, mergers and acquisitions (M&A), and other business initiatives. For example:

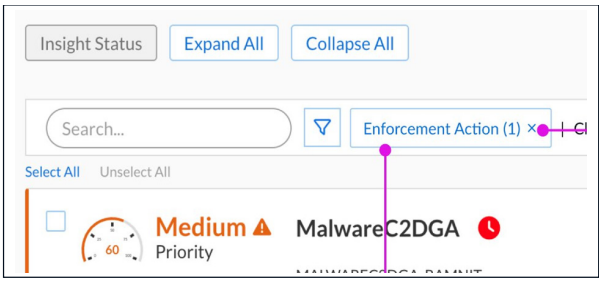
- The nature of DNS makes it easy to unify a new location or business partner onto a common DNS infrastructure in minutes, rather than months.
- Configuration insights are highly proactive to help mitigate breaches or data loss due to "misconfiguration"—one of the top three factors reported in error-related breaches.[3]
- Autocorrelation of malware, phishing, botnet and other major or spreading activities empowers responders to address many threats at once, raising their efficiency.
- Move to a more proactive security posture with the ability to monitor insight categories such as outliers, DNS tunneling and open resolver, as well as Infoblox Threat Defense's unique lookalike and application visibility features.
- Intelligence integration of the security ecosystem improves the ROI of the entire security stack by offering actionable insights instead of just raw logs and events.
- SOC Insights auto-collects relevant data and enables analysts to see and pivot around that data to reach conclusions faster and with greater confidence. This contributes to lower stress and higher retention of skilled and experienced security professionals.

POWERFUL FEATURES, AMAZING RESULTS

SOC Insights includes three powerful features that simplify and streamline SOC workflows: Asset Enrichment, Enforcement Prioritization and Traffic Exclusion. These additions help security teams maintain operational momentum and improve their response tempo. Analysts can now investigate incidents faster, respond more efficiently and boost overall effectiveness.

Asset Enrichment provides detailed context about devices, making it easier to assess the scope of an incident. Rich attribute collection now includes IP, MAC, hostname, VLAN, network info, device category and location.

Enforcement Prioritization highlights unblocked threats first, allowing teams to act quickly on the most urgent and potentially threatening issues.



Traffic Exclusion filters out irrelevant data, such as guest network traffic, so analysts can stay focused on what matters. In the "Insight Setting," the user can add exclusion traffic for insight generation. It can be based on subnet or DNS forwarding proxy (DFP).

Together, these features improve SOC performance, save valuable time and increase ROI. Faster investigations also help reduce the risk and impact of cyberthreats. Customers report significant benefits using SOC Insights with Infoblox Threat Defense, including:

- A 50 percent reduction in EDR and FW alerts
- An average of 500 SOC analyst hours saved per month
- $400,000 in productivity savings realized per year

UPLIFT SIEM, SOAR AND OTHER PARTS OF THE ECOSYSTEM WITH INSIGHTS

SecOps knows the value and limitations of sharing raw data around the security ecosystem. This has made SIEM and SOAR expertise one of the most challenging skill sets for most organizations. SOC Insights takes the burden off these other tools and can share the resulting insights across the security stack to make other tools more effective, further uplifting overall SecOps efficiency.

1 *SANS 2023 SOC Survey*, Cowley, Chris, Filkins, Barbara, Pescatore, John, SANS Institute, June 13, 2023.
2 *NSA launches pilot program to secure defense contractors*, Williams, Lauren, C., NEXTGOV/FCW, June 18, 2020.
3 *2023 Data Breach Investigations Report*, The Verizon DBIR Team, Verizon, 2023.
4 *2022 Voice of the SOC Analyst*, Tines, 2022.
5 *The Orca Security 2022 Cloud Security Alert Fatigue Report*, Galea, Deborah, Orca Security, 2022.
6 *Five challenges to cloud adoption and how to overcome them*, PwC, 2021.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20250611v3