



SONICSENTRY

SOC in Action: The Lifecycle of a Cyber Threat

The SonicSentry Security Operations Center (SOC) defends our customers 24 hours a day, 7 days a week. When an alert or threat comes in to the SOC, the team jumps into action. Here's how.



SonicSentry Security Operations Center monitors for alerts and abnormal behavior 24 hours a day to protect our MSP partners and their clients from cyber threats. When alerts come in from security tools, a SOC analyst investigates.



Alerts are classified as minor, major, or critical alerts. The SOC team sets rules and configurations that automatically classify alerts, and then the SOC analyst can upgrade or downgrade the alert as necessary.



Minor alerts are used for abnormal activities on endpoints, such as files being quarantined in unusual folders. They have a high likelihood of false positives. The SOC will contact you by email if further investigation is recommended.



Major alerts are used when there is confidence of malicious activity on the endpoint. Often this activity was stopped by security tools, such as malware being quarantined automatically by a next-generation antivirus. The SOC will contact you by email with recommended follow-up, such as additional phishing training for end users.



When there is high confidence of a breach or compromise actively occurring, that's a critical alert. The SOC team jumps in to quickly minimize the damage and keep the compromise from spreading further across your network.



During a critical alert, the SOC team will call the emergency phone number you provided every 15 minutes for the first hour, then every hour after that if you don't answer. However, they won't wait for you to answer to begin defending you; they will immediately take whatever actions are necessary to stop the attack and protect the rest of your environment, typically by isolating endpoints.



The SOC analyst will create a report to document what happened, the scope of the incident, and any other areas of impact. The SOC will also make recommendations for your next steps.



Once the active threat is removed, you can work with your customer to repair their network, restore any isolated endpoints to a known-good state, and follow through on any other remediation needs.

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.

© 2025 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or

sonicwall.com



SONICWALL®