ALERT LOGIC®

SOC 2 COMPLIANCE:
STEP-BY-STEP PREPAREDNESS GUIDE

SaaS companies and service providers who use the SOC 2 requirements to secure their customer data benefit from an improved overall security posture, better performance and availability of service delivery and a valuable risk assessment tool for prospective business partners.

Complying with the SOC 2 trust service principles can be particularly challenging because they require a combination of security tools, threat intelligence. This is where Alert Logic is uniquely positioned to help with a security platform, threat intelligence and experts:

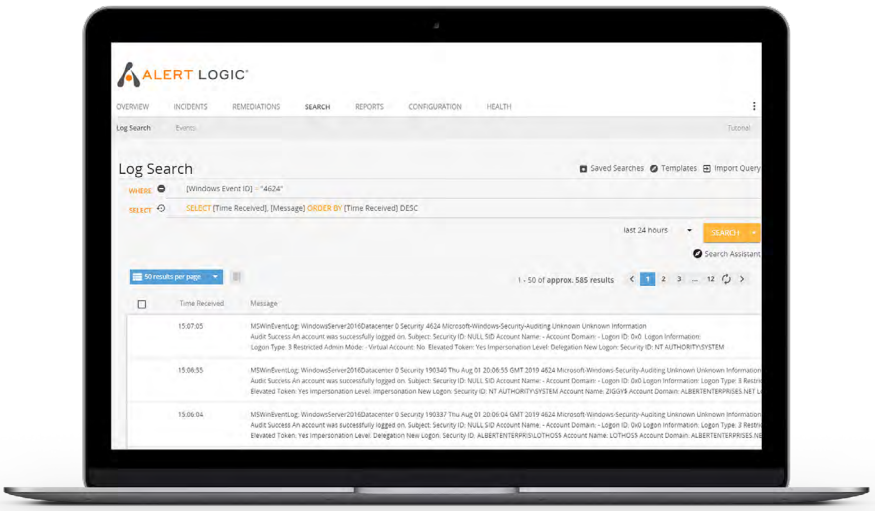
- Protect all systems against malware
- Develop and maintain secure systems and applications
- Track and monitor all access to network resources and cardholder data
- Run vulnerability scans at least quarterly, and after any significant change in your network
- Implement an Incident Response Plan

Alert Logic will help you capture the right data, minimize storage requirements, so you can address these SOC 2 trust service principles, and trace activity to gain a deeper understanding of what happened when an event occurs.

To Learn more about the Alert Logic Console and Reports, visit the Alert Logic documentation page

LOG MANAGEMENT

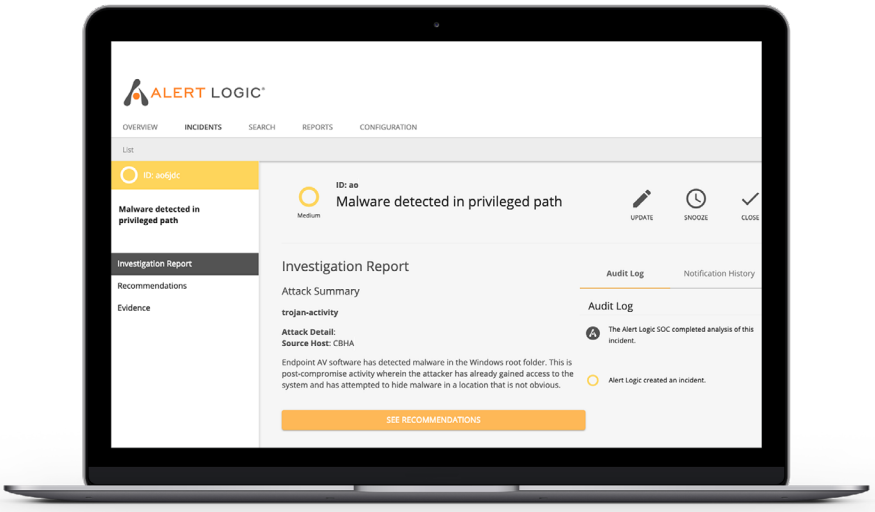
- LOG MANAGEMENT USERS
- LOG MANAGEMENT DEPLOYMENT
- LOG MANAGEMENT TRAFFIC
- LOG RETENTION SETTINGS
- LOG SOURCES
- LOG SEARCH STATS
- LOCAL APPLIANCE ACCESS LOGS
- APPLIANCE & AGENT HEALTH
- NOTIFICATION POLICIES



Alert Logic collects, aggregates and normalizes log data whether it originates in your own data center, a hosted environment or the cloud. You get a unified view into all your data, with tools. Alert Logic provides hundreds of pre-built reports, saved views, and dashboards to meet many of your security and compliance requirements on day one. It's easy to correlate events and set automatic alerts and reporting to enable rapid response to security events to rapidly uncover the insight and alerts you need to remain secure and compliant.

MALWARE PROTECTION

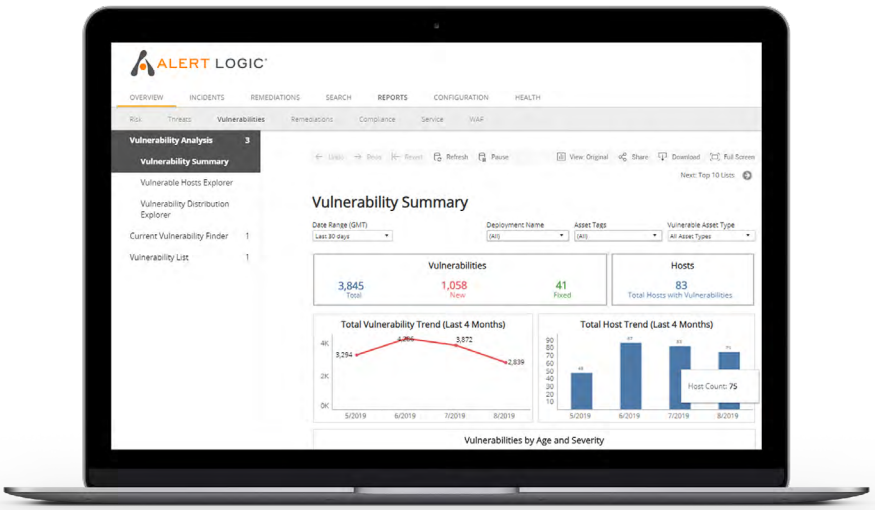
- AUTOMATICALLY GATHER NEW MALWARE AND GOODWARE SAMPLES
- CONTINUOUSLY TRAIN PROTECTION MODELS AGAINST NEW SECURITY THREATS
- TAILOR PROTECTION MODELS BASED ON ORGANIZATION PROFILE
- MAXIMIZE PROTECTION AND MINIMIZE FALSE POSITIVES

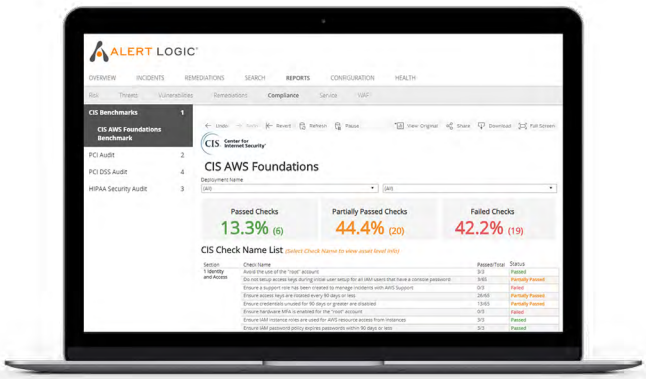


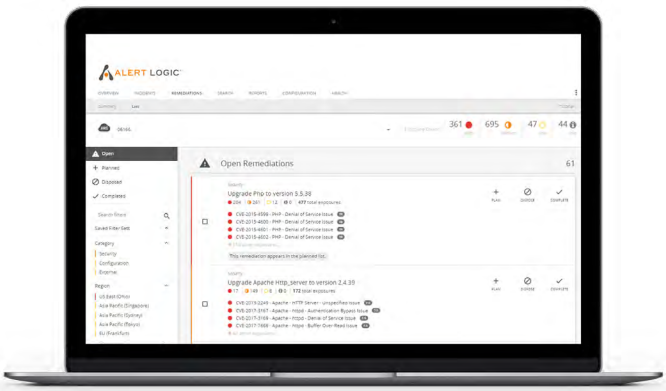
The Alert Logic Console – Event Viewer will display the latest malware attempts to help you meet SOC-2 service trust principles.

VULNERABILITY MANAGEMENT

- INTERNAL SCAN SCHEDULE
- INTERNAL SCAN RESULTS
- PCI ASV SCAN SCHEDULE
- PCI ASV SCAN RESULTS
- NEW VULNERABILITY CHECKS
- CIS BENCHMARK SCAN RESULTS
- CONFIGURATION REMEDIATIONS
- SECURITY REMEDIATIONS
- TRI SCORES



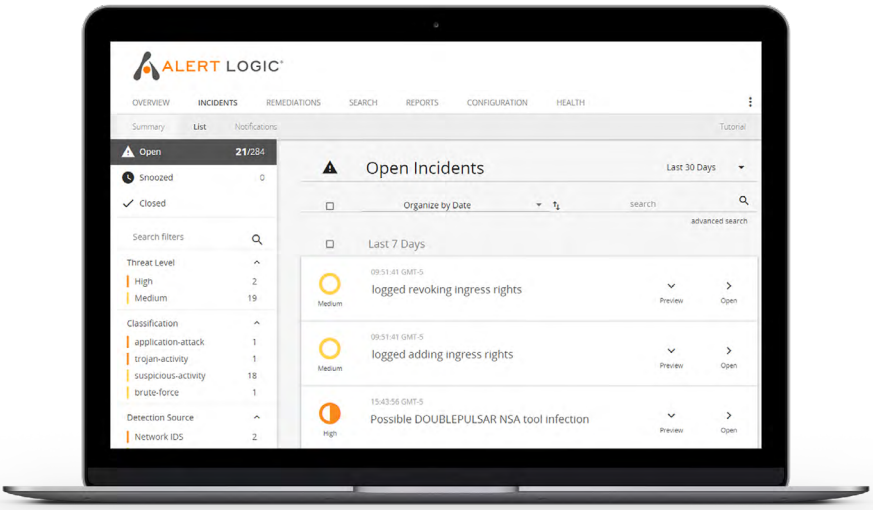




Alert Logic is an approved PCI Scanning vendor. Through the Alert Logic console, you can schedule external scans that can assist in SOC-2 compliance preparedness.

THREAT DETECTION

- NETWORK IDS DEPLOYMENT
- PROTECTED NETWORKS & HOSTS
- NETWORK IDS TRAFFIC
- NETWORK IDS EVENTS
- NETWORK IDS INCIDENTS
- DEPLOYED IDS SIGNATURES
- SIGNATURE UPDATE HISTORY
- LOG REVIEW INCIDENTS
- LOG MANAGEMENT INCIDENTS
- LOG CORRELATION POLICIES
- WEB APPLICATION IDS INCIDENTS
- APPLIANCE & AGENT HEALTH
- NOTIFICATION POLICIES

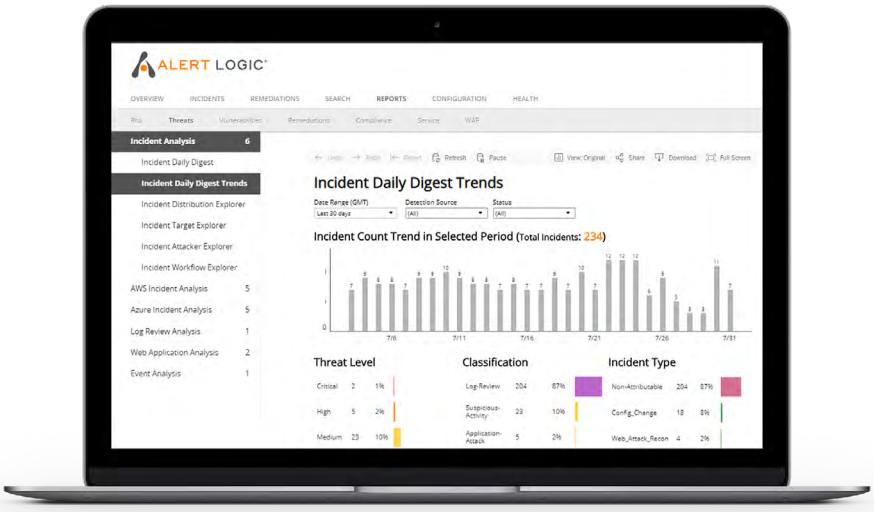


Alert Logic uses colors and icons to help you easily identify the threat levels of exposures.

High Medium Low Info

THREAT RESPONSE

- CURRENT ESCALATION CONTACTS
- INCIDENT NOTIFICATION CONTACTS
- ESCALATED INCIDENTS
- INCIDENT WORKFLOW ACTIONS
- MONTHLY LOG REVIEW
- WAF BLOCKING
- ALERT PREFERENCES



Alert Logic provides you with information about the exposure, including threat level, evidence, and recommendations to address the exposure.

DETAILED SOLUTION MAPPING FOR SOC 2 COMPLIANCE

SOC 2 (TSP 100)	ALERT LOGIC ESSENTIALS	ALERT LOGIC PROFESSIONAL	ALERT LOGIC ENTERPRISE
CC3.2 - Risk Identification	•	•	•
CC6.6 - External Threats	•	•	•
CC6.8 - Unauthorized and Malicious Code Protection	•	•	•
CC7.1 - Configuration and Valnerability Management	•	•	•
CC6.2 - User Registration		•	•
CC6.3 - Access Modification and Removal		•	•
CC7.2 - Security Event and Anoimoly Detection		•	•
CC7.3 - Incident Detection and Response		•	•
CC7.4 - Incident Containment and Remediation			•

Using these capabilities, Alert Logic helps you to address the most challenging SOC-2 compliance requirements, so you get better outcomes across your entire compliance program.

SAVE MONEY

- Single Integrated Solution.
- Suite of Security Capabilities.
- One Monthly Subscription.

STAFFING RELIEF

- Our Experts are Included.
- 24/7 Threat Monitoring.
- 15-Min Live Notifications

START FAST

- Ready-to-Use Services.
- Expert Onboarding Assistance.
- Personal Tuning & Training.

LET'S GET STARTED

SCHEDULE A DEMO | TRY IT NOW | CONTACT SALES

VISIT HTTPS://WWW.ALERTLOGIC.COM/GET-STARTED

ALERT LOGIC®