ALERT LOGIC™

SOLUTION OVERVIEW

Alert Logic™ for SOX Compliance

Introduction

The Sarbanes-Oxley Act (SOX) came into force in July 2002 and introduced major changes to the regulation of corporate governance and financial practice. By mandating the requirements for reliability and usefulness of financial reporting, SOX is designed to renew investor's trust and understanding of public corporation financial reporting.

The SOX Act provides specific details on IT and IT security including any computers, network hardware, and other electronic equipment that financial data passes through. The Act helps to ensure that proper controls are in place to prevent data breaches, prevent unauthorized users from viewing sensitive financial information and have tools ready to remediate incidents should they occur.

An independent external SOX auditor is required to review controls, policies, and procedures during a Section 404 audit and the audit requires all financial reports to include an Internal Controls Report. This shows that a company's financial data are accurate (within 5% variance) and adequate controls are in place to safeguard financial data.

SOX auditing requires that "internal controls and procedures" can be audited using a control framework like COBIT. Log collection and monitoring systems must provide an audit trail of all access and activity to sensitive business information.

Alert Logic Solutions

Using Alert Logic solutions, companies can implement a broad range of regulatory and industry security standards (such as SOC 2, PCI DSS, HIPAA, SOX, and GDPR) with less complexity, and at a fraction of the total cost and time of traditional security tools. Alert Logic integrates cloud-based software, analytics and expert services to

assess, detect and block threats to applications and cloud environments to improve your security visibility and compliance programs. We focus on the threats most relevant to cloudhosted applications by defending each layer of your application and infrastructure stack against hard-to-detect web application attacks. Integrated expert services augment your in-house security team by monitoring your cloud workloads and environment 24/7. Analyst investigate alerts and contact you within 15 minutes if we detect suspicious activity such as: unauthorized access, exposur or modification of accounts, controls or configurations.Reduce your risk of attacks with continuous vulnerability scanning and configuration inspection of your applications and cloud environments.

Quickly respond to attacks and post-breach activities with distributed IDS sensors that provide full-packet inspection and real-time alerts.
Protect customer data from network and OWASP Top 10 attacks with web application scanning and web application firewall technologies.
Prepare for audits, anytime with the event and log data you need for automated alerts, audit trails and easy access for reporting and audits, stored in our secure SSAE 16 Type 2 audited data centers for as long as you need.
Free up resources with ActiveWatch™ experts for daily log reviews and 24/7 event and threat monitoring.

Alert Logic maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, and ISO 27001-2013 certification for UK Operations.

Alert Logic SOX Solutions Mapping

The integrated services that make up Alert Logic® address a broad range of SOX requirements to help you prevent incidents that threaten the security, availability, integrity and privacy of financial and customer data.

SOX 404	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE †
DS 5.9 Malicious Software Prevention, Detection and Correction	●	●	●
DS 5.5 Security Testing, Surveillance and Monitoring **DS 5.6** Security Incident Definition **DS 13.3** IT Infrastructure Monitoring		●	●
AI3.2 Infrastructure resource protection and availability			●

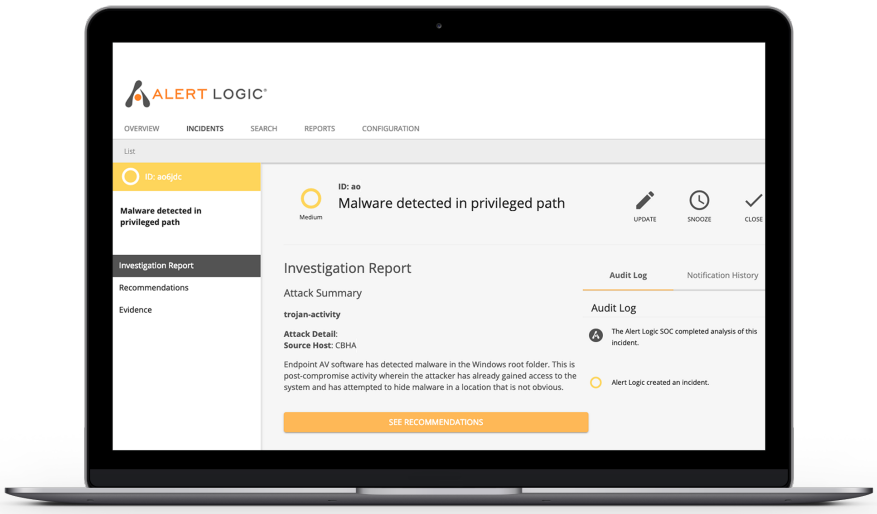
ALERT LOGIC	SOX 404
ALERT LOGIC MDR ESSENTIALS *Vulnerability & Asset Visibility* • Asset discovery • Vulnerability scanning • Cloud configuration checks • Endpoint Detection • Threat Risk Index • Compliance scanning and reporting	**DS 5.9** Malicious Software Prevention, Detection and Correction
ALERT LOGIC MDR PROFESSIONAL INCLUDES ESSENTIALS *24/7 Managed Threat Detection and Incident Management* • 24/7 Incident Monitoring & Management • Security Analytics & Threat Intelligence • Log Collection and Monitoring • Intrusion Detection • Security Event Insights and Analysis • Office 365 Log Collection & Search • Cloud Vendor Security Integrations • AWS User Behavior Anomaly Detection • Anti-Virus Integration • File Integrity Monitoring	**DS 5.5** Security Testing, Surveillance and Monitoring **DS 5.6** Security Incident Definition **DS 13.3** IT Infrastructure Monitoring
ALERT LOGIC MDR ENTERPRISE INCLUDES PROFESSIONAL *Designated Security Expert* • Continuous Threat Hunting • Pro-Active Tuning and Sensor Optimization • Weekly Security Review	**AI3.2** Infrastructure resource protection and availability

Demonstrate SOX Compliance Preparedness

Alert Logic ingests AV logs and analyzes them to provide key insights for alerting and Security Operations Center (SOC) support, such as:

Detection of known hack tools such as pwdump, wincred, and mimikatz whose presence is highly correlated with malicious post-compromise activity.

Detection of writing to privileged locations on the local system, which is indicative of a user or malware with administrative privileges – often a later stage action in the attack cycle.

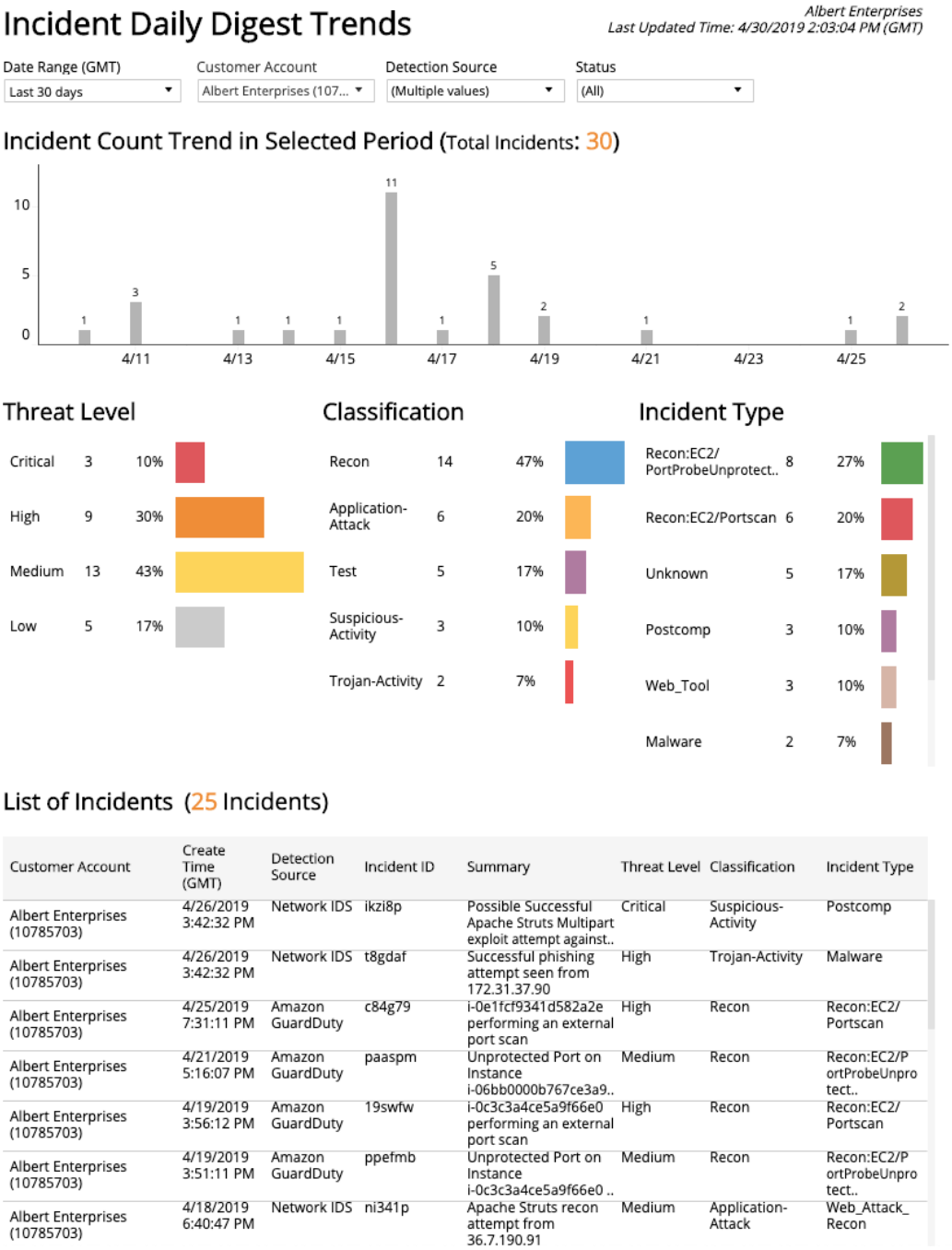


Monitor the infrastructure for security-related events

Alert Logic provides Interactive reports that provide convenient access to analysis, statistics, and trending data. The Incident Analysis report group provide valuable insights and trending data for incidents.

Incident Daily Digest - Threat status of your infrastructure from incidents detected on the previous day for the selected detection types.

Incident Daily Digest Trends - Histogram chart that allows you to focus on how your threat landscape of detected incidents has evolved within the specified date range.



Incident Daily Digest Trends

Albert Enterprises
Last Updated Time: 4/30/2019 2:03:04 PM (GMT)

Date Range (GMT): Last 30 days | Customer Account: Albert Enterprises (107... | Detection Source: (Multiple values) | Status: (All)

Incident Count Trend in Selected Period (Total Incidents: 30)

Threat Level

Critical	3	10%
High	9	30%
Medium	13	43%
Low	5	17%

Classification

Recon	14	47%
Application-Attack	6	20%
Test	5	17%
Suspicious-Activity	3	10%
Trojan-Activity	2	7%

Incident Type

Recon:EC2/PortProbeUnprotect..	8	27%
Recon:EC2/Portscan	6	20%
Unknown	5	17%
Postcomp	3	10%
Web_Tool	3	10%
Malware	2	7%

List of Incidents (25 Incidents)

Customer Account	Create Time (GMT)	Detection Source	Incident ID	Summary	Threat Level	Classification	Incident Type
Albert Enterprises (10785703)	4/26/2019 3:42:32 PM	Network IDS	ikzi8p	Possible Successful Apache Struts Multipart exploit attempt against..	Critical	Suspicious-Activity	Postcomp
Albert Enterprises (10785703)	4/26/2019 3:42:32 PM	Network IDS	t8gdaf	Successful phishing attempt seen from 172.31.37.90	High	Trojan-Activity	Malware
Albert Enterprises (10785703)	4/25/2019 7:31:11 PM	Amazon GuardDuty	c84g79	i-0e1fcf9341d582a2e performing an external port scan	High	Recon	Recon:EC2/Portscan
Albert Enterprises (10785703)	4/21/2019 5:16:07 PM	Amazon GuardDuty	paaspm	Unprotected Port on Instance i-06bb0000b767ce3a9..	Medium	Recon	Recon:EC2/PortProbeUnprotect..
Albert Enterprises (10785703)	4/19/2019 3:56:12 PM	Amazon GuardDuty	19swfw	i-0c3c3a4ce5a9f66e0 performing an external port scan	High	Recon	Recon:EC2/Portscan
Albert Enterprises (10785703)	4/19/2019 3:51:11 PM	Amazon GuardDuty	ppefmb	Unprotected Port on Instance i-0c3c3a4ce5a9f66e0 ..	Medium	Recon	Recon:EC2/PortProbeUnprotect..
Albert Enterprises (10785703)	4/18/2019 6:40:47 PM	Network IDS	ni341p	Apache Struts recon attempt from 36.7.190.91	Medium	Application-Attack	Web_Attack_Recon