LogicHub

USE CASE

DLP Alert Triage

Data Loss Prevention (DLP) protects an organization's most precious commodity: its data. By monitoring the flow of data by email, web protocols, and transfer to portable media such as USB sticks, DLP systems enable organizations to detect, block, and investigate suspicious activity that could lead to sensitive data leaving the organization. This is mission-critical work, protecting intellectual property and other confidential data such as customer records, and helping organizations ensure they comply with data privacy and data security regulations, which could include Gramm-Leach-Bliley, HIPAA, the California Consumer Privacy Act, and the EU GDPR.

Of course, even in small organizations, there's a high volume of email and file transfers for DLP systems to monitor. Larger Security Operations Centers (SOCs) receive as many as 10,000 DLP alerts per week.

Processing these alerts is time-consuming work. Security analysts often have to copy alerts from SOC email inboxes and paste them into spreadsheets. Next, analysts de-duplicate alerts, sometimes by comparing timestamps, so that events aren't represented by multiple alerts. Then analysts examine the individual alerts, looking for signs of suspicious activity and comparing the volume of similar events to a baseline for a particular system or user, assuming the analysts have been able to determine what those baselines should be. URLs may need to be investigated and attachments opened and scanned. Investigating a single alert may require 25 minutes or longer of a security analyst's time.

Small Banking Customer
DLP Alert Triage Problem

20 True Positives per Day	**15 mins** MTTR per Incident
130 (87%) False Positives per Day	**20 secs** MTTR per Incident

Too Long
MTTD

Total time

5.72 Hours/Day

2088 Hours/Year (24/7/365)

- Alert Fatigue contributing to staff turnover
- Written playbooks do not always match current practice
- Minimal documentation of investigations
- Siloed security products force costly human data fetching

This is detailed, repetitive work. It can be frustrating, too, since up to 95% of those closely examined alerts will turn out to be false positives or duplicate tickets. To find the few alerts that genuinely require action may take a SOC 7 to 10 hours or longer each week.

With data volumes rising dramatically and SOCs famously short-staffed, organizations need a better way of handling DLP alert triage to ensure they can protect their sensitive data.

The LogicHub SOAR+ Solution for DLP Alert Triage

The LogicHub SOAR+ security automation platform provides autonomous threat detection and response automation for SOC teams. By applying machine learning and advanced analytics on large data sets, LogicHub automates security analyst workflows and decisions, helping SOC teams save time, find critical threats, and eliminate false positives.

The LogicHub platform integrates with DLP systems and applies playbook rules to filter out benign alerts based on URL path, filename, user, and other attributes, dramatically reducing the total volume of alert data. From there, leveraging predefined thresholds and even tracking "normal" activity for each user over time, the platform can flag activity that appears genuinely suspicious. The platform can also automatically open cases for these incidents, feeding them automatically into a case management system, and sparing analysts the trouble of working in email and Excel. Next, analysts can investigate cases themselves.

Even here, the LogicHub platform can help with automation. For example, the platform can automatically send an email to the user or the user's manager, flagging the possible security violation and asking for confirmation that the activity is both benign and necessary for business.

Human Resources Customer DLP Alert Triage Problem

49
True Positives per Day

945 (95%)
False Positives per Day

Up to a Week
MTTD

Total time

16 Hours/Week

832 Hours/Year

- Batch processed once/week to save employee time
- Manual comparison of audit emails and spreadsheets
- No playbooks
- Minimal documentation of investigations

Benefits of the LogicHub SOAR+ DLP Alert Triage

The LogicHub platform delivers important benefits for SOCs performing DLP alert triage:

- Reduction of false positives, dramatically reducing SOC workload for DLP triage
- Acceleration of response to genuine incidents of potential data loss
- Faster processing of DLP cases, ensuring that legitimate communications can take place without delay
- Analysis that applies machine learning to automatically adjust to the evolving usage patterns of individual users and groups, so that anomalies can be promptly and accurately identified
- Support for reporting and security audits
- Improved overall security posture

The LogicHub solution for DLP Triage can be quickly deployed and tailored to a specific organization's DLP systems and security policies.

About LogicHub

LogicHub, the SOAR+ company, is the only security automation platform that delivers autonomous detection and response automation for security operations teams. By applying machine learning and analytics on large data sets, LogicHub automates security analyst workflows and decisions, helping teams save time, find critical threats, and eliminate false positives.

LogicHub SOAR+ DLP Alert Triage Solution

Small Banking Customer

MTTD = Processed as events happen

Total time

35 Mins/Day to review automated report

212 Hours/Year (24/7/365)

90% reduction with automation of DLP alert triage

1867 Hours saved/Year

- Greatly increased security posture
- Staff can focus on more important tasks
- No Alert Fatigue
- Playbooks are current and accurately followed
- Fully documented investigations of false and true positives

Human Resources Customer

MTTD = Processed as events happen

Reduced by up to **97%**

Total time

35 Mins/Day to review automated report

212 Hours/Year (24/7/365)

620 Hours saved/Year

- Immensely increased security posture
- Staff can focus on more important tasks
- Playbooks are current and accurately followed
- Fully documented investigations of false and true positives

LogicHub

a: 301 N Whisman Rd. Mountain View, CA 94043
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756