elastic

LOGGING FOR PUBLIC SECTOR:

5 ways to make the most of your mission-critical data

Many government agencies and educational institutions are focused on log management to ensure operational resilience, increase threat hunting capabilities, and comply with federal mandates, such as M-21-31 in the US. As you implement and refine your logging strategy, here are five ways to make sure you're using your data to move your mission forward.

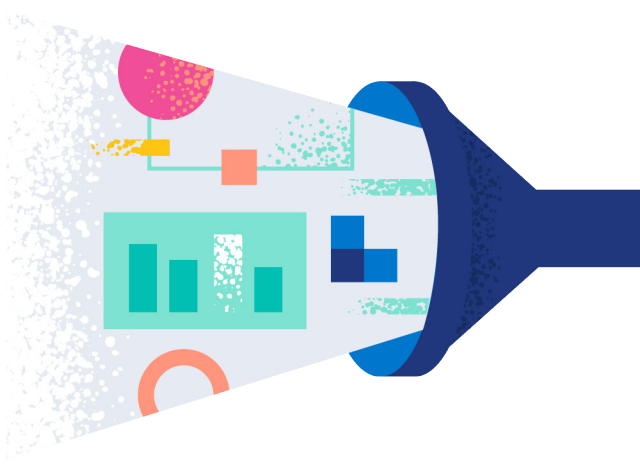
What's a log?

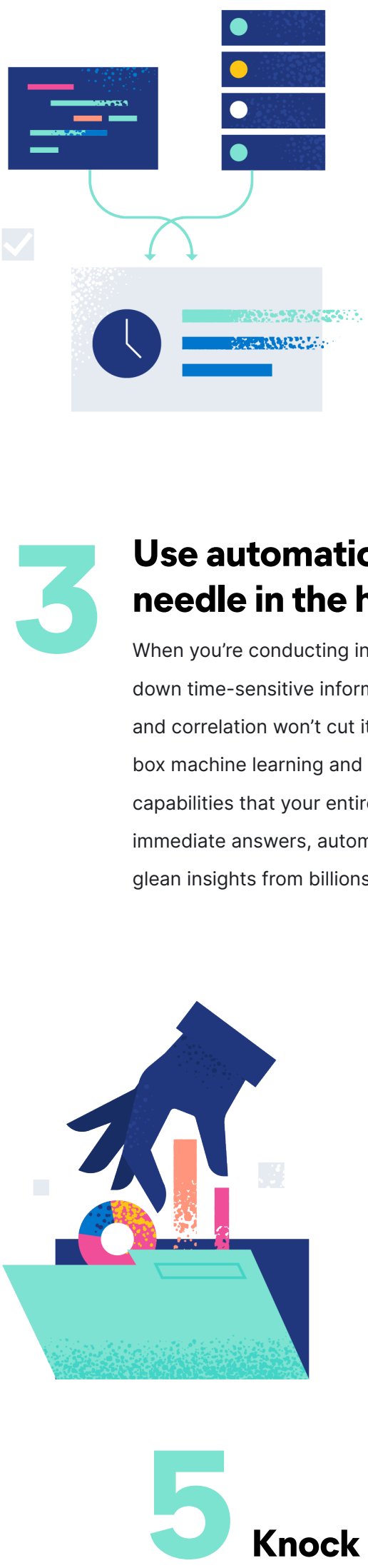
A log is a record of events generated by a wide range of systems and applications, typically containing details about when it happened, what was accessed, what or who originated it, plus any relevant metadata.

5 ways to maximize logging data for mission success

1 Streamline data onboarding

Pulling different types of data from different sources typically requires multiple tools and processes and can put unnecessary strain on your team.
Reduce time with a single agent that can ingest all your logs, metrics, and traces and eliminate dependency on external plugins and integrations that may require you to give up control of your sensitive data.





2 Integrate mission and logging data

Even organizations that have solid logging management capabilities may have separate data stores for mission data and logs. But when you can access and aggregate your logging and mission data in one place, you gain real-time situational awareness and the ability to quickly prioritize remediation.
For example, if you have five servers down, you can identify which ones directly affect your mission and start there.

3 Use automation to find the needle in the haystack

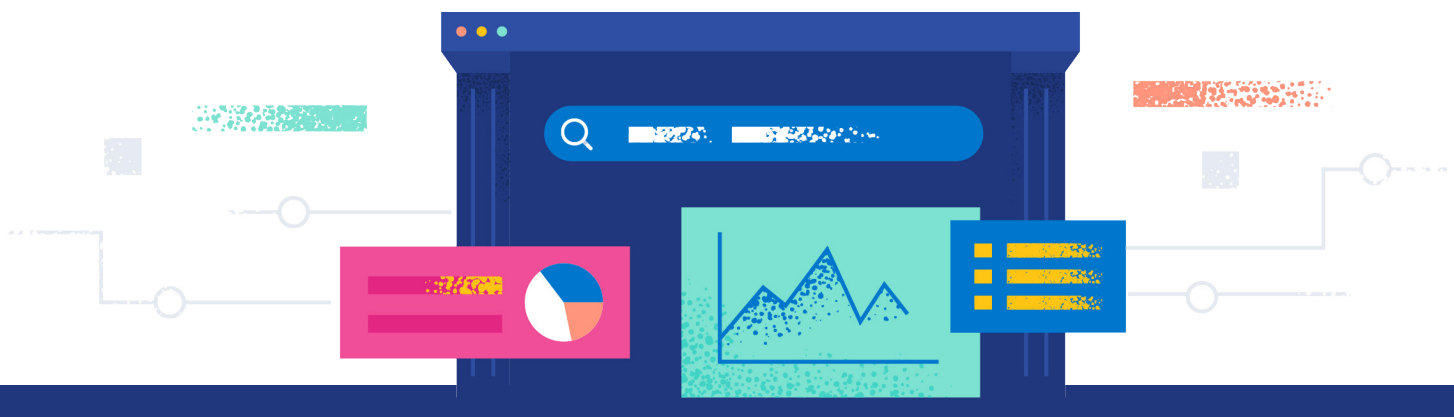
When you're conducting investigations or hunting down time-sensitive information, manual search and correlation won't cut it. Look for out-of-the box machine learning and artificial intelligence capabilities that your entire team can use to find immediate answers, automate alerts, and quickly glean insights from billions of logs.

4 Quickly access historical data when you need it

Does historical data need to be searchable, or can it be archived? Why not both? Make sure your older data meets log storage compliance requirements, but is also quickly accessible (without time-consuming manual data rehydration) if you need it.
You never know what information might suddenly need to be resurfaced in the event of an investigation or incident.

5 Knock down information silos

Many organizations keep their metrics, logs, and traces in separate systems – don't do that. Unify your data in a single observability solution that combines metrics, logs and traces (plus mission data, as mentioned above). But beyond that, the ability to find data via a single search query, across regions and cloud environments, without manual aggregation, will save your team countless hours and improve decision-making where every millisecond counts.



Logging is just the beginning

Start with logging – then when you're ready, use your logs as a launchpad into application performance monitoring (APM), automated analytics, and full-stack observability.
Learn more at www.elastic.co/observability,
or watch the "Logging for Public Sector" on-demand webinar.

elastic