Collect Everything: Host, Network & Cloud

ISSUE: SIEM correlation is often relational, and not maintained for all records. SIEM databases are also not immutable.

WHAT SHOULD YOUR RETENTION GOAL FOR COMPLIANCE?

<table>
<thead>
<tr>
<th>Compliance Standard</th>
<th>Retention Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>6 Years</td>
</tr>
<tr>
<td>HIPAA</td>
<td>6 Years</td>
</tr>
<tr>
<td>DFS</td>
<td>3 Years</td>
</tr>
<tr>
<td>FISMA</td>
<td>6 Years</td>
</tr>
<tr>
<td>SOX</td>
<td>Requirement is for Financial Data Retention.</td>
</tr>
<tr>
<td>GDPR</td>
<td>EU retention of EU subject data is generally 10 years, but varies widely.</td>
</tr>
</tbody>
</table>

Audit Fundamentals & Compliance Success

The 3 Needs of Audit Compliance

1. Search Cost & Days and Store a Minimum of One Year
2. To compensate for a slow database, SIEMs use fast and expensive drives. The cost of a SIEM to store data is very expensive. Fluency is the only service that by default stores for a year. It was written for AWS, and dynamically allocates resources. Its flow-oriented database does not require expensive disks to work.

3. Collect Everything: Host, Network & Cloud

ISSUE: Data is doubling every two years. SIEMs from five years ago can no longer handle all the data.

PCI
CAPACITY
1 Year
500,000 EPS.
The ability to capture everything.
FUSION
CORRELATES AND STORES RECORDS INTO A SINGLE IMMUTABLE DATABASE.
The ability to relate event, result, device, and user for a given time.

Audit Focus

WHAT SHOULD YOUR RETENTION GOAL FOR COMPLIANCE?

$1.29
$7,000
$0.78
$11,032
$1.33
$12,000

Fun Facts: Did you know...

FISMA requirements are based on NIST Special Publication 800-53 Series guidelines. But when it comes to how long its retained, it's the National Archives who's responsible. Security audit data mostly falls under 6 years according the General Record Schedule.

New York State Department of Financial Services (DFS) 23 NYCRR 500 is a cyber regulation addressing financial institutions doing business in New York. It requires three (3) years audit retention of security and system logs.

SIEM technology uses all-purpose databases. Fluency uses a flow-oriented immutable database which is a factor of 50 times faster than Elastic.

1. Cost to Store

<table>
<thead>
<tr>
<th>Cloud Service</th>
<th>90 Days Retention Cost per Gigabyte</th>
<th>100Gb per Day Monthly Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPLUNK</td>
<td>$1.29</td>
<td>$12,000</td>
</tr>
<tr>
<td>ELASTIC</td>
<td>$1.29</td>
<td>$11,032</td>
</tr>
<tr>
<td>FLUENCY</td>
<td>$0.78</td>
<td>$7,000</td>
</tr>
</tbody>
</table>

DON'T BE FOOLED.
BE FLUENT.

www.FluencySecurity.com

The Needs of Audit Compliance

Record Authentic and Remotely Authorize to ke Eure Events

Audit Fundamentals & Compliance Success

The 3 Needs of Audit Compliance

1. Search Cost & Days and Store a Minimum of One Year
2. To compensate for a slow database, SIEMs use fast and expensive drives. The cost of a SIEM to store data is very expensive. Fluency is the only service that by default stores for a year. It was written for AWS, and dynamically allocates resources. Its flow-oriented database does not require expensive disks to work.

3. Collect Everything: Host, Network & Cloud

ISSUE: Data is doubling every two years. SIEMs from five years ago can no longer handle all the data.

PCI
CAPACITY
1 Year
500,000 EPS.
The ability to capture everything.
FUSION
CORRELATES AND STORES RECORDS INTO A SINGLE IMMUTABLE DATABASE.
The ability to relate event, result, device, and user for a given time.

Audit Focus

WHAT SHOULD YOUR RETENTION GOAL FOR COMPLIANCE?

$1.29
$7,000
$0.78
$11,032
$1.33
$12,000

Fun Facts: Did you know...

FISMA requirements are based on NIST Special Publication 800-53 Series guidelines. But when it comes to how long its retained, it's the National Archives who's responsible. Security audit data mostly falls under 6 years according the General Record Schedule.

New York State Department of Financial Services (DFS) 23 NYCRR 500 is a cyber regulation addressing financial institutions doing business in New York. It requires three (3) years audit retention of security and system logs.

SIEM technology uses all-purpose databases. Fluency uses a flow-oriented immutable database which is a factor of 50 times faster than Elastic.

1. Cost to Store

<table>
<thead>
<tr>
<th>Cloud Service</th>
<th>90 Days Retention Cost per Gigabyte</th>
<th>100Gb per Day Monthly Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPLUNK</td>
<td>$1.29</td>
<td>$12,000</td>
</tr>
<tr>
<td>ELASTIC</td>
<td>$1.29</td>
<td>$11,032</td>
</tr>
<tr>
<td>FLUENCY</td>
<td>$0.78</td>
<td>$7,000</td>
</tr>
</tbody>
</table>