**Securing your IT infrastructure with SOC/NOC collaboration**

Universal log management for IT operations

<table>
<thead>
<tr>
<th>Table of contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>2</td>
</tr>
<tr>
<td><strong>IT operations: Handle IT incidents and performance issues</strong></td>
<td>2</td>
</tr>
<tr>
<td>Problems that arise when IT operations need to scale</td>
<td>3</td>
</tr>
<tr>
<td><strong>Log management: Universal log data collection, aggregation, analysis, and retention</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Better together: Log management and IT operations</strong></td>
<td>4</td>
</tr>
<tr>
<td>Why integrate log management with IT operations?</td>
<td>5</td>
</tr>
<tr>
<td>Why integrate IT operations tool with log management?</td>
<td>5</td>
</tr>
<tr>
<td><strong>Customer use case</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>7</td>
</tr>
<tr>
<td><strong>For more information</strong></td>
<td>7</td>
</tr>
</tbody>
</table>
Executive summary

The emergence of Enterprise 2.0 with social, mobile, local, and cloud applications within the enterprise has increased IT operational challenges. Other trends, such as bring your own device (BYOD), coupled with multiple operating systems, vendors, etc. are adding to the complexity in IT operations. Your customers and employees are demanding an open platform that can facilitate better collaboration. However, your IT operations may not be in a position to support Enterprise 2.0 or BYOD due to security issues or resource constraints. So, how do you align your business requirements and IT resources in a safe and secure manner?

Figure 1. Secure Enterprise 2.0, social, mobile, and cloud data

The convergence of IT and security operations has been an ongoing effort in most enterprises. The benefits of this convergence are clear to many organizations that need to optimize resources, lower cost, increase efficiency in both groups, and deliver an open and secure platform for communication and collaboration.

This white paper explains how you can seamlessly integrate log management into IT operations as a starting point of a security operation center (SOC)/network operation center (NOC). The SOC/NOC integration empowers your organization to effectively manage your IT infrastructure, while keeping it safe.

Let us understand the type of data that these two groups collect and analyze, and how it can be used in context. The actionable knowledge from this data is derived from the security and operations context.

“The SOC/NOC integration empowers your organization to effectively manage your IT infrastructure, while keeping it safe.”

IT operations: Handle IT incidents and performance issues

IT operations monitor, consolidate, and correlate performance events of the IT infrastructure through a single pane of glass (unified console). This helps identify the root cause, conduct impact analysis, isolate IT issues, and effectively correct incidents all through a single interface.

IT operations typically have predefined policies to capture exceptions, performance issues, or IT incidents across applications and network devices. These incidents are correlated and rolled up to business service views to facilitate prioritization based on impact of the event.

The integration of IT operations with other tools such as a centralized Configuration Management Database (CMDB) provides the service context to node topology. By seamlessly connecting with the service management tools, an IT operations group can create service tickets to correct the IT incident, therefore helping IT operations align with the IT Infrastructure Library (ITIL) process and deliver best practices.
Problems that arise when IT operations need to scale

As the size of the managed environment grows, the monitoring of events from the infrastructure elements becomes harder. IT operators rely on event reduction techniques such as correlation engines, or limit either the breadth or depth of data collection to only machine data from business-critical applications. The machine data collected is typically not categorized or normalized, and there are no tools to search events or logs. The data is also retained for the short term and may not fulfill the need to keep services up and running at all times. This short-term retention of data limits the intelligence in the system as events fixed and annotated a few months ago may not be stored to retrieve. The alternate option is to invest in expensive databases and resources to manage the data.

In many organizations, security operations work in silos. As a result, security vulnerabilities have to be handled twice: once by the SOC groups or security teams; and then again by the IT operations team that could not initially identify the issue. Consequently, you cannot establish any automation for information sharing or event correlation between security vulnerabilities and performance issues. Let us see how some of these automation challenges can be addressed between security and IT operations. A good starting point is to understand the tools available to manage the data comprehensively from a security, risk, compliance, and operations standpoint, while being able to integrate them with existing IT operations.

Log management: Universal log data collection, aggregation, analysis, and retention

Log management is a process of collection of logs from any device, aggregation of logs into a single searchable format, analysis of logs through data enrichment, and long-term retention of log data. Log management is primarily driven by security and IT GRC (governance, risk, and compliance) requirements, while adding a security context to all the log data.

Effective log management helps in quick resolution of fault, configuration, accounting, performance, and security (FCAPS) issues. It is estimated that only a small percentage of mission-critical application downtime is caused by technology/environmental failure or a natural disaster, whereas a majority is caused by people or process failures. Part of this majority of downtime is caused by cyber security issues, and the larger part is correlated to poor change and application management. Since log management maintains an audit trail of comprehensive machine data for a long time, forensic analysis and faster resolution of IT incidents is made simpler.

Figure 2. Log management solution for IT security, IT operations, and IT GRC

Log management solutions collect both structured and unstructured raw data from any log-generating source. All types of machine data from any source in various formats is collected and aggregated. Logs from “in-house” applications, custom, or new applications can also be extracted easily. The log management is both broad and deep in data collection.

The logs collected in various formats are then consolidated through a process of aggregation, where it is typically converted into a single format. This common event format helps logs to categorize data into logical groups such as firewall or router data, irrespective of vendor-specific details. The log data is enriched with metadata so that domain experts don’t need to search or interpret logs. For instance, the log data coming in from all firewall devices goes through the normalization and categorization process. Hence, irrespective of whether Cisco calls it “Deny” or Check Point calls it “Drop,” the metadata always puts it in the “/Failure” category, and identifies it automatically as firewall devices.
Table 1. Unified data from various log formats with enriched metadata

<table>
<thead>
<tr>
<th>Time (Event time)</th>
<th>Name</th>
<th>Device vendor</th>
<th>Device product</th>
<th>Category behavior</th>
<th>Category group</th>
<th>Category outcome</th>
<th>Category significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/17/2009 12:16:03</td>
<td>Deny</td>
<td>Cisco</td>
<td>PIX</td>
<td>/Access</td>
<td>/Firewall</td>
<td>/Failure</td>
<td>/Informational/warning</td>
</tr>
</tbody>
</table>

The logs in common event format are indexed for simple and ultra-fast searching at over million events per second through a simple user interface. A keyword search such as “Firewall AND Failure” searches for the failed login attempts on all firewall devices across the network in seconds. Without normalization, the same report would have taken several hours worth of research and collaboration between various domain experts.

This log data, both raw and in common format, is archived using high compression rates, and can be retained for a number of years in flat file format reducing the cost and complexity of log data management. This unified data can be used for searching, indexing, archiving, analysis, reporting, and IT audit. The data sent to a correlation engine for instance can identify patterns and security vulnerabilities based on the built-in security and compliance rules. Once these threats are identified, the integration with other tools, such as service management tools can use the same unified data to prevent and correct threats and IT incidents. Let us see how this unified data is beneficial to IT operations tools and provides security context to operations data.

Better together: Log management and IT operations

Integrating log management solution and IT operations is mutually beneficial to both organizations. With the increasing number of cyber attacks, it is critical to share the tools and knowledge between security and IT operations as many organizations cannot detect breach until it is too late.

The Data Breach Investigations Report (DBIR) of 2012 conducted by Verizon, states that 98 percent of the data breaches come from external agents. 97 percent of those breaches could have been avoided by implementing simple controls like a log management solution.

Of all the breaches that were studied, 92 percent were reported by third parties. It is an embarrassment to organizations if they do not detect a breach in their internal system. Log management plays a critical role within the organization to detect and share knowledge about security threats that can be prevented through IT operations.

Figure 3. See, understand, and act for better SOC/NOC collaboration

“92 percent of the data breaches were detected by third parties.”

Data Breach Investigations Report (DBIR) of 2012 conducted by Verizon
Why integrate log management with IT operations?

We have seen that a comprehensive log management approach to understanding machine data from a security, risk, compliance, and operations viewpoint helps the organizations manage their IT better. Let us see the advantages of comprehensive log management:

- Collection of logs from any log-generating source, in any format, using agent or agentless collection
- Categorization and normalization of the log data to filter, parse, and enrich the events
- Aggregation of logs into an indexed, common event format for search capabilities
- Bing/Google™ like search capability for the IT operations team to search past events without vendor-specific keywords
- Long retention of events, and easy access of those events for audit purposes
- Forensic investigation of incidents
- Seamless integration into security correlation engine to take events from IT operations and check for false positives
- Configure security metrics onto the IT operations console
- Addition of security threat and vulnerability use cases for IT operations
- Automated compliance reporting

Why integrate IT operations tool with log management?

Now that we’ve seen that comprehensive log management helps IT operations add security and risk context to machine data, let us see the advantages of adding IT operation tools to the SOC.

- Provide business context for security incidents for event prioritization
- Automate the prevention and correction of security incidents
- Visualize impact of security incidents on business services
- Visualize root cause and isolate network devices affected by service incidents
- Create service tickets for security incidents
- Add security metrics to the high-level IT operations dashboard

The convergence of data helps IT operations to get the security context on the IT incidents along with a broader and deeper monitoring of IT infrastructure through comprehensive log management. The convergence ultimately helps you answer the questions such as, “Who caused the performance degradation of IT operations and why?” and “Was the performance degradation caused by user load or by a cyber attack?”

Gartner report on log management for IT Operations (July 2011)¹ suggests that shared infrastructure saves a significant amount of money and adds access to a broader set of log data sources. The report also suggested that IT operations should have access to log management infrastructure for search and analytics.

Both security and IT operations need to collect, store, and analyze events logged by a common set of critical event data sources. Although the interpretation of these events is different, the actionable response to these events needs to be unified. A patch solution or point solutions may not be comprehensive. However, choosing a single vendor that exhibits seamless integration makes your IT align with business and keep it secure.

Customer use case

HP-IT is an internal organization of Hewlett-Packard that runs the HP IT operations for 350,000 employees worldwide. HP, being a Fortune 10 company, runs some of the best Enterprise 2.0 applications to enable its employees to collaborate with customers and partners. With remote working and BYOD/mobility requirements from employees, HP-IT is one of the largest and complex IT organizations.

HP-IT has integrated the log management tools with IT operations to manage one of the most complex IT organizations in the world, and to deliver the demanding SLAs from both internal and external customers.

The convergence of data helps you answer who caused the performance degradation of IT? Load or cyber attack?

Figure 4. Enhanced triage by using Logger as a single repository of IT events, logs, and security events

HP-IT has deployed HP ArcSight Logger (Logger) for universal log management solution and HP Operations Manager i (OMi) for managing the IT Operation Center. The predefined connector for OMi provides seamless integration between log management solution and the IT operations solution. The IT incidents from business-critical applications are monitored by OMi and are pulled into Logger. All these events are converted into an industry-standard common event format (CEF) by Logger.

These events then go through parsing and filtering through normalization and categorization, which are then fed to the security event correlation engine (HP ArcSight ESM) for real-time, cross-device, correlation of security events across the organization. This security information and event management (SIEM) correlation solution helps HP-IT to manage, prioritize, and isolate the security incidents, while reducing the false positives in IT operations.

As the integration is bi-directional, the security incidents detected by Logger are fed into HP OMi. These security events that were undetected by IT Operations tools are then correlated to check for exceptions and are prioritized based on the policy information on OMi. The security incidents, triggered by Logger and prioritized by OMi, go through the service management tool to be corrected.

Figure 5. Events detected by Logger in IT operations tool

The integration enables security events to participate in advanced cross-domain event correlation in HP OMi such as identifying the business and service impact of a security event across the organization. This reduces the number of events created by various network services impacted by one event allowing HP-IT operations teams to discern between symptom events and causal events, and focus on the root cause.

All the events are rolled up to the high-level IT operations console for business service views that provide measurable security metrics to HP executives and the HP-IT operations team. This helps spread the cost of IT operations with the security operations helping in faster realization of IT investment. The data convergence helps HP-IT to foster employee and customer collaboration.
Conclusion

Relying heavily on event reduction techniques or limiting the breadth and depth of machine data collection to business-critical applications may not be the solution for IT incident management challenges. Comprehensive log management and a strong security event correlation engine can help your IT organization to scale incident management and simplify it.

Convergence of data between IT operations and log management facilitates a deeper understanding of roles, risks, threats, and security vulnerabilities enabling faster time to resolution through clear communications and a comprehensive view of security health. This collaboration is effective when implemented through industry-leading enterprise tools that integrate and automate key IT operations and security operations functions.

For more information

Go to hpenterprisesecurity.com/logger for more information, and download a free trial copy of the log management solution to integrate it with your IT operations tool (hp.com/go/logger).

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts delivered directly to your desktop