ScienceLogic Forum Release

Automated workflows accelerate your digital transformation journey. ScienceLogic helps you transform your IT environment with a modern automation framework that leverages data and context from legacy and modern tools to make IT work flow—faster and easier. With the Forum release, ScienceLogic expands your ability to see, contextualize, and act to accelerate your journey to AIOps.

Forum Release Summary: What's New

With ScienceLogic SL1, you can see everything across multi-cloud and distributed architectures, contextualize data through relationship mapping, and act on this insight through integration and automation. With this approach, you set the foundation for AIOps by assimilating and normalizing varied sets of data from across your ecosystem to gain insightful context and put those insights in action with IT workflow automations.

With our Forum release, we introduce the following capabilities to accelerate and secure your AIOps journey:

See

- **Expanded cloud monitoring** for 90+ additional AWS and Azure services
- **Simplified, self-service onboarding** of customers and new technologies so you can quickly fill monitoring visibility gaps

Contextualize

- **New event insights** reveal the impact of SL1's noise reduction capabilities, enabling you to measure SL1's impact on accelerating root cause analysis and driving operational efficiencies

Act

- **New pre-built automated workflows** for SecOps, Incident Management, DevOps, and Orchestration tools

We continue to prioritize the security of the SL1 platform. We recently introduced the ability to **run Crowdstrike agents** on your on-premises SL1 appliances and Restorepoint agents to help protect your data at the edge. We also continue our focus on securing the SL1 platform in Forum by:

- Offering **automated workflows based on Crowdstrike security event notifications**
- Adding the ability for Restorepoint to **request credentials from CyberArk** as and when needed. This allows for central credential management, control, and audit of credential-related activity
- **Certifying SL1 Distributed MUD version in AWS GovCloud**, helping to accelerate the move to cloud for federal and other organizations with strict certification requirements

Forum is planned for external release in December 2022.

Read on for more details on this new release.

© 2023 ScienceLogic

Forum Release Reinforces the AIOps Framework

In each new SL1 release, we deliver new capabilities aligned to the key tenets of AIOps:

1. **See**: Data is the foundation that helps you see what you have in your IT environment.
2. **Contextualize**: Analytics help you derive insights from service context and machine learning.
3. **Act:** Intelligent automation helps you increase productivity, solve problems faster, and drive business agility.

Let's take a deeper look at the Forum release capabilities across these pillars:

See: Simplify and speed a more complete view of your entire IT estate

SL1 continually monitors your environment so you can see what you have, know what's working and what's not, and take corrective actions immediately. With Forum, you can monitor more cloud services and start monitoring faster.

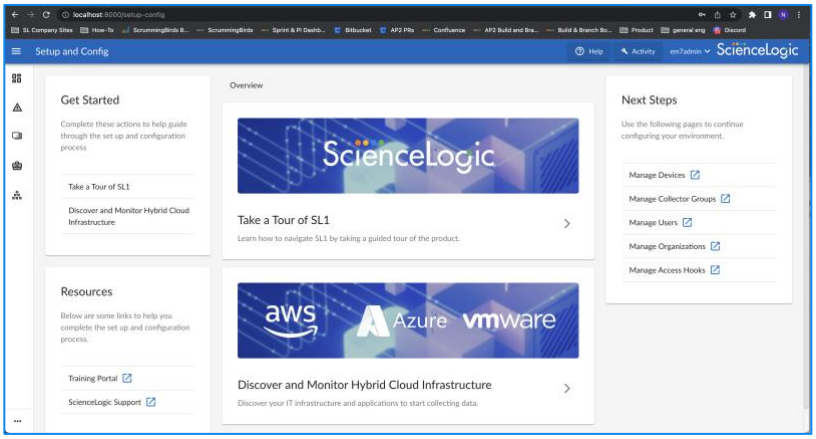
Expanded cloud monitoring capabilities for 90+ newly supported AWS and Azure services

SL1 supports more than 90 new AWS and Azure services so you can discover, map, and monitor their health and relationships. As you achieve complete IT estate visibility, you improve your ability to reduce event noise, expedite troubleshooting and remediation, and better yet, avoid outages altogether.

Quicker onboarding of new technologies and customers for faster monitoring

The sooner you start monitoring, the sooner you have the insights you need to optimize your IT estate and fuel time-saving automations. With Forum, you can start monitoring faster with:

1) **New guided set-up and configuration administrator workflows**. Streamline onboarding of new technology and customers with guided workflows that include activities, knowledge, external links, and tasks associated with discovering, mapping, and monitoring AWS, Azure, and VMWare devices and services.



You'll also get guidance on "What's next" where you can get information on SL1-specific administrator functions, such as managing users, managing organizations, and collector groups.

2) **Direct download of SL1 Data Collector and Message Collector images from Microsoft Azure Marketplace.** We've streamlined the process for deploying SL1 Collectors through direct download access and self-service actions.

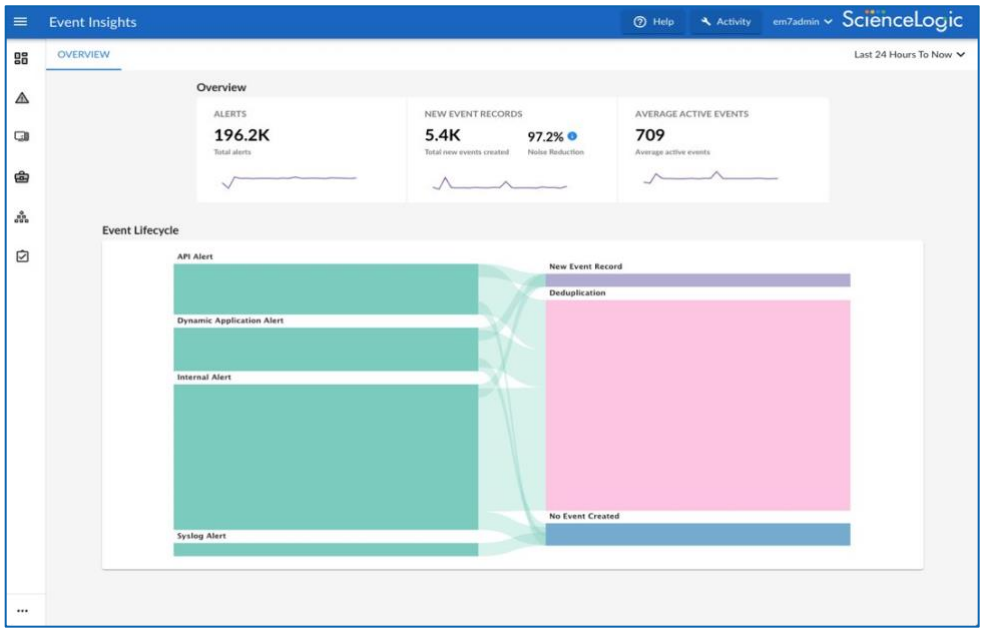
© 2023 ScienceLogic

The SL1 Collector onboarding process is now 2 steps: 1) Go to Azure Marketplace, and 2) download your SL1 Collector images and install them directly into your Azure account. Done! Similar support for other cloud service providers is coming soon. You can also register and connect your SL1 Collectors to an SL1 Database as a self-service function (introduced in the 2022 Eiffel release).

Contextualize: Measure the Value of SL1 Event Correlation

Part of the power of SL1's machine learning-driven behavioral correlation is its ability to correlate events within a service context to reduce event noise and help you zero-in on the root cause of service-impacting incidents. However, measuring the impact of correlation hasn't been obvious.

With the Forum release, ScienceLogic introduces Event Insights to help you visualize SL1's alert and event filtering, deduplication, suppression, and correlation abilities—allowing you to measure how much work SL1 is doing behind the scenes. This can help you demonstrate the value of SL1 to key stakeholders or provide you with feedback as you tune SL1's event policies over time.



In the Event Insights image above, you can see the volume of alerts SL1 is processing along with the resulting events, showing a 97.2% noise reduction rate. You also see a graphical depiction of the substantial number of alerts that have been deduped, correlated, and filtered out, resulting in fewer high-value or actionable events.

Act: Move faster with automated workflows

Automated workflows are the fastest way to increase your productivity and accelerate your journey to automated operations or AIOps. Integration with the tools you commonly use and have already invested in can amplify the value you gain from those tools and from SL1. With Forum, you can tap into new pre-built closed-loop workflow automation solutions that connect your IT ecosystem tools and promote collaboration between your ITOps, DevOps, SecOps, and ITSM teams.

© 2023 ScienceLogic

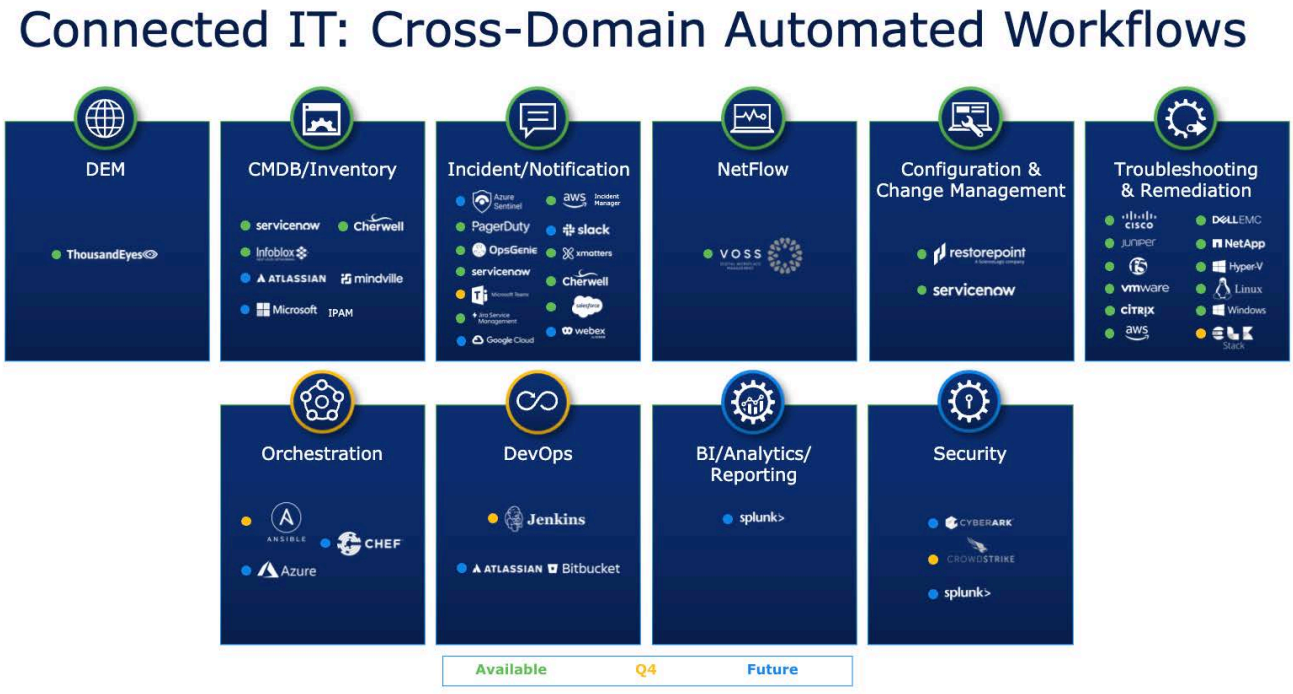
Connected IT ecosystem tool support

New IT ecosystem tool support in the Forum release includes:

- **CMDB/Inventory:** Infoblox
- **Incident/Notification:** Jira Service Management, Salesforce, MSFT Teams
- **Troubleshooting and Remediation:** AWS, ELK Stack
- **Orchestration:** Ansible
- **DevOps:** Jenkins
- **Security:** CrowdStrike

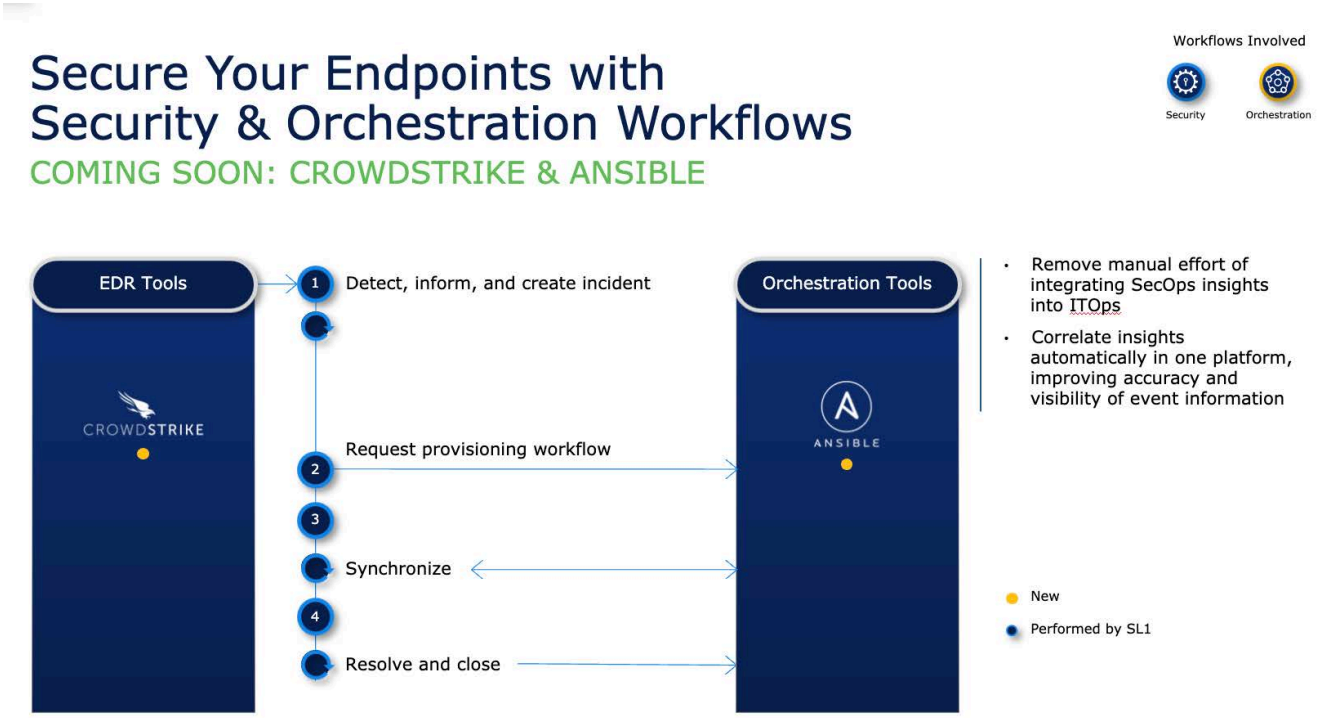
Legend: **Green –** available; orange – coming soon

The image below illustrates **all** supported workflows for SL1, allowing wide flexibility to automate cross-domain workflows leveraging your existing IT ecosystem tools.



© 2023 ScienceLogic

Let's look at a few examples of how you can drive operational efficiency in your environment.

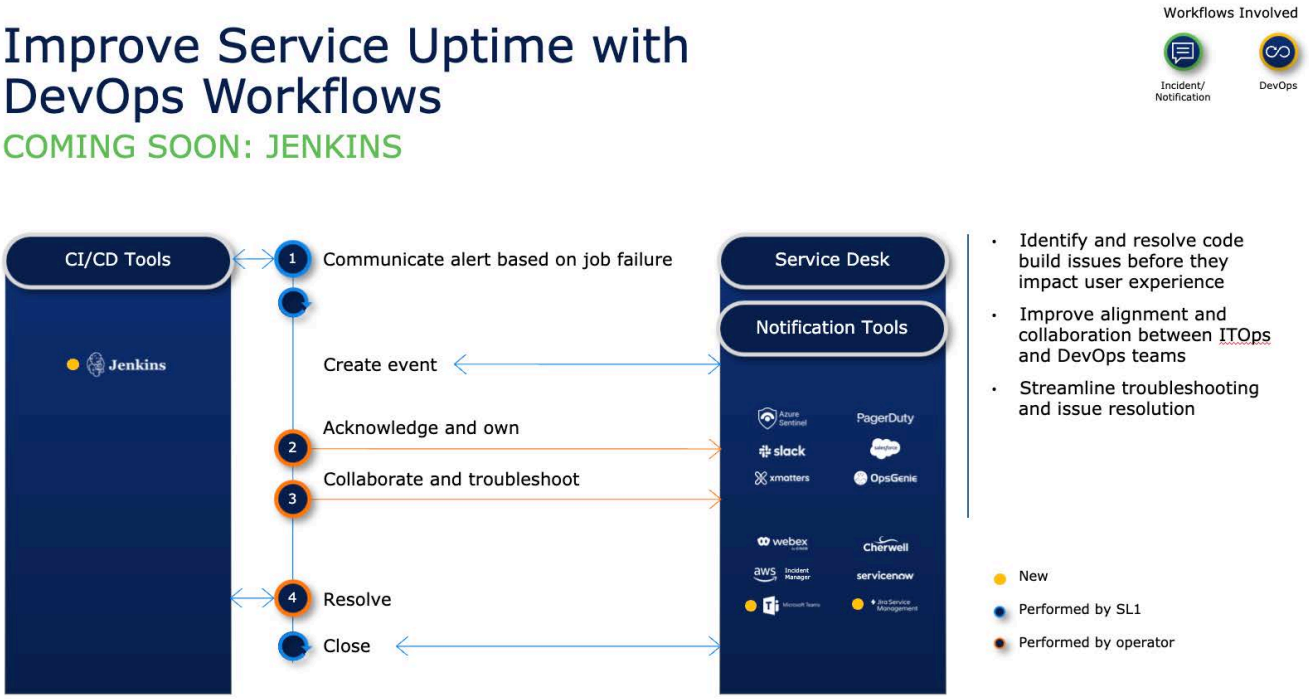


Use case 1: Secure your endpoints with security and orchestration workflows - CrowdStrike and Ansible

Summary of use case: With cybersecurity threats constantly evolving, tools like CrowdStrike are critical to stop breaches, ransomware, and cyber-attacks. In this use case, CrowdStrike detects potential malware on a device and sends that information to SL1 as an event. Based on pre-defined rules, SL1 automatically requests a workflow through Ansible, for instance to quarantine the device in question. SL1 can then simultaneously create an incident to document the issue.

SL1 automatically synchronizes the updates made by Ansible and the operator actions taken on the event within SL1 or the incident in your ticketing system with both CrowdStrike and Ansible, so no matter which tool you log into, you see up-to-date and consistent information across your SL1, CrowdStrike, Ansible, and ITSM systems. By removing the need for human intervention, you mitigate your security risk faster, resolve security incidents faster, minimize any risk of human error, and free your staff to focus on business priorities.

© 2023 ScienceLogic



Use case 2: Improve service uptime with DevOps workflows – Jenkins

Summary of use case: As your application developers and DevOps teams continue to roll out new and updated applications, it becomes more important than ever to ensure that any issues based on those changes are managed and mitigated quickly. By leveraging SL1 DevOps workflow automation solutions, organizations that use CI/CD tools like Jenkins to automate their software deployment lifecycle can quickly detect and resolve application code issues before they impact end users and/or critical business services. When combined with SL1 Incident/Notification workflows, you can also avoid the extra effort required to integrate your CI/CD tools with your Service Desk, Notification, and Collaboration tools. With this automated workflow:

1. Jenkins detects a job failure and communicates an alert to SL1.
2. Based on pre-defined policies, SL1 creates an event and initiates a communication to the responsible team, who takes ownership for the event/incident investigation.
3. The team responsible collaborates and troubleshoots to clear the issue. This may include additional automated workflows with your Service Desk, Notification, and Collaboration tools.
4. Once the root cause is confirmed, the operator can re-run the appropriate Jenkins job to resolve the issue.
5. Once the issue is resolved, and the Jenkins job is re-run successfully, SL1 automatically resolves and clears the event and updates the associated incident in the relevant Service Desk, Notification, Collaboration tools to reflect the latest status.

By automating workflows between SL1 and your DevOps, ITSM, and Notification/Collaboration systems, you can proactively detect and quickly resolve application issues caused by changes; thereby avoiding critical application/service outages and ensuring optimal user experiences.

© 2023 ScienceLogic

Take the next step in your AIOps journey today.

For more information on these latest updates, contact us. If you are exploring your next steps on your AIOps journey, check out our Getting Started page and obtain expert insights by attending a webinar.

Existing customers can contact your customer success manager and learn more about "What's New" on the ScienceLogic Support Portal.

About ScienceLogic

ScienceLogic empowers intelligent automated IT operations freeing up IT talent, accelerating innovation and transformation, and driving business outcomes. ScienceLogic's AIOps and Observability platform monitors customer data across clouds and on-premises, enabling actionable insights to predict and resolve service impacting problems faster through machine-driven analytics and automation.

SL1 removes the difficulty of managing complex, distributed IT services today and provides the flexibility to face the needs of tomorrow. Trusted by thousands of organizations, ScienceLogic's technology meets the rigorous security requirements of U.S. Department of Defense, has been proven for scale by the world's largest service providers, and is optimized to meet the needs of large enterprises and government agencies.

© 2023 ScienceLogic