Restore IT Services NOW

How Moogsoft Optimizes Your ServiceNow ITSM Deployment with Situational Awareness

For information about Moogsoft and servicenow, visit www.moogsoft.com.

1.0 Executive Summary

When IT service incidents occur, your IT reputation is immediately on the "desk" – the ITSM Service Desk.

You have modernized your service management processes with ServiceNow ITSM Service Desk, streamlining the front-end process of reporting, escalating and updating incidents to improve your customers' experience.

But the biggest bottleneck next to tackle is in backend operations. If removed, it will cut a big chunk of your Mean Time to Detect (MTTD) and Mean Time to Restore (MTTR), improving your customers' experience much further.

This operational bottleneck spans across three vectors: (1) inability to detect warnings as incident storms are still forming, (2) lack of situational awareness to identify causes and impacted services, and (3) inefficiency of the right domain experts to engage and remediate.

Forrester Research: "74% of end user problems are not detected by IT."

Gartner: "80% of the mean time to resolve is wasted on trying to locate the issue."

By modernizing your event and alert management, you can effectively unclog these lengthening processes. The results are dramatic:

- Detect real incident-triggering alarms up to 24 hours earlier than traditional event management systems;
- Reduce spam events, alert storms, and false incidents by up to 99%;
- Restore degraded service hours or days before incidents cascade and turn into severity 1s.

This white paper describes how Incident.MOOG, a ServiceNow certified, modern event management backend,

Metrics Over a 30-Day Period	Before	After	% of Improvement
Number of raw events	~9,728,896	~34,228	99.6%
Number of real "Situations", i.e. Cleaned, Clustered and Contextualized "Alerts"	0 (almost)	~1,939	99.98%
Average time taken to create corresponding ServiceNow incidents	>=24 hours	1-2 hours	95.8%

integrates with ServiceNow IT Service Management and IT Operational Management products. Incident.MOOG's unique real-time machine learning and modern social collaboration technologies provide IT Operations teams with situational awareness, so incidents can be detected earlier, automatically, and ultimately resolved faster, before the customer has to call to complain. This paper will also explain how you can:

- Optimize your ServiceNow incident, change and problem management by adopting change-tolerant, situation-aware event management
- Reduce incident volume and restore services faster for ServiceNow ITSM

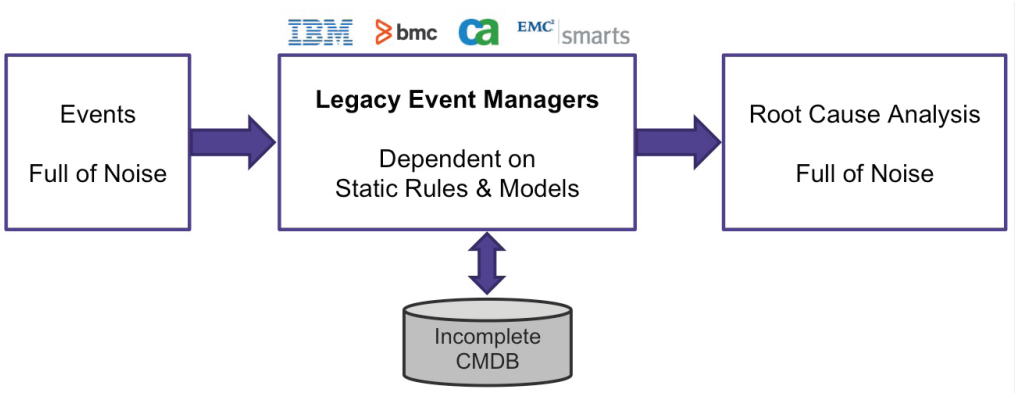
As one large enterprise customer of Incident.MOOG sums it up: "ServiceNow is our single system of record. But Incident.MOOG is our single point of engagement for problem solving."

2.0 Legacy Event Management Can No Longer Keep Up: It's Holding You Back

ServiceNow ITSM has streamlined the customer-facing Service Desk. However, the operational side behind ITSM hasn't changed much over the years, despite the fact that your IT environment has dramatically changed. Legacy event management and alert prioritization are not change, error or scale tolerant, given their architectures and code are 10-20 years old. As a result, incident management and Root Cause Analysis (RCA) have become more reactive, more lengthy and less inaccurate.

The reason for this can be simply explained: the noise in, noise out event management approach, see Figure 1.

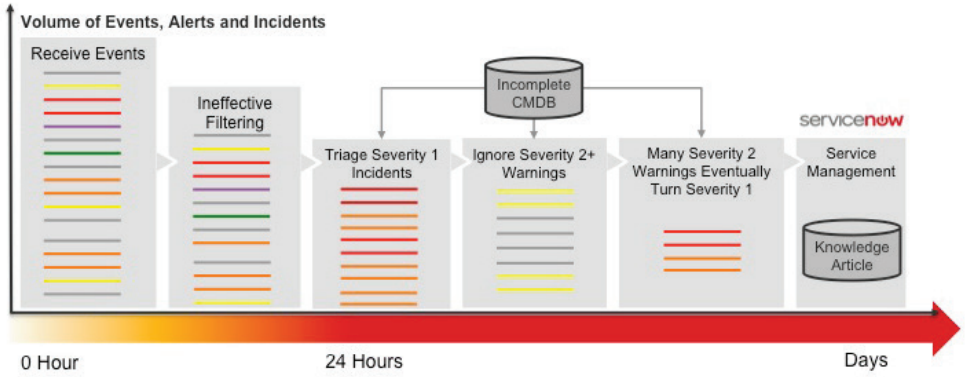
FIGURE 1: Legacy Event Management Paradigm: Noise In, Noise Out



In large enterprise IT environments, outages are more often the result of simultaneous, cascading, and transient events and faults across multiple technology domains – exasperated by virtualization, mobility and cloud. True culprits of outages are often buried deep among millions of events and thousands of alarms – generated daily and without context. Yet, the increasing pace of IT complexity and change instantly leaves any infrastructure to services mapping inaccurate, most notably the Configuration Management Database (CMDB). This renders ineffective an event management system that depends on static rules based off a 100% accurate topology model.

When relying on these outdated models and rules to triangulate outages that are full of noise, you get noise in, noise out. Figure 2 depicts this workflow, spanning from event collection and processing, to incident management and problem remediation, to ultimately service restoral and RCA - all while the Service Desk team (and customers) wait.

FIGURE 2: Legacy Event Management Workflow Slows Down ServiceNow ITSM



There are far too many manual and redundant workflows with this legacy model:

- Events are sourced one by one from individual technology silos – e.g. app, database, compute, storage, and network – then are presented without context to experts operating in different silos. Multiple teams are often troubleshooting separately, but not collaborating to solve the same problem.
- The sheer volume of events often obscures the problem source. Therefore, IT ops and legacy event management systems process only priority 1 alerts based on SLAs. Or they use aggressive filtering to make event volume manageable. But this often hides important events including severity 2+ that contain early warnings.
- There is no way of seeing how alerts are related (other than tribal knowledge, or a lengthy manual triage process). This leads to multiple tickets raised off multiple critical alerts – all pointing to the same problem.
- After an outage has occurred, tickets are often merged into a master ticket, a manual time-consuming process, and a poor use of any domain expert's time.
- Once an incident is being worked on by operations and domain experts are called in, the Service Desk lacks visibility into what's going on.
- Finally, after an incident has been resolved, there is no easy and automatic way to update a knowledge article. Even if there is, correlating past articles to future incidents is often a slow, manual process.

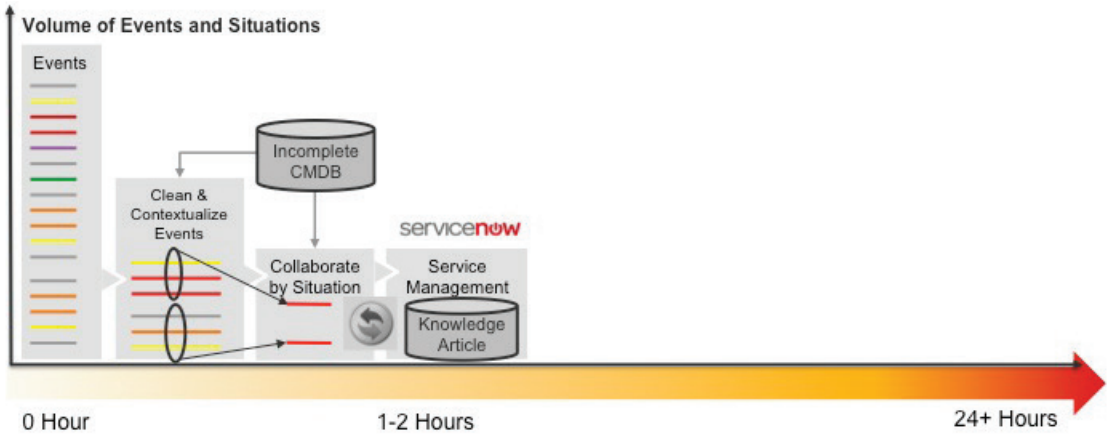
To transform workflow for dramatically higher efficiency, service quality, and customer experience, IT Ops needs to solve this problem from a very different perspective.

3.0 Add Situational Awareness to Event Management: Restore Services NOW for ServiceNow ITSM

Instead of assuming that configuration is fully known at any moment in time and that incidents all have singular root cause, Incident.MOOG relaxes the rigid constraints around event-based anomaly detection – casting a wider net by ingesting larger a broader set of unstructured event data and tolerating inconsistencies and incompleteness. By doing so, it finds what other systems can't, along with full context across the incident narrative. The result is much faster detection of multiple cascading issues. Legacy tools assuming fully accurate configuration data and single root cause simply can't do this.

Incident.MOOG is also able to detect abnormalities that haven't occurred nor been seen before. Using a three step process, Incident.MOOG accomplishes this all much faster than your legacy approach, as depicted in Figure 3:

FIGURE 3: Situational Awareness Added to Event Management Accelerates Workflow



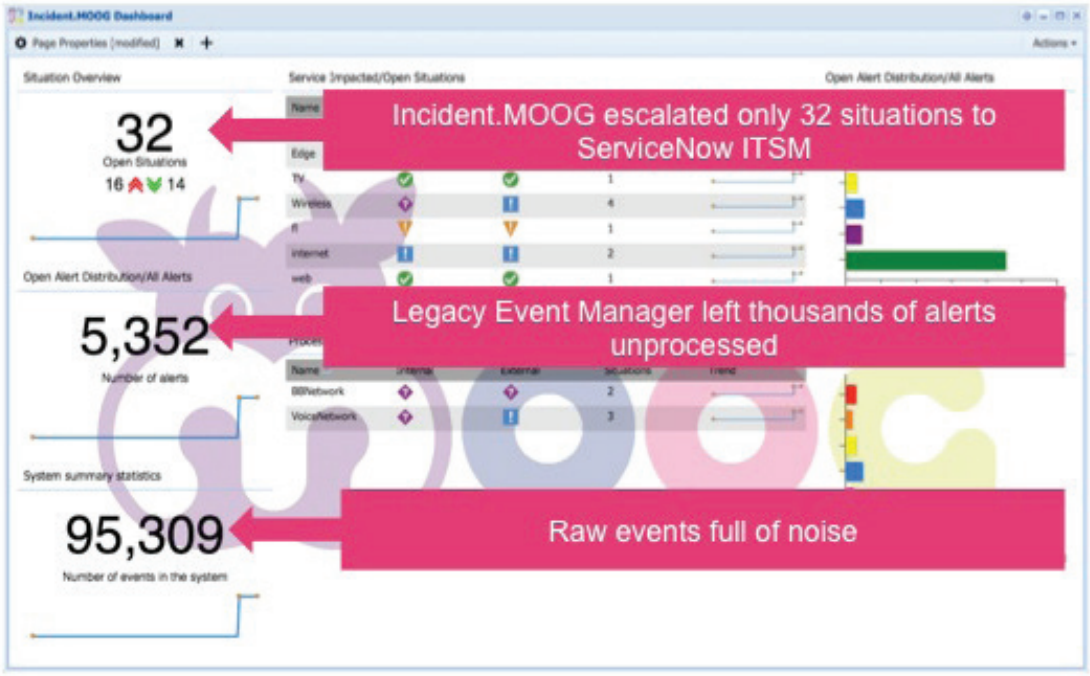
A - Clean: Solve the data overload problem by cleaning in real-time the voluminous event stream that's full of noise and partial warnings, despite a partial and inaccurate CMDB underneath. Automated machine learning and natural language processing algorithms replace hard-coded rule and models to ingest loosely defined, text rich events across domain silos in the IP stack, from application to infrastructure. This approach is particularly well suited in dynamic IT environments using software infrastructures, virtualization and cloud and a migration toward continuous application delivery (i.e. DevOps).

B - Contextualize: Virtually eliminate troubleshooting triage by showing the resulting alerts in context, specifically, clustering related alerts into situations, which are then decorated with service-specific details. Moogsoft uses a data driven approach, change- and error-tolerant algorithms that automatically identify clusters of related alerts (rather than always assuming singular root cause). This approach captures the entire narrative of an incident and presents it situationally. Because this data-driven approach can analyze a situation from multiple angles, IT teams have less actionable alerts to deal with, and hence can deal with many more.

C - Collaborate: Use social collaboration technology to orchestrate push notifications of relevant domain experts, getting them together in a virtual war room we refer as Situation Rooms. Here, the experts can log communications, query other tools, and capture the remediation process, automating knowledge recycle and keeping in sync with the Service Deck team.

The following screenshot **(Figure 4)** shows after the above 3-step automated process, a large enterprise user with ServiceNow ITSM has reduced its raw events from nearly 96,000 to 32 situations, i.e., only 32 incidents were escalated to ServiceNow Service Desk. Other raw events and alerts were either discarded as noise, or clustered together with narrative of causes and impacted services.

FIGURE 4: Tens of Thousands of Raw Events Reduced to 32 Situations for ServiceNow ITSM

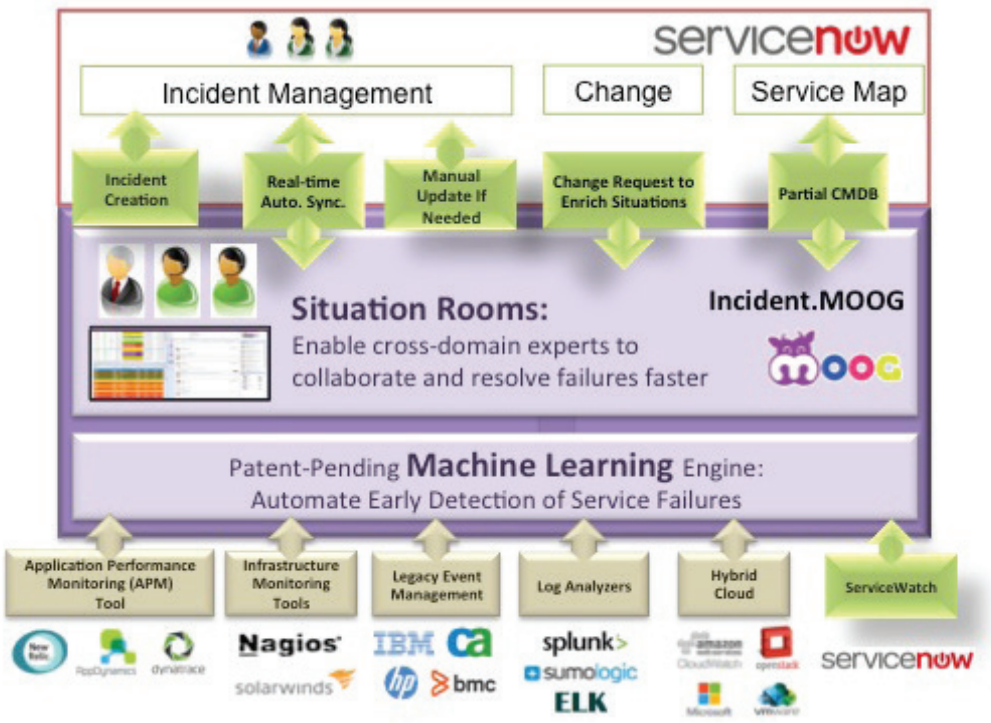


As we will discuss short below, this process is where much of the integration occurs between Incident.MOOG and the ServiceNow Service Desk.

4.0 A ServiceNow Certified Implementation of Incident.MOOG

Figure 5 depicts a reference architecture showing how Incident.MOOG fits into your ServiceNow ITSM environment. Let's now walk through this architecture, starting from the bottom of the figure.

FIGURE 5: ServiceNow Certified Implementation of Incident.MOOG



To present a cleaned and contextualized set of events across your entire IT environment, Incident.MOOG casts a much wider net by ingesting a greater variety of data events. This is where the bottleneck of detecting early and seeing full context can be removed. These event data can come from any technology domain (**Table 1**):

TABLE 1: Incident.MOOG Ingests Big Data Events across the Entire IT Environment

Categories of Tools	Examples
Application Performance Monitors (APM)	New Relic, AppDynamics, Dynatrace
Infrastructure Monitors	Nagios, Solarwinds, CA NimSoft
Legacy Event Managers	IBM Tivoli Netcool, BMC TrueSight Event Manager, CA Spectrum, HP OVi
Log Monitors	Splunk, Sumologic, ElasticSearch (ELK)
Cloud Monitors	Amazon CloudWatch, Openstack, VMware, Microsoft Azure
Customer Experience Monitors	Social Media Channels (e.g. Twitter), CEM Tools

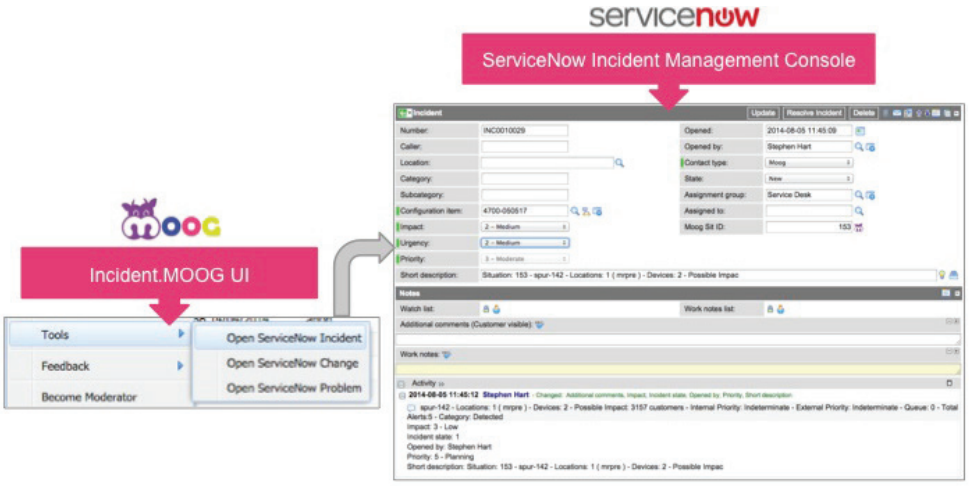
At the top of Figure 5, Incident.MOOG Situation Room integrates with ServiceNow Service Desk to automate generate of cleaned, fewer, and contextualized incidents, as well as keep sibling incidents and situations in sync. This is where the bottleneck of restoring services is removed, described in greater detail next.

5.0 Rapid 2-way Integration between Incident.MOOG and ServiceNow: Restore Services NOW

To effectively accelerate the workflow between backend operations and Service Desk, the integration points between Incident.MOOG situation room and ServiceNow ITSM include: incident management, change management, and ServiceWatch Service Mapping (CMDB). Specifically, these are the Moogsoft certified, out-of-the-box integrations with ServiceNow Incident Management:

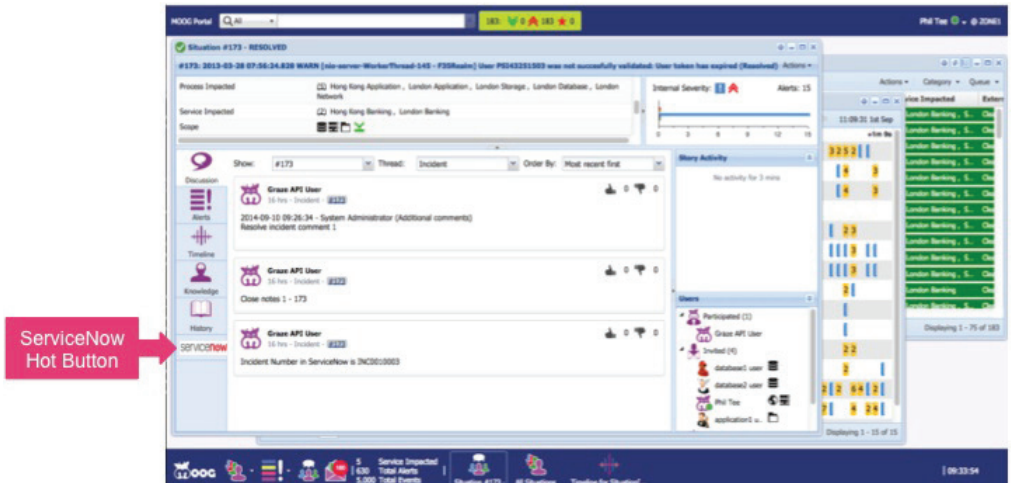
5.1 Automatic Creation of Incidents: For specific types of situations created in Incident.MOOG, Incident.MOOG Situation Room can be configured to automatically create an incident in ServiceNow Incident Management console. IT operations teams can do this on behalf of the ServiceNow Service Desk team, giving them earlier visibility into incidents, so they are more knowledgeable when customers call to report the incident. This is shown in Figure 6.

Figure 6: Automatic Creation of Incidents from Incident.MOOG Situation Room UI



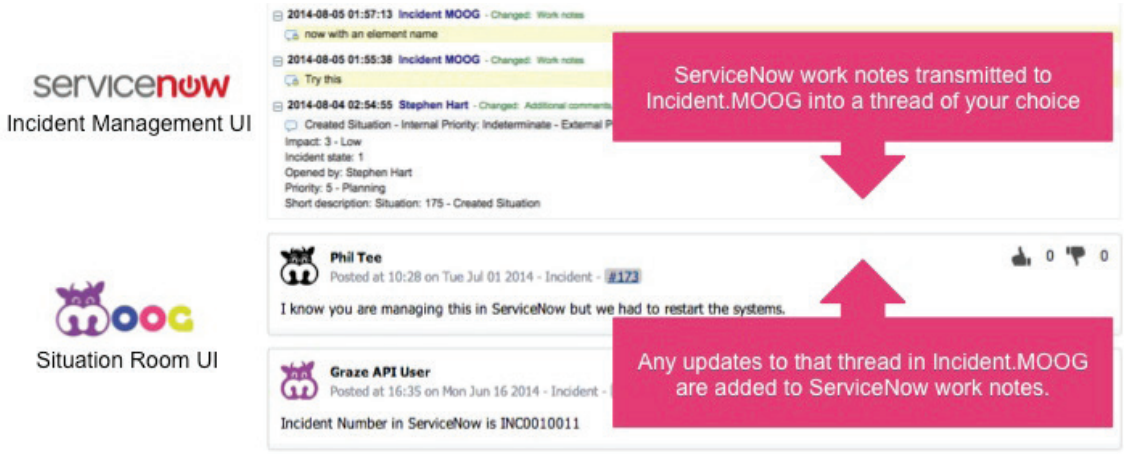
5.2 Real-time Synchronization: Real-time bi-directional updates are synchronized between an Incident.MOOG "situation" and a ServiceNow "incident". When either the situation or incident is closed, the synchronization will automatically resolve the other. The ServiceNow "hot button" in the Incident.MOOG situation room in Figure 7 indicates this integration.

Figure 7: Real-time Synchronization with Incident.MOOG Situations and ServiceNow Incidents



The screenshot below (**Figure 8**) shows ServiceNow discussion threads are transmitted to Incident.MOOG, into an operator-selected conversation thread. Any updates to that thread in Incident.MOOG are automatically added to ServiceNow work notes.

FIGURE 8: Real-time Synchronization of Discussion Threads



5.3 Two-way Visibility: Via a "hot link" in ServiceNow Incident Management UI, Service Desk staff have a 'live' view of the related incident embedded in the situation room. The Incident.MOOG icon takes the user directly to the Situation Room and alert list in Incident.MOOG Situation Room. Service Desk staff can also see related incidents in ServiceNow. This is shown in Figure 9.

FIGURE 9: Two-way Visibility, e.g. See ServiceNow Incidents in Incident.MOOG Situation Rooms

Conversely from Incident.MOOG Situation Room, operations teams can also view the associated ServiceNow incident and update its record. Also, multiple incidents can be associated to a single situation, this greatly reduces redundant workloads and confusions when multiple customers call in to complain about the same situation.

These integrations work with standard ServiceNow security mechanisms, and support all deployment options - e.g. Incident.MOOG on-premise and ServiceNow in the cloud.

5.4 Going forward, there are additional integration points to be certified by ServiceNow and Incident.MOOG:

- **ServiceWatch**: Incident.MOOG adds an out-of-the-box Link Access Module (LAM) to ingest the events and alerts from ServiceWatch into Incident.MOOG situation clustering/contextualizing engine.
- **Service Maps:** This is the ServiceNow CMDB with a visual front-end, which can display relationships between Configuration Items (CIs) and Services. Incident.MOOG enriches this CMDB to show the components that are failing in their mapped display. This is shown in Figure 10.

FIGURE 10: Two-way Visibility, e.g. See ServiceNow Service Maps in Incident.MOOG Situation Rooms

- **Change Request**: Incident.MOOG enriches a situation with the associated ServiceNow change request, so that the situational analysis presents how changes may have triggered an outage. Incident.MOOG enriches situations by dynamically cross-referencing change information between Incident.MOOG and ServiceNow. Operations teams can also reduce spam alerts, by creating a blackout list via dynamic lookup of Configuration Items (CIs) under maintenance.

With Incident.MOOG, all these integrations can be easily achieved using a RESTful API.

6.0 Summary

ServiceNow ITSM has transformed IT to a service-centric experience. Now IT operations support needs to transition in the same way. But without a modern, new approach to the event management backend – one that's change-tolerant and situation aware - the benefits of ITSM are at risk.

Situational Awareness for ServiceNow allows IT operations to detect real incident-triggering alarms up to 24 hours earlier than legacy event managers. It reduces spam events, alert storms, and false incidents by up to 99%. And it restore services hours or days before incidents cascade widespread.

Instead of relying on what is not longer reliable – a fully accurate configuration model and singular root cause – to make event management work and scale, Incident.MOOG allows IT ops teams to leverage analytics to break free from rule-based models, and then adds the narrative context to find multiple cascading issues earlier, accurately, and efficiently.

This is the modern event management approach that you need to support your IT environment today. Your event management must now be agile, tolerant to change and variability. You also need a situation-based approach with embedded collaboration tools to get the right people together to restore the problem quickly.

Incident.MOOG is a ServiceNow certified, modern event management backend you need that tightly integrates with ServiceNow IT Service Management and IT Operational Management products.

As parting words to ponder, consider how you can achieve visibility across your entire IT environment, and how to convert all your monitoring data into full 360 degree situational awareness. As you look to the future as your business grows and IT complexity increases, ask yourself some critical questions: Can your event management system cope with a 10 fold increase in scale? How long does it take to commission something new into monitoring? How will this all look when you're deploying multiple new apps daily as you move to DevOps? And finally, is your ServiceNow ITSM operational ready?

For more information, visit www.moogsoft.com.

U.S. 140 Geary Street
Office 1000
San Francisco, CA 94108
+1 415 738 2299

U.K. The Sanctuary
23 Oakhill Grove
Surbiton KT6 6DU
+44 208 399 8266

NY +1 646 843 0455

Singapore +65 3158 4393