

## Machine Learning Data Correlation, MTTR

## Machine Learning Data Correlation, MTTR



## Monitoring in a Connected Enterprise:

# Machine Learning, Data Correlation, and MTTR

***Discovering, responding to, and resolving incidents in a DevOps environment is a complex endeavor. This narrative attempts to show how a company could do it quickly and effectively with a toolchain of AppDynamics, Moogsoft, and xMatters. AppDynamics is an Application Performance Management and ecosystem monitoring tool, Moogsoft is an ecosystem management system, and xMatters is an integration-driven collaboration platform.***

At 8:15 am, Darla, the Operations Response Director for First Universe Bank, blinked at the screen in front of her. Her monitor looked largely the same as any other day, with dashboards tracking user experience and transactional performance across the most critical revenue impacting business applications. Then she started getting baseline deviation alerts from AppDynamics, her APM monitoring tool.

AppDynamics was showing that the Automated Underwriting System (AUS) for First Universe Bank was intermittently showing slower than normal response time. Lags could quickly become bottlenecks, outages, or outright failures. Since there were no alerts coming in from anywhere else, her playbook called for her to check the AppDynamics console to see what was going on. The AUS product owners hadn't reached out, so at least there were no obvious indications of a service-impacting incident. She performed a quick check for active change tickets or other work that might explain the anomalies. Darla was also keeping an eye on the ticketing queue numbers in case employees were feeling the impact of the violations AppDynamics was reporting; but again, all looked normal.

Failure Rate ▾

## SYSTEM HEALTH

Refresh ↻

Nov 15, 2018 11:46 AM CET

### EVENTS

● Application Errors ● System Errors





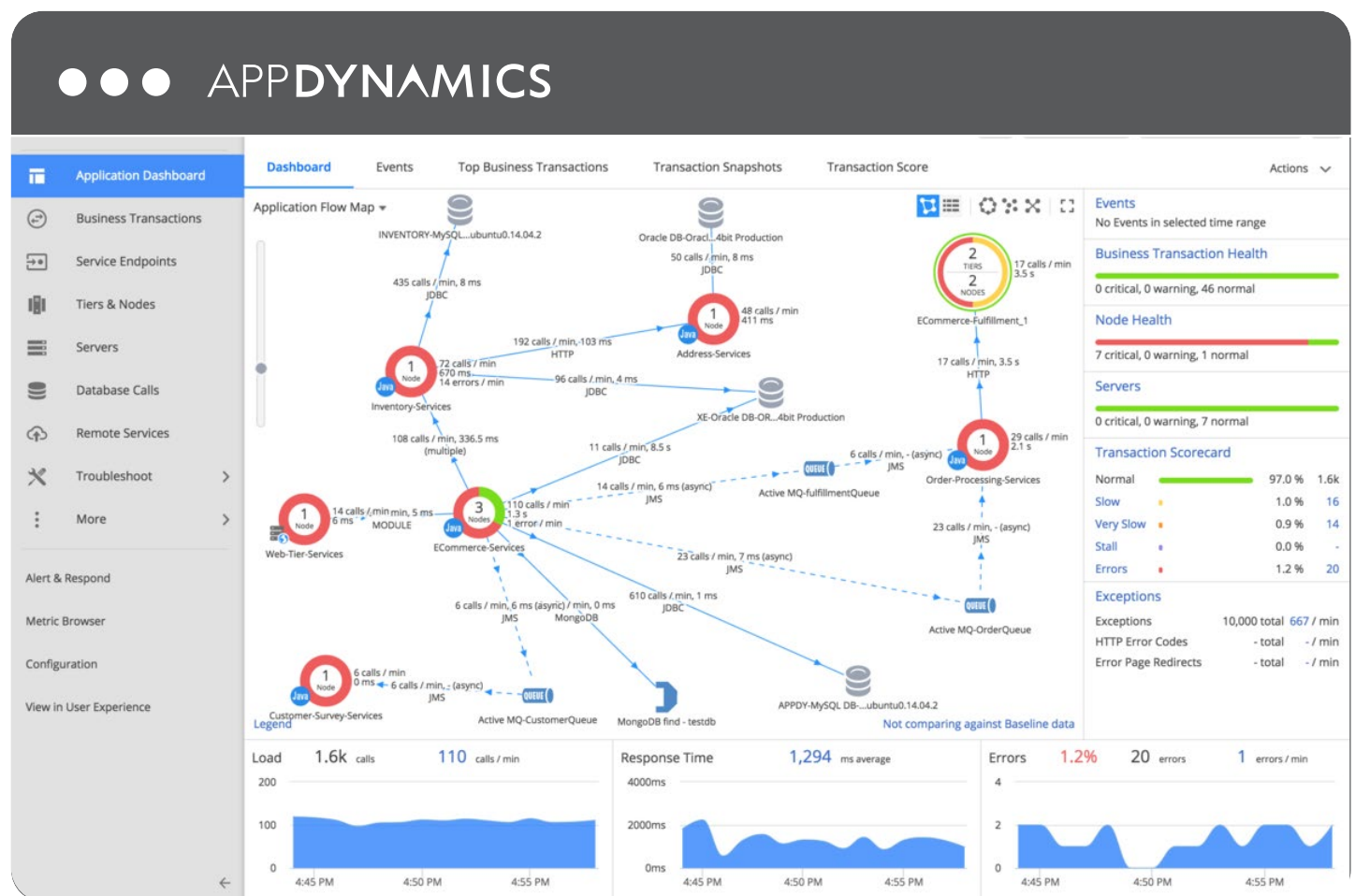
The AUS takes new insurance policies, queries actuary tables, and pulls in other information. When it gets an error in an associated system, it signals an error and maps it back to originating systems.

She knew there was an issue with a system associated with the AUS, but she didn't know:

- Which system?
- What error?
- When was the error introduced?
- Who made the error?
- What other systems might be affected?

To make good decisions, she had to correlate data and find the root cause. She remembered something one of her idols had said once. David Eagle, Manager of Enterprise Monitoring Systems at Pacific Life, says correlation is key. "You have to correlate data with regressions through your APM so you can pinpoint when changes were made and who made them," Eagle explains. "Then you have to notify the right people."

No one person or tool can uncover the root cause, discover all the potential effects of the issue, notify the right people, and fix the problem, Eagle explains. "Compound integrations play a huge role in resolving issues as quickly as possible." Common tools include originating applications, data analytics, issue management, chat, and communication.



AppDynamics reveals interdependencies with auto-generated flow maps, and traces key business transactions based on production application behavior.

Following the AppDynamics flow map, which shows application transaction dependencies and performance anomalies, Darla was quickly pointed to likely culprits. She didn't get very far before an AppDynamics "red alert" popped onto her Moogsoft screen. Moogsoft is an event correlation platform, and Darla accessed AppDynamics and other tools through its interface.

Things were lighting up on her AppDynamics screen, and it wasn't going to be long before users started reporting issues and this became business-impacting. It was time to bring in the DevOps team that is responsible for all underwriting apps at First Universe Bank.

“Compound integrations play a huge role in resolving issues as quickly as possible”

## Common Mistakes in Monitoring Solutions

Darla knew some organizations are still stuck in the “right way” of 2007. David Eagle had told her several ways they fall behind:

- They map out their apps and services manually, cross-reference against org charts, and hope they defined all the dependencies.
- Some still create CMDBs manually.
- They set static thresholds for monitoring and alerting systems to be notified of faults.
- They neglect the data quality of the CMDB, which is critical for production workloads. If people don't trust or use the CMDB, there's no feedback loop and therefore nothing improves.
- They try to capture everything in a CMDB or ignore it completely.
- They roll out a CMDB without specific goals in mind, then expand it into an unwieldy mess.

Other common errors are less technical. Some organizations don't define major incident management processes well, rendering even the best tools ineffective.

“A person has to acknowledge an escalated alert,” Eagle says, “and he is on the hook until the application developer says OK. It starts with knowing when – and to whom – to send an alert.”

“A person has to acknowledge an escalated alert”

# AppDynamics, Moogsoft, and xMatters

AppDynamics and Moogsoft both have built-in integrations with xMatters, which integrates with chat tools (including Slack and HipChat), issue resolution solutions (Jira, Confluence), service desks (Zendesk, ServiceNow, BMC Remedy, Cherwell), or virtually any other tool you might want to use.

Darla opened a Jira issue and updated StatusPage for the AUS with a message so customers and employees could stay up to date through self-service.

The strength of xMatters is its ability to connect systems and tools to relevant people. When Darla needed to investigate the initial notification, she used xMatters to find the right person or group so she could assess whether she had a major incident in minutes, not hours.

AppDynamics learns the applications in your ecosystem and automatically visualizes complex web and mobile applications that reveal interdependencies with auto-generated flow maps. Using AppDynamics, Darla can trace key business transactions based on production application behavior and see which other applications and services are likely to be affected.

To provide visibility across First Universe Bank's entire production stack, Moogsoft applies a series of machine-

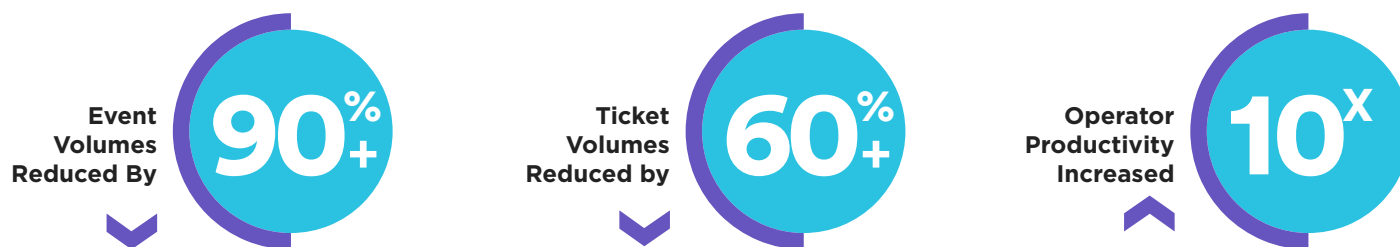
learning algorithms to correlate alerts across applications, networks, and infrastructure.

"DevOps and IT Ops roles know monitoring with additional correlation produces insights that other organizations miss," says Matthew Harper, Vice President of Marketing at Moogsoft.

DevOps and IT Ops at many large organizations augment a leading monitoring platform like AppDynamics with other tools. Together they provide important visibility into each component of their applications, network, and infrastructure. The challenge is that event volumes are now so large that human operators are no longer capable of manually analyzing these alerts, detecting incidents, and furthermore, understanding relationships across alerts for context.

While Darla and her team still need to be at the center of troubleshooting complex incidents, machine learning and AI must be applied to automate the tasks of identifying the signal in the noise and discovering relationships across toolsets.

With this burden taken off of humans, DevOps and Ops can be more agile than ever before without worrying about instability introduced by change. Moogsoft sees real results for its customers:



Darla used an xMatters integration with Slack to automatically post to a major incident Slack channel and open a new ticket based on the reference number.

Engaging the DevOps team was a quick step that involved selecting the Moogsoft alert on the console and paging them via the xMatters alerting channel. Darla put on her Incident Manager hat and fired up a Moogsoft Situation

Room, where relevant people could collaborate in a social environment. Her role now was to provide cover for the DevOps team and others who might step in, help keep track of tasks that everyone was working on, and keep any stakeholders in the loop, all the while making sure that key information was being tracked for review after everything was back to normal.

Moogsoft Cloud DevOps

COLLABORATE TASK BOARD

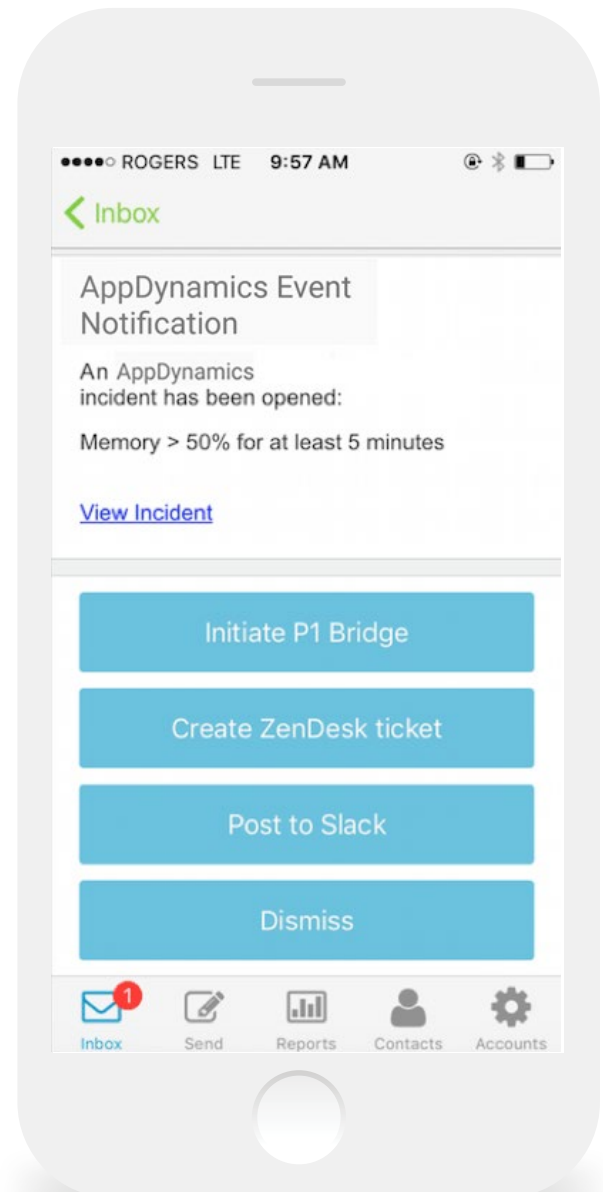
OPENED	ASSIGNED	IN PROGRESS	RESOLVED
<b>#175</b> 15:46:33 02/21/2017 Alerts with a similar description [ASSIGN] [OWN]	<b>#170</b> AB 15:45:40 02/21/2017 Alerts from a similar source [OWN]	<b>#180</b> A 15:47:16 02/21/2017 Critical Alerts [RESOLVE]	<b>#162</b> A 15:44:38 02/21/2017 Alerts from a similar source [CLOSE]
<b>#173</b> 15:46:16 02/21/2017 Critical Alerts [ASSIGN] [OWN]	<b>#172</b> AB 15:45:56 02/21/2017 Non-Critical Webserver Alerts [OWN]	<b>#177</b> A 15:46:37 02/21/2017 Alerts from a similar source [RESOLVE]	
<b>#168</b> 15:45:31 02/21/2017 Alerts with a similar description [ASSIGN] [OWN]	<b>#167</b> AB 15:45:01 02/21/2017 Non-Critical Webserver Alerts [OWN]	<b>#105</b> A 15:35:00 02/21/2017 Non-Critical Webserver Alerts [RESOLVE]	
<b>#165</b> 15:44:46 02/21/2017 Critical Alerts [ASSIGN] [OWN]			
<b>#157</b> 15:43:38 02/21/2017 Critical Alerts [ASSIGN] [OWN]			
<b>#156</b> 15:43:32 02/21/2017 Alerts from a similar source [ASSIGN] [OWN]			

A Moogsoft Situation Room provides situational awareness for relevant stakeholders.

The on-call DevOps engineer, Alfonso, received an xMatters alert on his Pixel XL phone, responded to the alert to take ownership, and quickly stepped into analysis mode. His xMatters alert responses were relayed to Darla and she brought him into the Moogsoft Situation Room. Alfonso confirmed that the AUS spikes were indeed getting more frequent and pronounced, and users were very likely starting to see slow or unresponsive behavior from the app. The AUS runbook called for an AppDynamics deep dive to get the resolution process started in earnest.

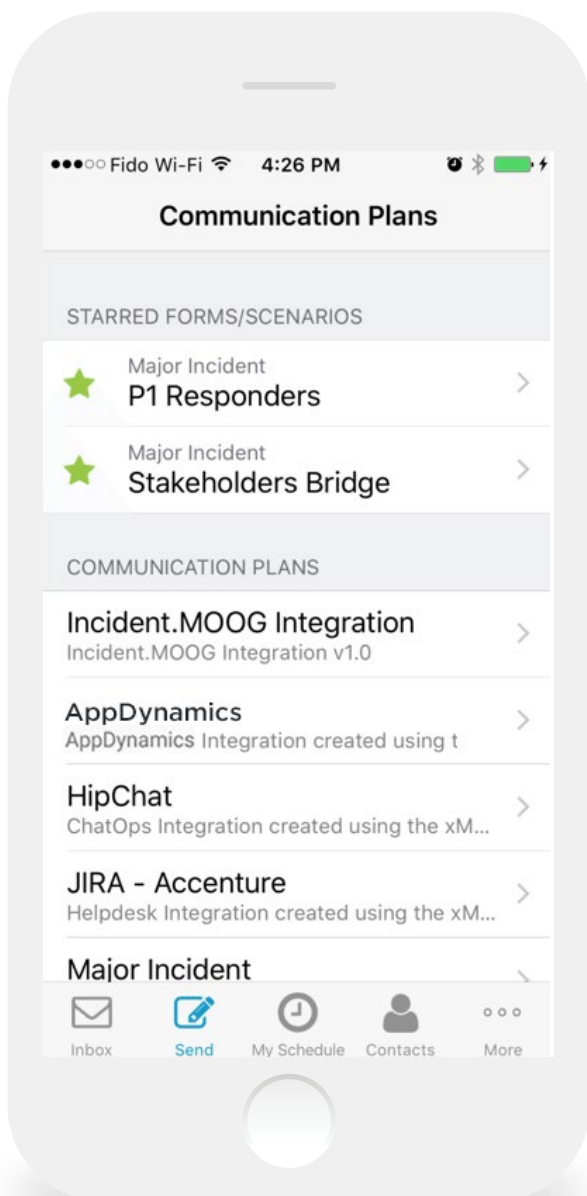
The DevOps team relied on AppDynamics in all stages of the lifecycle of the AUS, so Alfonso quickly eliminated front-end issues and core app issues. The AUS app was dependent on a number of Postgres data repositories, and one of the critical paths was intermittently failing and the retries were slowing down the whole app. The application maps, thresholding, and drill-down metrics seemed pretty clear. That meant that he needed help from outside the DevOps team and maybe one of the core developers to help focus the resolution path further.

Alfonso popped back into the Situation Room and used the xMatters integration to round up the additional help. The AUS dev team always had an on-call person designated, as did the Postgres admins, both listed by their respective team leads in xMatters so there was no manual hunting around required. As xMatters was hunting down his soon-to-be extended incident management team, Alfonso brought Darla up to speed on the situation.



*Taking action directly from a notification in xMatters.*





xMatters notifications provide a range of next steps with embedded closed-loop integrations to other systems in the toolchain.

Darla confirmed to Alfonso that there was user impact and she could see it in a spike of reported incidents from users of the AUS. With the involvement of other teams on this incident, increasing reports of user impact, and the criticality of the AUS, Darla had to start the stakeholder communication process. She took what was known, summarized key activities to date, and got that information out via the xMatters communication scenario for this type of issue. Anyone who was pre-designated to receive those alerts, or had subscribed to them, would now be in the know – which would take a little heat off the service management teams.

## Monitoring basics and the relation with DevOps

Successful DevOps typically leads to more frequent deployments of services and applications that are implemented with diverse technologies. The top complaints we hear from Operations teams in DevOps organizations are increased technical complexity, poor code and monitoring quality, alert overload, and disruption of traditional operations teams.

For Darla and others responsible for operations responses, solving these problems starts with a better monitoring approach across the tools and services in an enterprise. Having more data doesn't mean better answers – unless you have the ability to automate data correlation and detect anomalies that impact your end users or SLAs.

Automated testing in both development and production environments can lead to better code maintenance so teams can correct issues before they affect customers. Effective testing is a discipline that goes hand-in-hand with an effective monitoring strategy.

# Analysis and Resolution

With all the on-call parties having been brought into the Situation Room, including Bort the developer and Alicia the DBA, they quickly figured out that it was a Postgres maintenance task run amok that was the root cause of the problem. Without insight into Postgres maintenance, they were always in reaction mode and unable to anticipate such tasks. Bort confirmed that the AUS would appear to be in an unhealthy state unless this particular application data request was fulfilled consistently and with a more predictable response time. Alicia cleared the maintenance tasks while the rest of the team kept an eye on their monitors, with Darla on end user response time and ticket volumes, and Alfonso and Bort on AppDynamics.

As the indicators on each of their consoles gave the all clear, Alfonso marked the incident as resolved and released Alicia and Bort back to continue their day. Darla used xMatters to send out a final “all-clear” update to all

the stakeholders for the AUS. She also added in any last-minute details into the Situation Room before closing it out. All the information shared during the collaborative firefighting exercise would come in handy for problem management and continuous improvement tasks. The StatusPage updated automatically.

Their operational processes had worked just as intended. Moogsoft alerted Darla, Alfonso and Bort were able to quickly isolate the problem at the level of detail each needed, and Alicia was confident that when the team came to her, it was because they knew she could help, not just a random call for everyone. In fact, from the initial “yellow-alert” all the way to resolution and incident closure, only the people who needed to be engaged were brought in via xMatters, which also kept all the stakeholders up to date, inspiring confidence in how the First Universe team IT org operates.

# Conclusion

With the issue resolution confirmed, xMatters automatically updated the status page for the AUS and preserved all the chat conversations in the issue resolution tool to be used for a post mortem. Splunk archived data to help improve responses for future issues. And Darla was able to do her real job.

As business accelerates and the stakes get higher, you need to use the right tools and implement effective processes to proactively prevent issues and resolve them quickly when they do occur. The potential impacts of major incidents on the business are huge:

- **Financial impacts**
- **Penalties and fines**
- **Loss of customer trust**
- **Public relations disaster**

That's why tools that can perform multiple jobs at an extremely high level are so valuable. AppDynamics finds issues, but its differentiator is its ability to find the root cause – not just at the application level, but all the way down to the code level. Moogsoft correlates data and also sets up a virtual war room to manage issue resolution.

The scope of a major incident can increase over time, so the ability to chain together all your issue resolution tools is crucial. You cannot afford to have data stuck in a silo where people like Darla can't access it. That's where xMatters comes in. Its integration platform enables applications across your toolchain to share data with each other and with important stakeholders so you can resolve issues fast.

With more than 200 integrations across a wide range of IT tools, xMatters automates and brings structure to collaboration. Build critical toolchains to proactively prevent outages, resolve incidents, and keep the right people informed.



## (x) ABOUT US

xMatters is an integration-driven collaboration platform that relays data between systems while engaging the right people to resolve incidents. The platform automates, operationalizes and contextualizes communications within key DevOps processes, fundamentally altering the way business units work together. xMatters also supports enterprises through major incident and change management, alerting the right people on the right channels to time-sensitive events and problems like network outages, supply-chain disruptions, natural disasters and medical emergencies. Founded in 2000, xMatters is headquartered in San Ramon, CA, with additional offices worldwide. For more information, please visit [xmatters.com](https://xmatters.com).

**Copyright 2018 xMatters.** All rights reserved. All other products and brand names are trademarks or registered trademarks of their respective holders.