BMC CLOUD OPERATIONS USES TRUESIGHT CLOUD SECURITY

Yes, we eat our own cooking.

Have you ever wondered how BMC Software keeps its cloud environments safe and secure? One of the proudest and most thrilling moments for our Cloud Engineering team was using our TrueSight Cloud Security, BMC's very own automated cloud security and compliance solution, to achieve 100% compliance of our multiple cloud environments. Seeing that dashboard transform from red to green in such a short time was quite an achievement. In this blog, we describe how we run Dev environment security with TrueSight Cloud Security (TSCS). BMC being our first customer provides us direct feedback so that we continuously deliver an ever-improving solution.

The Challenge - You cannot manage what you don't measure

We have thousands of cloud resources changing every day in our development cloud accounts as developers continuously push new functionality to prod. S3 buckets, firewall security groups, IAM roles, EC2 instances, and more are created or updated with daily pushes through DevOps pipelines. After each release, the big question on everybody's mind was, "Are we secure? Did we mistakenly open a port to the internet?" Yes, just like your dev teams, we are constantly striving to increase our agile velocity; yet, we do not want to compromise on security. The old business axiom, "You cannot manage what you do not measure" is especially true for DevSecOps and cloud security. So, our first step was to benchmark our security posture and look for ways to fix high risk vulnerabilities, burning down our security backlog to secure our cloud resources... and keep them that way!

The First Security Scan

It took us less than an hour to assess our security posture, much to the delight of the team and exactly as we had envisioned when we set out to build our cloud security service. We pointed TSCS cloud service to our own AWS cloud accounts and started scanning them for CIS compliance with over 50 controls for AWS. Within a few minutes, we finished the setup, and the initial security posture data started lighting up on the dashboard. RED! To our surprise, about 15% of our resources were noncompliant to the CIS security benchmarks.

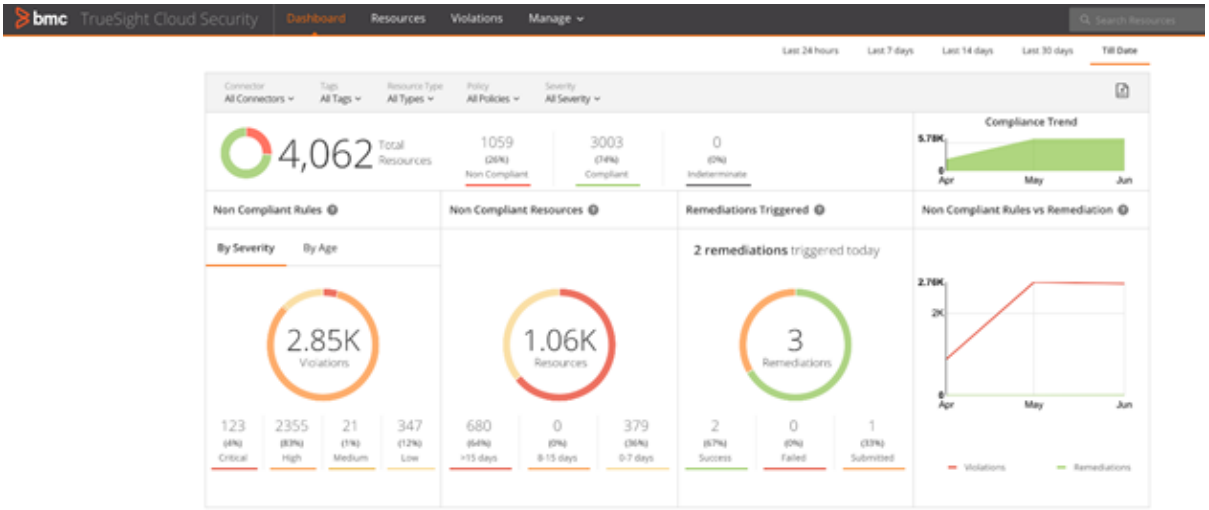

Figure 1: Example dashboard in TrueSight Cloud Security showing security at a glance

Thankfully, no S3 buckets were open to public, as so many highly publicized data breaches were caused by publicly accessible S3 buckets. With automation built-in by design, TrueSight Cloud Security can easily find and fix such open public buckets in minutes. We were, however, alerted that 50 S3 buckets did NOT have encryption turned on. Ouch. Encryption at rest is a best practice for data security that we needed to resolve. We also found 70 IAM policy rule violations, such as lack of MFA, lack of key rotation, and more. Key compromise is one of the ways that can lead to data or account breaches, and we knew this one also would need a quick resolution. Once we knew our complete security posture in our development accounts, the team started triaging, risk assessment, and putting together a plan for remediation. **PRO TIP: Assess posture, triage results, and build a remediation plan, much like you would groom a Scrum backlog.**

Instant Remediations

First things first: 70 critical IAM security violations were easy to fix, and the team remediated most of these through a single click from TSCS. Cloud Operations were confident about these not impacting Application and quickly remediated these. Nice going. As the engineering team kept deepening remediation action content, we soon realized the power of instant remediation with a single click from our UI. On a few others security issues, such as S3 buckets and EBS web tier encryption, the team created Jira tickets to track findings from TSCS and assigned them to developers. As our infrastructure is immutable, these issues were resolved through the DevOps pipeline updates to infrastructure. Within hours and days, we dramatically improved our security posture, with only 5% noncompliant rules remaining. Measuring security posture and reporting it in our dashboards and PDF reports motivated the team to continuously improve. **PRO TIP: Gamification of security posture**

across multiple accounts and teams clearly leads to higher security as nobody wants to be at the bottom of the security grade.

Exceptions

The process of managing security issues can at first seem daunting but TSCS helps manage the volume of these issues very effectively. Powerful search capability available in the UI details security posture by application, services, owner, or account tags, context which prioritizes the most critical app and infrastructure issues for resolution first. Many issues can be remediated quickly through actions from UI or through incident integration process. There are always exceptions. After discussing with Security, a few findings were identified as acceptable low risks and were moved to the bottom of the backlog. Security is a risk management process where highest risk issues need to be fixed first, while low risk issues can be deferred and put on an exception list. This is where our last of remaining 5% issues ended up. We used TSCS to mark the last of our findings as exceptions, to reduce noise and "alert fatigue" while the Dev team added this to their technical debt. **PRO TIP: Some security violations should not be resolved by Cloud Ops, but by Development. Use RBAC to provide remediation privileges to those who own the code. Use the UI to filter security by app, tag, accounts, etc.**

Multiple Accounts

As we completed securing our first batch of accounts, we quickly realized that multi-account management is a challenge. Leveraging the multi-account connector within TSCS, we created trust relationships to child accounts, streamlining multi-account security management. We now began collecting security data for multiple accounts. Teams are now filtering security findings by account and environment, as well as visualizing the aggregate security posture across accounts. Many enterprises, including BMC, have 100's, even 1,000's of public cloud accounts, where this account consolidation capability enables security at scale and simplifies security operations. **PRO TIP: Begin with the end in mind. Start small, securing a handful of accounts, and be prepared to use account consolidation to simplify your cloud security methods.**

We are the Watchers on the Wall

Getting the first scans and securing our accounts is only the first step. Are we done? Of course not. Our next step was to ensure that the high level of security is continuously maintained.

- Daily reports automatically notify us of new security violations.
- We are also working on a self-driving remediation feature, to automatically fix certain vital security issues (which we define), thereby reducing the mean time to resolve.

"We are the watchers on the wall... Night gathers, and so my watch begins... For this night, and all the nights to come." -- #GameOfThrones, from Oath of the Night's Watch

Take the Test Drive

Would you like to see what TrueSight Cloud Security can do for you? Take the free 14-day trial. Connect the service to your account. Kick the tires. See how it drives. Then, if you're interested contact Sales.