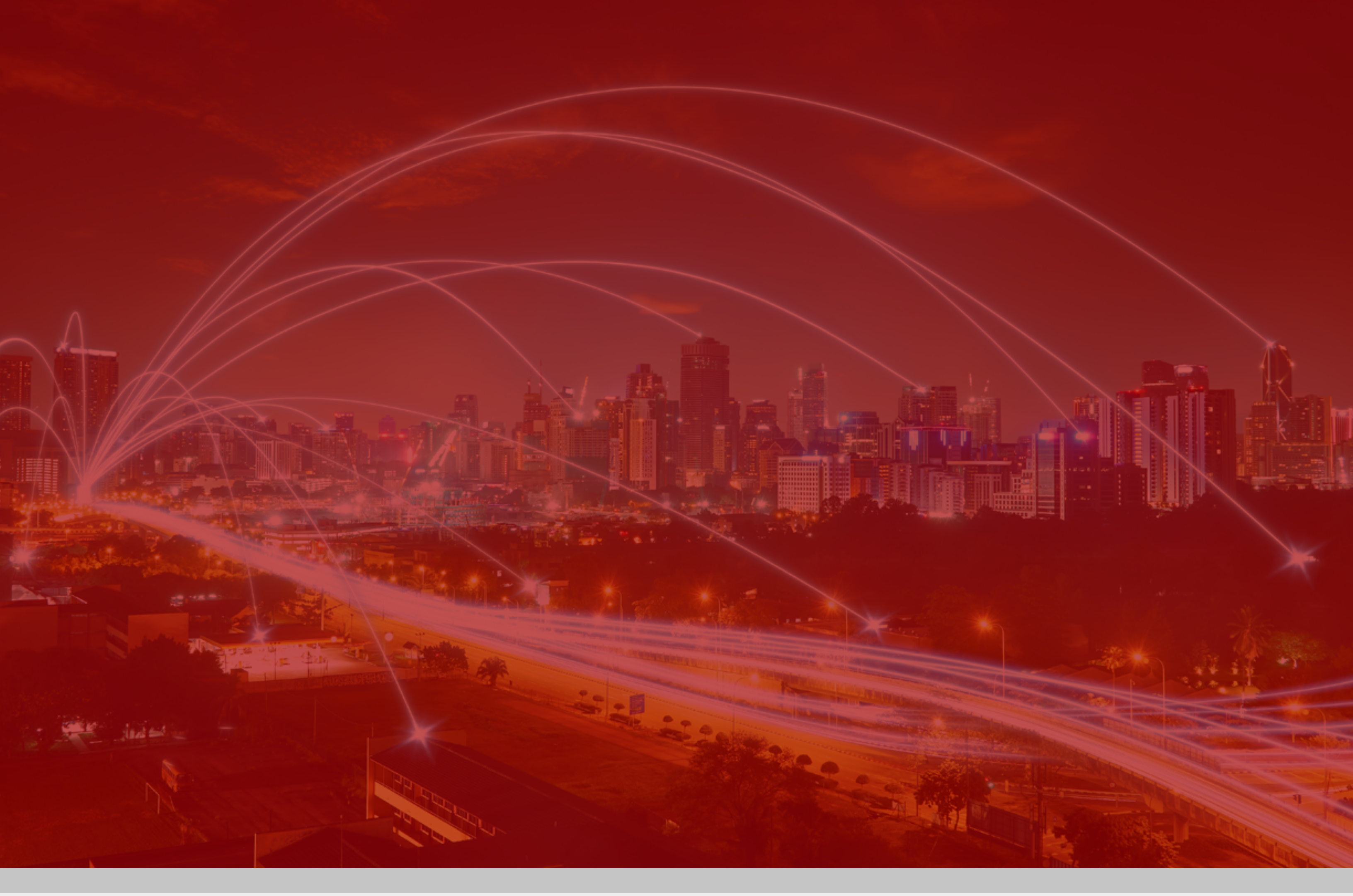

WHITE PAPER

BROADCOM®

A Broadcom Point of View

AISecOps from Broadcom®

Powered by Automation.ai

Bridging the Gap Between Security and Operations for Secure, Resilient Infrastructures

Table of Contents

Executive Summary 3

The Need to Understand Security Insights from an Operations Point of View 3

Recommendations for a Successful Start to Your AISecOps Journey 4

Our AISecOps Vision and Strategy 4

Conclusion 7

Executive Summary

Security operations (SecOps) is the collaboration of security and operations teams to integrate technology, people, and processes. The goal is to facilitate the successful implementation of resilient and secure infrastructure, applications, and data. AISecOps is the method of applying artificial intelligence (AI) and machine learning (ML) techniques to ingested security and operations data to improve accountability, visibility, and collaboration—all while automating operational tasks to maintain secure, high performance infrastructures.

The Need to Understand Security Insights from an Operations Point of View

The need for SecOps is probably best illustrated by recent Gartner research that reveals that 95% of CIOs expect threats to increase and impact their organization.[1] Additional research from Gartner states that approximately 70% of data center networking tasks are performed manually, which increases time, cost and likelihood of errors, and reduces flexibility.[2]

> "95% of CIOs expect threats to increase and impact their organization."

Network operations (NetOps) teams have always cared about security, but they live in a world ruled by innovation, the need to lower operational costs, and impossible SLA guarantees. They are responsible for maintaining rapidly-growing network environments which are often made up of tens of thousands of physical or virtualized components, and also using them to deliver more and more value to the business and its customers.

Due to historic divisions, there's little coordination among tool buyers within NetOps and security teams. This lack of coordination is present even if those tools share common instrumentation points and use cases. This always leads to duplicate efforts and wasted money. Additionally, modern network complexity and threat sophistication mandates that NetOps and security teams automate low-level tasks and improve network traffic visibility for threat detection, analysis, and response. The increases in the use of the cloud, as well as network encryption, have also hindered network visibility for both teams, and the rise of disjointed NetOps and security initiatives exacerbates these challenges.

Unfortunately, today's network performance is often crippled due to security bottlenecks and network designs that leave critical resources vulnerable and exposed. An intersection and overlap in network operations and security is essential for establishing a defensive posture and risk management approach required by today's dynamic environments. Gartner agrees in their latest research that the goals of network operations are increasingly aligned with security operations, which share the objective of guaranteeing a well-performing and secure network.[3]

[1] **https://www.gartner.com/smarterwithgartner/why-cisos-must-evolve-alongside-cios/**

[2] 2019 Strategic Roadmap for Networking, Published 10 April 2019 - ID G00377506

[3] 2020 Market Guide for Network Performance Monitoring and Diagnostics, ID G00463582

Recommendations for a Successful Start to Your AISecOps Journey

In order to successfully build SecOps practices, Broadcom® recommends focusing on tools, processes, and people. Tool rationalization is the easiest to implement and provides the most savings back to the business. Explore the possibilities of using a common tool that shares similar capabilities like log management, change tracking, event management, network traffic analysis, and remediation/automation—all while exposing this data to a shared data lake where AI and ML methodologies can be applied. Teams could measure success with improved visibility into operational data and performance levels as well as a reduction in the costs of duplicate solutions.

> "In order to successfully build SecOps practices, Broadcom recommends focusing on tools, processes, and people."

Aligning security and operational processes and workflows will undoubtedly bridge the gaps that have existed between these teams for years. Bridging these gaps opens up new possibilities for automation, coordination, and communication. This process can be challenging. But with the adoption of a tool rationalization strategy, information sharing will significantly improve visibility across the different teams and improving response and remediation times.

Finally, people are the hardest to change as it would require changes in organization, company culture, and human mindset. But aligning people from both teams to coordinate closely and enact fine-tuned role-based access controls will allow security to identify issues and apply approved fixes quickly, while still giving operations the oversight and control to test and ensure that proposed security fixes don't hinder critical business network operations. Such changes like these would take time and should be tackled last.

Example of IT Operations roles and their responsibilities that would benefit from access to security insights:

- Level 1 network operations staff who are responsible for quickly finding the root cause of any outage among the thousands of alarms they receive. They must remediate the issue or quickly route it to the appropriate team member.
- Site Reliability Engineers (SREs) who are responsible for the overall customer experience based on the right monitoring data across development, test, operations, and security that delivers improved service-levels and business results.

A triage example covering both roles would be a high number of application logins or high network bandwidth usage detected. Could this be due to an application, infrastructure or network problem, or are we under a distributed denial-ofservice (DDOS) or an insider attack?

Our AISecOps Vision and Strategy

Our AISecOps capabilities will be powered by Broadcom's Automation.ai, the industry's first AI-driven software intelligence platform. Automation.ai harnesses the power of advanced AI, ML, and Internet-scale, open-source frameworks to transform massive volumes of enterprise data into actionable insights. Automation.ai offers this unparalleled combination of features:

- **AI-driven services** – The platform provides a predefined, prepackaged set of automated, AI-driven services for analysis, correlation, recommendation, and remediation.

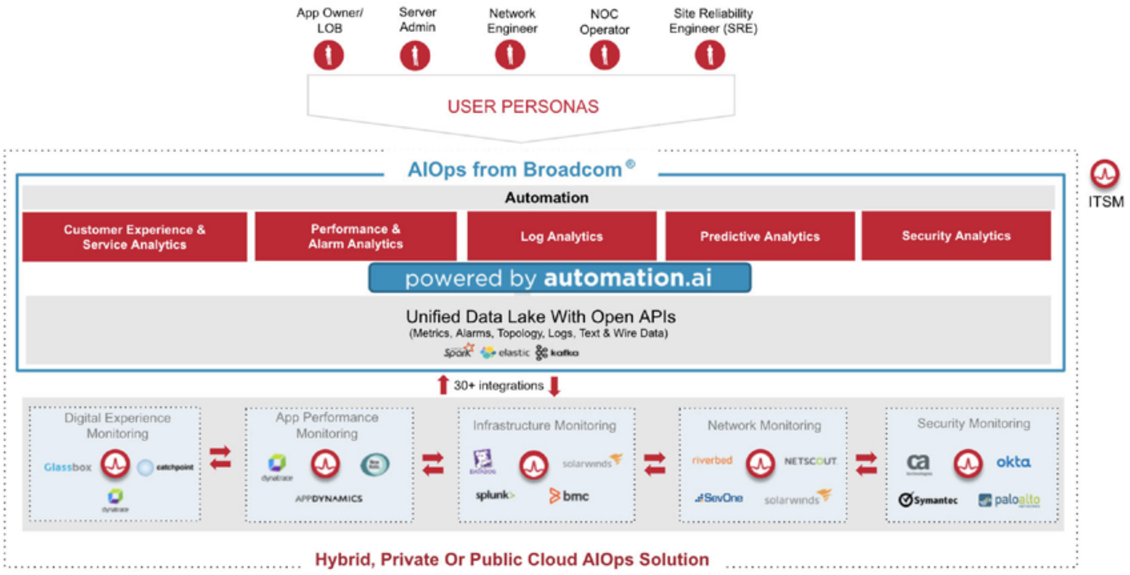

Figure 1: Cross-Domain, Contextual Intelligence to Run Reliable Infrastructures that Deliver Exceptional Customer Experiences.

- **Openness** – The platform ingests data from across the software development lifecycle, and from a comprehensive range of systems, including Broadcom products, third-party tools, and open-source platforms. The solution offers an advanced data ontology that enables contextual, yet unified aggregation of diverse sets of IT and business data.
- **Continuous learning** – Automation.ai continuously validates and improves decision making methodologies based on real-world outcomes.
- **Extensibility** – The platform can be run entirely independently or incorporated into a customer's existing AI and machine-learning frameworks.
- **Multi-cloud support** – Automation.ai employs Kubernetes-based orchestration capabilities that are fully containerized, enabling efficient implementation across multiple ecosystems, including public and private cloud environments.

> "AIOps from Broadcom correlates data across users, applications, infrastructure, network and security services."

Core to the success of our AISecOps vision is AIOps from Broadcom. The solution delivers AI and machine learning, automation, and comprehensive ecosystem observability. AIOps from Broadcom correlates data across users, applications, infrastructure, network, and security services.

The solution then delivers cross-domain contextual intelligence by ingesting and analyzing a diverse data set including metric, topology, text, and log data providing your teams with:

- Service analytics that expedite root-cause analysis by providing end-to-end visibility across key business or IT services.
- Performance and Alarm analytics that reduce false and redundant alerts which reduces Mean Time To Repair (MTTR).
- Contextual log analytics that automatically correlates security and application events and performance data.

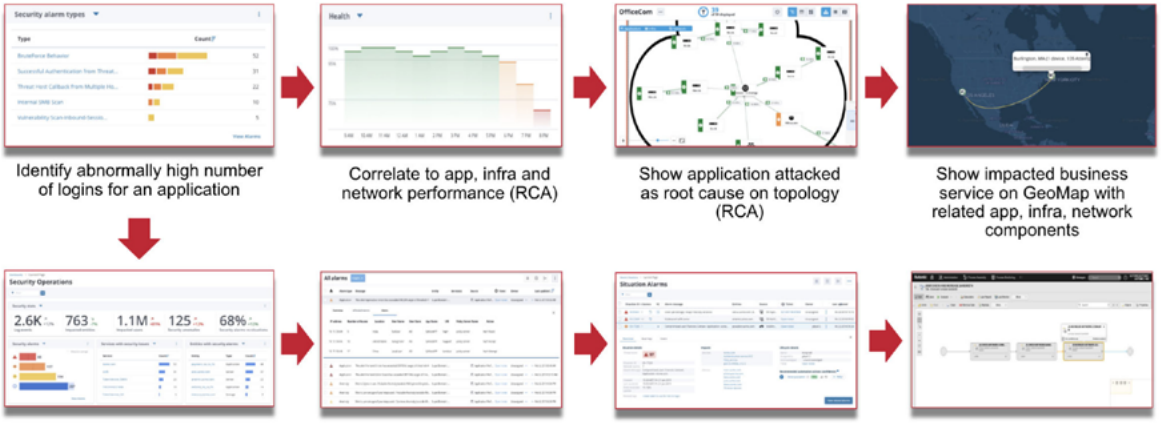

Figure 2: AISecOps Automated Threat Analysis Workflow Example.

Identify abnormally high number of logins for an application

Correlate to app, infra and network performance (RCA)

Show application attacked as root cause on topology (RCA)

Show impacted business service on GeoMap with related app, infra, network components

Identify the user(s) who are hitting the application highest number of times

Show the users (IP Addresses)

Show the devices used in security threat

Block user access automatically

- Predictive analytics to identify network bottlenecks before disruption and optimize resources by identifying waste.
- Contextual automation that delivers closed-loop, service driven autonomous remediation.

By reducing the gaps between security and network operations with a common AIOps solution, key capabilities that can be expected are:

- Improve visibility with security risk dashboards based on security logs correlated with Application, Infrastructure, and Network performance data.
- Monitor suspicious user activity and link it to the impacted applications and business services.
- Monitor misconfigured login policies or suspicious privileged user access change activities and link to impacted business services.
- Identify misconfigured software, hosts or routers, and link to performance.

Our goal and vision of AISecOps is to deliver unified dashboards for network management and security events, AI-powered threat detection for greater visibility and awareness, and automation to address sophisticated threats anywhere in the network. This is no more apparent then with the Broadcom AISecOps integration into Symantec™ Enterprise Business security solutions—providing unparalleled visibility for compromised known users and devices (User and Entity Behavior Analytics [UEBA]) with the ability to take immediate remedial action (Security Orchestration, Automation, and Response [SOAR]).

Additionally, data sources like firewall logs, identity and access management solutions, and logs from operating systems are also ingested and correlated with existing performance and security data to broaden threat detection and enrich operations with meaningful insights during the threat triage process.

Conclusion

You can count on Broadcom's rich experience in networking and network monitoring; as well as future integrations with Symantec Endpoint Security to deliver on the promise of AISecOps with a rich set of security data sources from user access, user activity, end points, application performance management, and security metadata. We have over 25 years experience in full-stack network monitoring with number one ranked solutions across troubleshooting, monitoring and capacity planning for traditional networks, software-defined and cloud technologies. Finally, we offer powerful AI and ML capabilities like log analytics, alarm noise reduction, anomaly detection, and automation remediation of network outages or security attacks.

To learn more about how Broadcom is connecting everything, please visit our site at **broadcom.com/aiops**.

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage and industrial. Our solutions include data center networking and storage, enterprise and mainframe software focused on automation, monitoring and security, smartphone components, telecoms and factory automation. For more information, go to www.broadcom.com.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.