Red Pill or Blue Pill? Navigating Compliance in Azure DevOps Security

Craig Forshaw

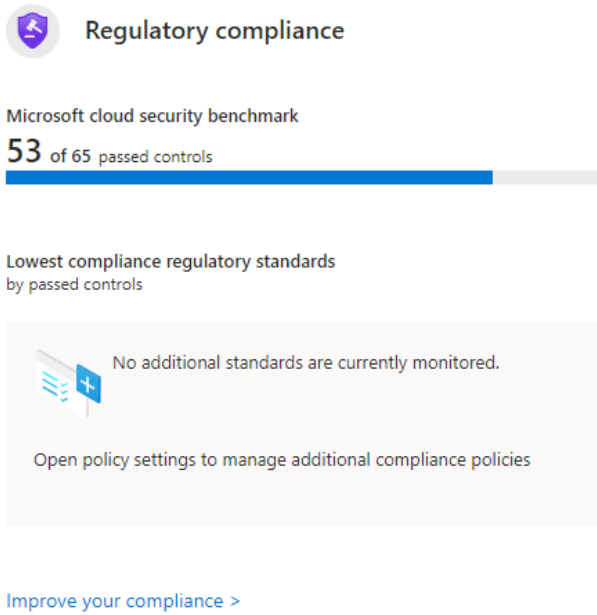
Craig Forshaw

- Cloud Architect at Atea
- Working with Microsoft Cloud technologies since 2014
- Organiser: Microsoft Security User Group
- Blog: Medium

What we will talk about

Not Azure DevOps...

Azure Regulatory Compliance for DevOps Security



Compliance in the infrastructure as code (IaC) matrix

How do we govern what is being actually being deployed to our environments?

- Blue pill – assume all is ok?
- Red pill – go down the rabbit hole. Investigate, establish governance policies and remediation actions that can be used to protect our cloud environments

Typical compliance challenges with DevOps Security in the cloud

Configuration vulnerabilities	Configuration drift	Security control enforcement	Validating compliance	Documenting and tracing
• IaC Templates • Hardcoding sensitive information • Missing security related components or features	• State storage encryption • State divergence • Out of band changes • Code analysis	• Evolving landscape • Incident response and recovery • Responsibility for remediation	• Assigning compliance remediation tasks • Measuring success • Compliance automation	• Implemeting logging and tracking of changes • Reporting challenges

Microsoft Compliance Frameworks for DevOps

Cloud Adoption Framework	Microsoft Security Development lifecycle (SDL)
• Security strategy • Microsoft Cybersecurity reference architecture • Microsoft Cloud security benchmark	• Guidelines and practices for security in the development lifecycle

Microsoft Cloud Security Benchmark

- Best practice recommendations to improve security of workloads, data, and services on Azure
- Covers multi-cloud environments
  - AWS guidance
  - GCP guidance
- Part of Defender for Cloud CSPM licence ‘security governance’
- Includes Purview integration

- MCSB Controls (v1)
  - Network
  - Identity management
  - Privileged access
  - Data protection
  - Asset management
  - Logging and threat detection
  - Incident response
  - Posture and vulnerability management
  - Endpoint security
  - Backup and recovery
  - **DevOps Security**
  - Governance and strategy

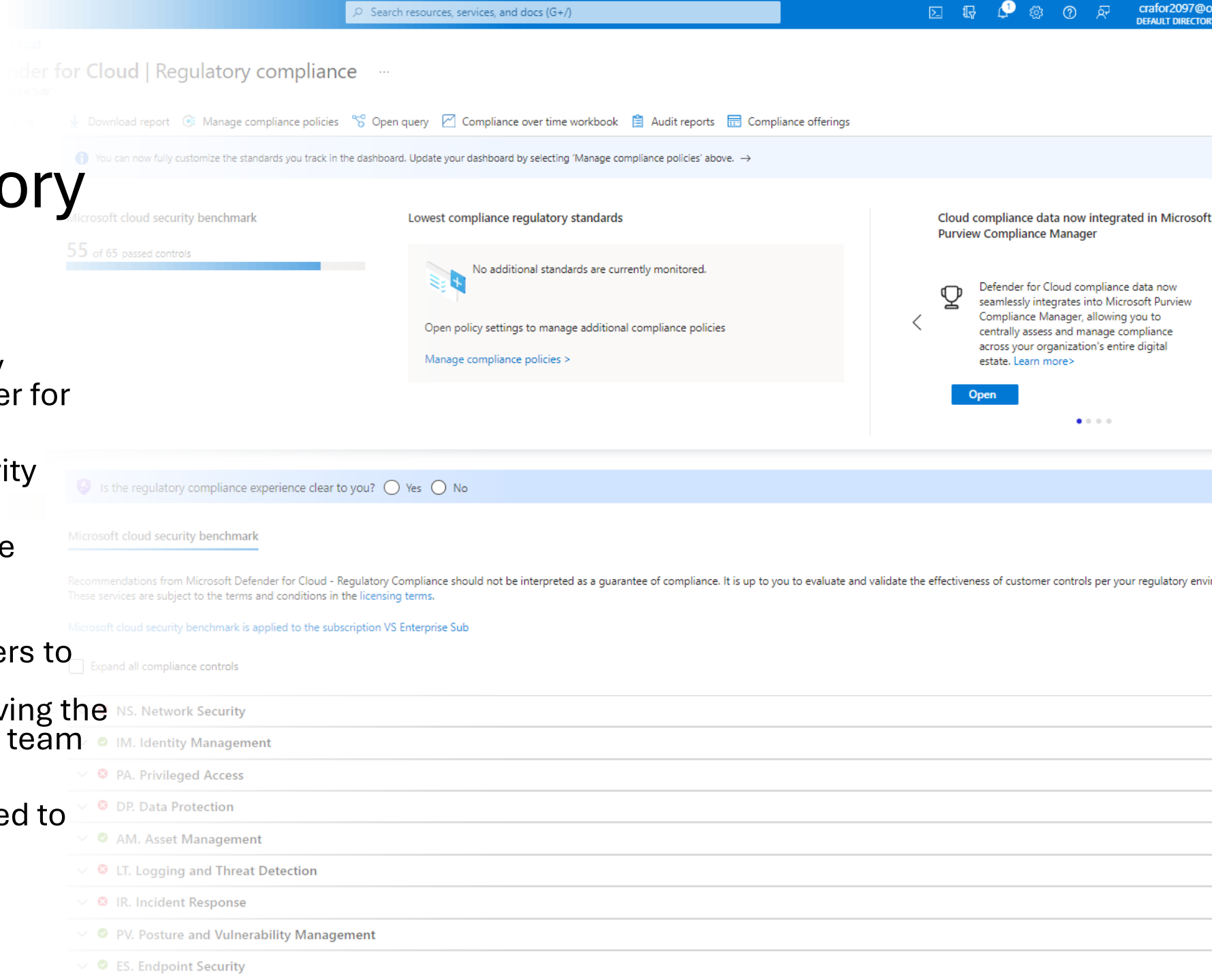
Defender for Cloud Security control: DevOps security

Security control
DS-1: Conduct threat modeling
DS-2: Ensure software supply chain security
DS-3: Secure DevOps infrastructure
DS-4: Integrate static application security testing into DevOps pipeline
DS-5: Integrate dynamic application security testing into DevOps pipeline
DS-6: Enforce security of workload throughout DevOps lifecycle
DS-7: Enable logging and monitoring in DevOps

Microsoft cloud security benchmark - DevOps Security | Microsoft Learn

Defender for Cloud regulatory compliance

- Dashboard for regulatory compliance is in Defender for Cloud
- Includes the cloud security benchmark controls
- Standardised way to drive remediation actions via governance rules
- Allows for resource owners to remediate security recommendations removing the overhead on the security team
- **Security admin role** on subscription level required to define rules



Drive remediation with governance rules

- Governance rules identify resources that require remediation according to specific recommendations or severities.
- define rules that assign an owner and a due date n on a timeframe of 7, 14, 30, or 90 days
- Can apply a grace period so that the resources given a due date don't affect the secure score.
- Owners emailed weekly

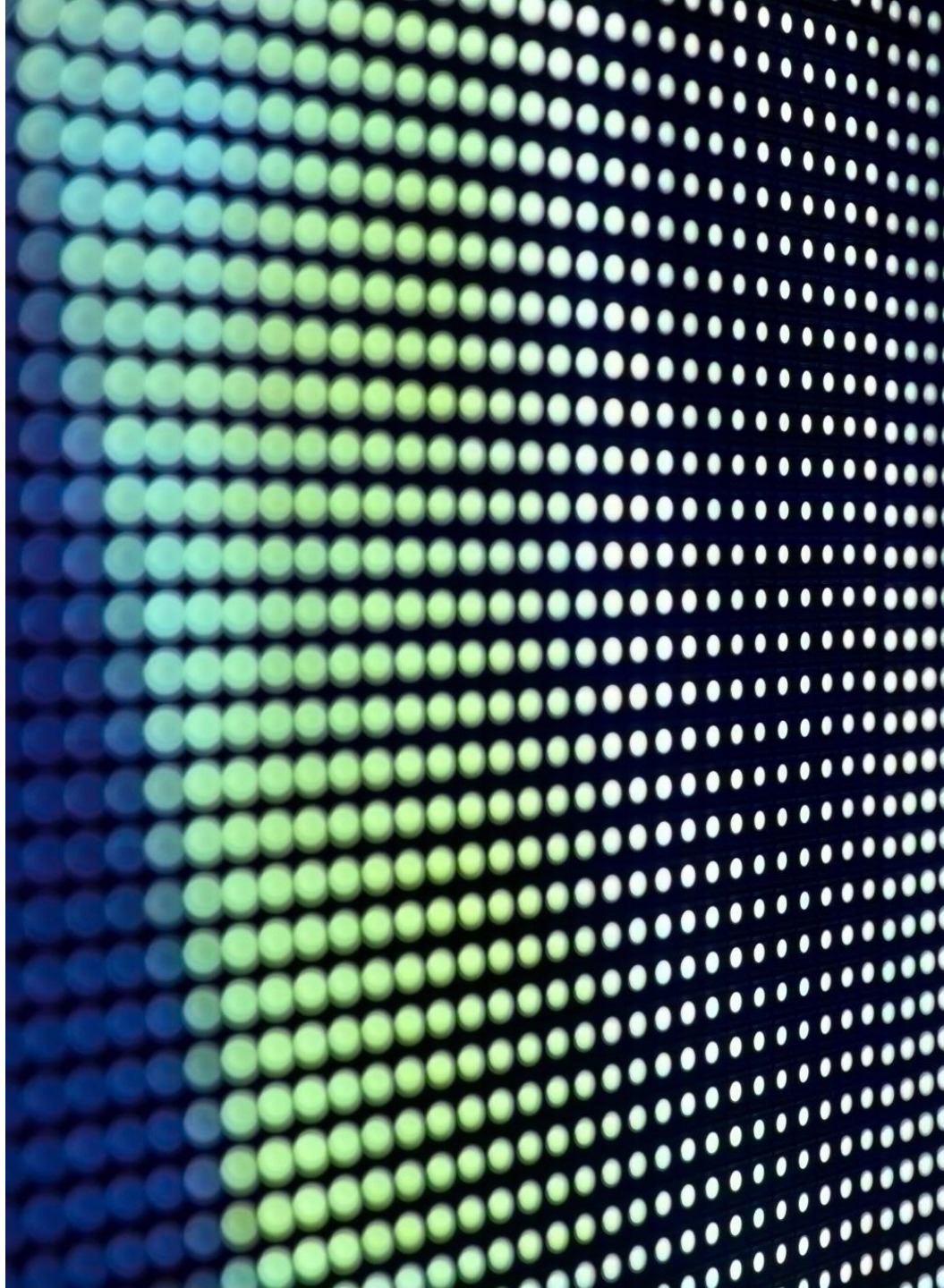
Remediate security recommendations with governance - Microsoft Defender for Cloud | Microsoft Learn

Defender for Cloud regulatory compliance

Demo

My Recommendations

Discover	Create	Implement
Discover what alerts are being generated from Defender for Cloud and where the vulnerabilities lie	Create governance rules for alerting that removes responsibility from the Security team, for example, per developer team in a subscription	Always implement alerting for high value assets Ensure governance routines actually work as intended Have a plan issue handling and isolation of vulnerabilities



Thank you!