DevSecOps To Go: Your Takeaways and To Do List

Eric Johnson, Principal Engineer
Puma Security
ejohnson@pumasecurity.io
@emjohn20
"The tools we built to do a great job at security, do a terrible job at continuous delivery....pipeline platforms are going to dominate innovation in security for the next decade."
Art of Automation: Creating A Serverless Threat Intel Bot
Ronald Eddings, Palo Alto

Threat intelligence stack:
1) Leverage the serverless framework to detect and respond in real-time
2) Automate everything
3) Bring threat intel to the tools already being used by the business
Serverless DevOps: Owning Security
Tal Melamed, Protego Labs

1) Learn the new attack surface
2) Inventory & evaluate function execution policies closely
A DevOps Approach to Security Controls
Ken Hartman, Security Consultant

1) Leverage version control automation to enforce policies
2) Prevent configuration drift using policy as code
Lunch Keynote
Shannon Lietz, Intuit

1) Phase 1 – Reversing Polarity
2) Phase 2 – Learning Storm
3) Phase 3 – Settling into a Groove
4) Phase 4 – Are we there yet?
5) Phase 5 – So now what?
Loose Keys Bring These: Attackers + Me
Jonathon Polling, Secureworks

1) Use a deny all policy for compromised tokens issued prior to detection
2) Figure out your secrets management strategy
3) Billing alerts in ALL regions
4) Monitor high risk actions (stop logging) for invocations
Embedding Security and Privacy in the World of DevOps
Aditya Sood, Symantec

1) Treat your DevOps (Git, CI / CD / CM) systems as high risk production systems
2) Exposing lower level cloud accounts (dev, qa, staging) to the Internet is BAD!
Developing Microsegmentation for Container Environment Networks
Thomas Keiser, Edgewise

1) Containerized environments greatly complicate network traffic rules
2) Traditional firewalls, IDS, IPS devices do not have enough visibility to manage container networks
Infrastructure as Code is Real!
Shaun McCullough, Software Engineer

1) Use Infrastructure as Code (IaC) for consistency, and repeatability across environments

2) Move IaC into version control to leverage git hooks, LINT checks, SAST scans against the infrastructure
Adding Continuous Compliance to CI/CD Pipelines

Eric Gerling, Trility Consulting

1) Build Cloud integration and functional tests using Kitchen or InSpec for achieving full compliance as code coverage

2) Automate compliance as code scans using Jenkinsfile + sh commands:
Components of Zero Trust:
1) Processes that store / process customer data
2) Endpoint devices, mobile, laptops, etc.
3) Backend infrastructure that does not store / process customer data
DevSecOps and the Cloud: An Organizational Primer
Tim Anderson, AWS Security

1) 70% of Cloud & DevSecOps challenges are non-technical

2) If security has to say not to parts of the business, we have failed
CloudSec Rules Everything Around Me
Kyle Dickinson, Koch Industries

1) Think about your logging strategy early and often.

2) Transform how Security is perceived, or watch out for Shadow Cloud Accounts!
Continuous Security Buddy – OpenShift, K8s, OpenStack
Mahesh Bang, Cisco Systems

1) Leverage Hackathons to find development advocates in the organization

2) Make security easy – playbooks for vulnerabilities with remediation steps
Get Off Your Buts and Move Your Apps
Christina Morillo & Ricky Pullan, Microsoft

1) Stop the bleeding. Eliminating legacy apps can simplify the portfolio and make it more secure

2) Leverage paved road libraries to modernize your app and auth portfolios
Managing Security
Vulnerabilities in the Cloud
David Hazar, HazarDSec

1) Use the Cloud to eliminate the on-prem vulnerability management headaches

2) Don't get comfortable, your program is going to need to be more agile in the cloud
In Summary
Eric Johnson, Puma Security

1) Culture is key. No journey is the same.

2) Security learns to code.

3) Leverage CI / CD automation to close your vulnerability windows.
Thank You For Attending!

Presentations are being posted at

sans.org/summit-archives