Stand Up Straight

- Security Posture And You
Please Join Me For A Stretch

- Standing is optional
- Always take care of yourself
- Always remember to breathe

"Juvenile Burrowing Owl stretching"
https://www.onthewingphotography.com/wings/portfolio-items/juvenile-burrowing-owl-stretching/
Hi. I’m Dwayne.

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of [The Security Repo Podcast](https://www.thesecurityrepopodcast.com)
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!
About GitGuardian

GitGuardian is the code security platform for the DevOps generation.

We help enterprises answer the issue of "Where are my hardcoded secrets and have they been leaked?"
Poll

Who here works on a security team?
Poll

How many people here work to improve security inside your code, deployments, and organization?
Who knows exactly what you should work on next to improve security the most?
What Should I do Next?
What Should I do Next?
What Should I do Next?
What Should I do Next?
What Should I do Next?
Security Posture Management Can Help You Answer "What Should I Do Next?"

Fog of war
Security Posture Management

- Priorities - What should I work on next?
- Risk - Which incidents would be the most expensive?
- In-Context Data - How do I know I need to fix that?
- Remediation - How should I fix it?
The Big 4 SPM Categories
(According to Gartner)

CSPM = Cloud
SSPM = SaaS
DSPM = Data
ASPM = Application
History of the Posture Management World (According to Gartner)

ASOC  CSPM  DSPM  ASPM
CNAPP  SSPM  
DLP  
SSCP  

2019  2022  2023  202X - ????
Areas Of Concern

On Prem Servers
- Application
  - DATA

Cloud Services
- Application
  - DATA

SaaS Tool
- DATA
- DATA

USERS
- USERS
- USERS
CSPM = Cloud

On Prem Servers

Cloud Services

SaaS Tool

On Prem Servers

Application

DATA

APPLICATION

SaaS APPLICATION

DATA

DATA

USERS

USERS

USERS
CSPM

Cloud Security Posture Management

Cares about:
- Anomalous clients/traffic
- Unencrypted S3 buckets
- Suspicious OS processes
- Cloud Misconfigurations
- OS Vulnerabilities
- IAM/ROLE/Permission changes
- Cloud API/Service usage

On services like:
- AWS: EC2, RDS, S3, Lambda, CloudFront
- Or Azure: Azure VMs, SQL DB, Blob Storage, Functions

Note: I am lumping Kubernetes Security Posture Management (KSPM) in with CSPM
CSPM
Cloud Security Posture Management

Example Vendors:

- Prisma
- CrowdStrike
- Wiz
- Sysdig
- PingSafe
- Orca Security
SSPM = SaaS
SSPM
SaaS
Security Posture Management

Cares about:
- SaaS Misconfigurations
- Anomalous clients/traffic
- User Devices
- User Permissions
- Third party access
- SaaS to SaaS connections
- IAM changes
- Cloud API/Service usage
- SaaS vulns

On services like:
- Salesforce
- Hubspot
- Figma
- Canva
- Google Suite
- Office365
- Confluence
- Jira
- Box
- Slack
- Asana
- Trello

@mcdwayne
SSPM

SaaS

Security

Posture

Management

Example Vendors:

- Netskope
- Obsidian
- Cynet
- Adaptive Shield
- AppOmni
DSPM = Data
DSPM

Data Security Posture Management

Cares about:
- Data Discovery
- Visibility of Data
- Data movement
- Saas to SaaS connections
- Regulatory Compliance
- Wrong type of data
- Too much data shared
- Third party access
- MFA
- Device access

On services like:
- NAS
- Local DBs
- Private cloud
- AWS
- GCP
- Azure
- Salesforce
- Hubspot
- Google Suite
- Office365
- Confluence
- Jira
- Slack
- Asana
DSPM
Data Security Posture Management

Example Vendors:
- Varonis
- Symmetry Systems
- Securiti
- Laminar
- Dig Security
- Cyera
ASPM = SaaS
ASPM
Application Security Posture Management

Cares about:
- Hardcoded secrets
- Unauthed APIs
- Unencrypted data flows
- App Misconfig
- App CVEs
- PII Data Leakage
- OSS/Code Vulns

On services like:
- WebApps
- DBs
- Message brokers
- Directory services
- 3rd party apps
- NAS
ASPM
Application Security Posture Management

Example Vendors:
- ArmorCode
- Defect Dojo
- Bionic (A CrowdStrike Company)
- Arnica
- Kondukto
How to measure your security posture?

Measuring Security == Measuring Risk
Measuring Risk

Risks are NOT threats.
Risks are NOT vulns.
Risks are NOT exploits.

Risks are what you are set to lose if things go bad.

– Walt Powell - Field CISO, CDW
Measuring Risk

Security Risk = Threat \times \cancel{\text{Exploitability}} \times \cancel{\text{Exploitability}}

Criticality

- Where am I vulnerable?
- What is the likelihood of a successful attack?
- What would it cost the company or you?
"Risk" means very different things to different parts of the organization. Beyond just security risk, business face:

- Business risk
- Compliance risk
- Operational risk
- Financial risk
- Investor risk
- Strategic risk
- Human risk
- Legal risk
Business Risks != Technical Risk

"The Board does not know or care what a CVE is. They care that something is going to make them lose money. Period."

– again, thank you to Walt Powell - Field CISO, CDW
SLIM GOODBODY

DESKERCISE

INCLUDES THE COMPLETE 35 PROGRAM SERIES!
Which holds the largest risk for your company?

1. Your cloud hosted logging platform has been compromised.

2. New OpenSSL vulnerability announced, high severity m ironically only affects latest patched version.

3. Your endpoint security product is suffering an outage can only be mitigated by disabling the security product for some time.

4. A security researcher disclosed finding Jenkins credentials for your testing environments in a pastebin dump.
Risk Impact Analysis

Comparing known risks to determine priority of remediation efforts.
Risk Impact Analysis Are Based On:

FACTS
SPM Tools Aggregate:

- SAST
- DAST
- SCA
- IAST
- Secrets Scanning
- IaC Scanning
- Network Monitoring
- Endpoint Security
- Test-Coverage Analyzers
- And more...depending on the solution
Scanners: Two Schools Of Thought
Option 1: Use the scanners you already use
Option 2:
Use scanners built into your SPM tool
Option 3:
Bad Data = A Bad Time

- False Positives
- False Negatives
- "Too many hops"
- Alert overload
- Looking for the wrong things
Remediation Effort

Risk

= LIkelihood Of Fixing
What is the best posture?

It depends...
Measuring Security == Measuring Risk

Risks are what you are set to lose if things go bad.
Security Posture Management

- Priorities - What should I work on next?
- Risk - Which incidents would be the most expensive?
- In-Context Data - How do I know I need to fix that?
- Remediation - How should I fix it?
Hi. I’m Dwayne.

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

Dwayne McDaniels
Stand Up Straight

- Security Posture And You