what sucks in security?

october 2024
maya kaczorowski

context

Maya Kaczorowski
security PM
funemployed

1. demographics
2. top security issues
3. tools
4. ML in security

demographics

who i
talked to

001

who i talked to

57 security leaders

29

~½ CISOs

25

~½ responsible for some area of security

Security Eng, SecOps, DevSecOps, Product Security, etc.

3

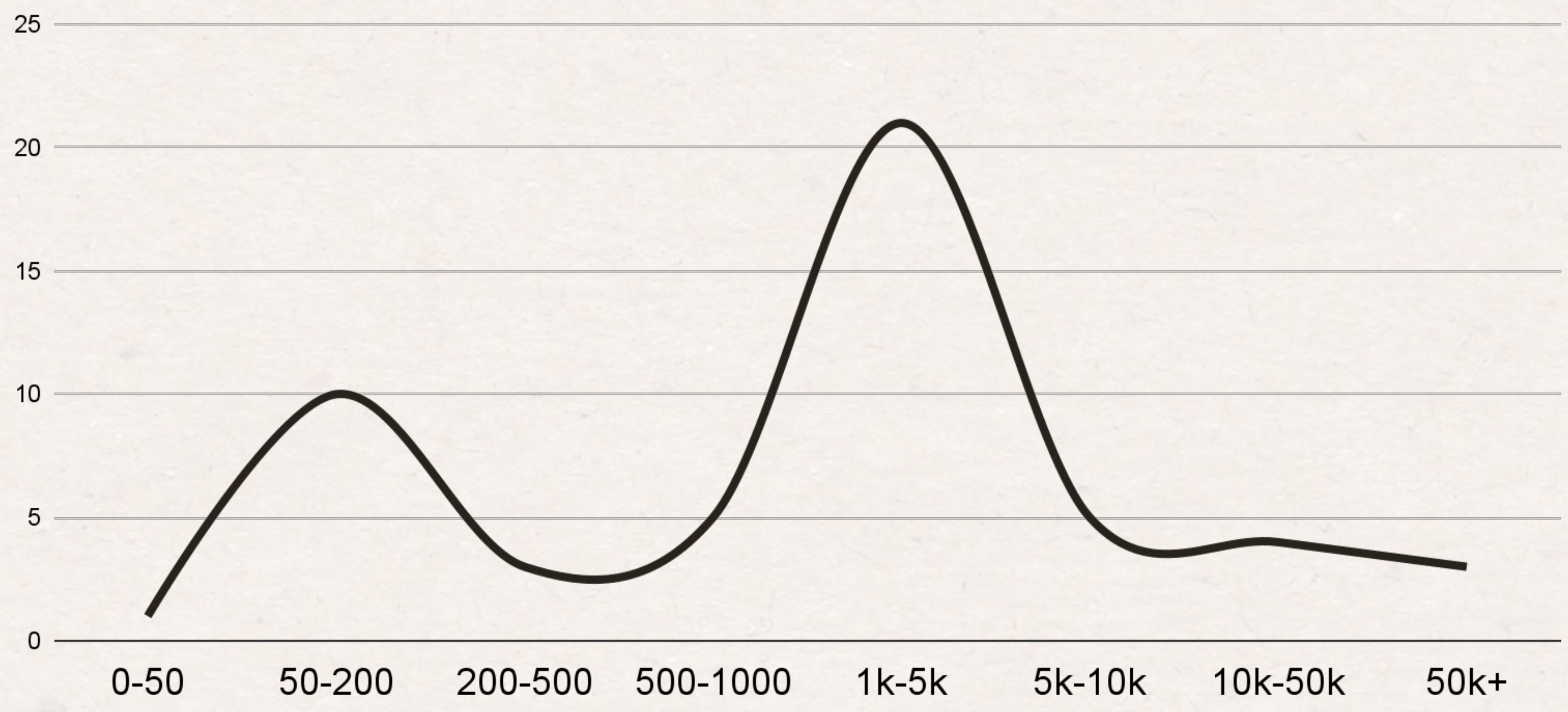
a few responsible for more than just security

CTO, VP Eng, CEO

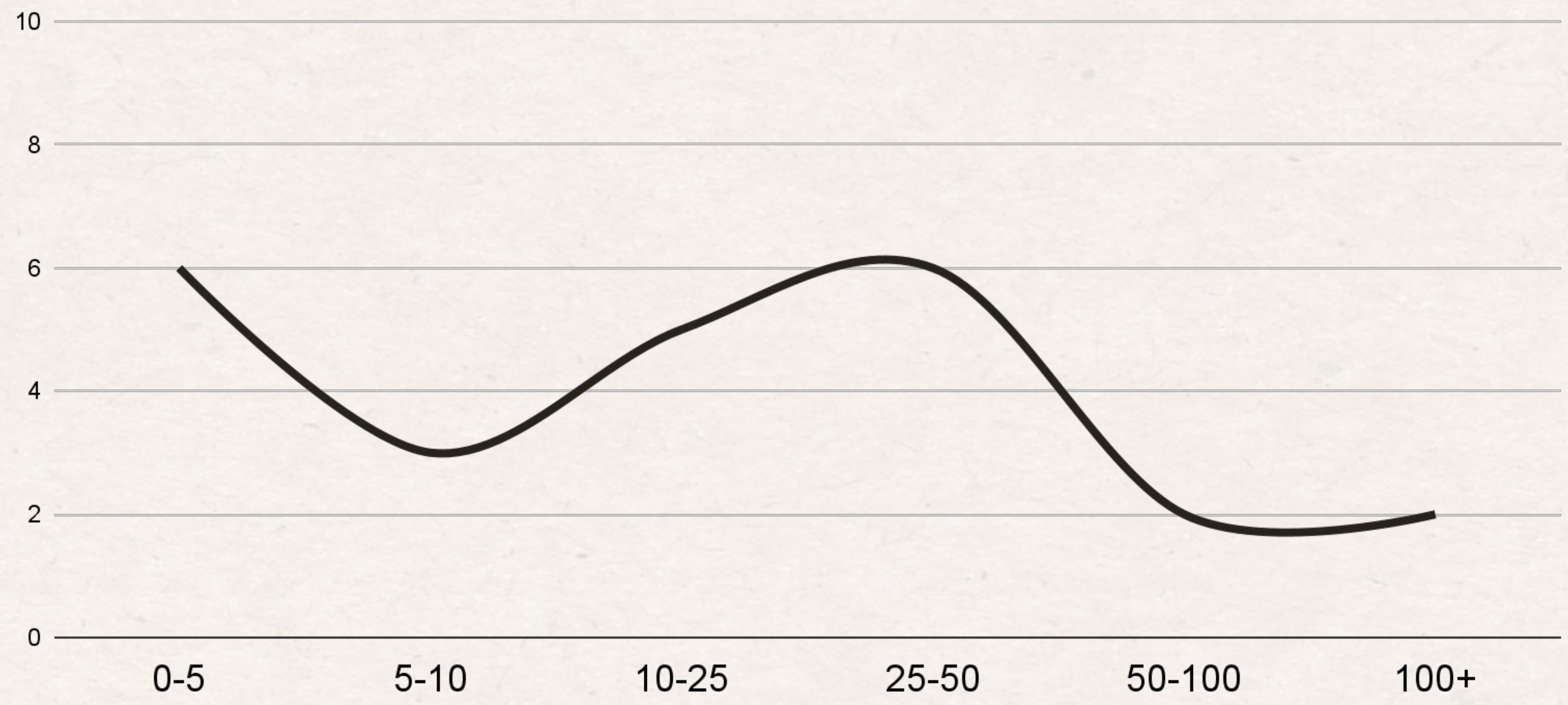
typical participant

CISO or security lead at a tech-forward company with 500-5000 employees in the United States

company + team size



number of employees



size of security team

from 30 to 240k employees, with

1525 median employees

from 1 to 300* security team employees, with

14* median security team

what i asked

- **Role**
  What is your role?
- **Company + team**
  How big is your company? How big is your security team? What is your security team responsible for? How much of your security team code?
- **Infra stack**
  What is your infrastructure on? What is your 'security infrastructure stack'? i.e. what security tools are you using?
- **Priorities**
  What are your security priorities? What's on your roadmap next year? Do you have any business mandates you need to support?
- **Eng projects**
  What are you building internally, because you can't buy?

but mostly, I asked people a very simple question

what sucks in security right now?

top security issues

what sucks
in security

002

vendor risk analysis
data classification
end user auth
secure web IDE
log ingestion
genAI governance
device compliance
data access
ownership
team morale
SBOMs
too many vendors
shadow IT/engineering
awareness training
political will
cloud security
secret mgmt
genAI
isolation
SaaS logs
customer audit logs
AI/ML
exploitabiilty
debugging Okta
identity governance
service to service auth
effectiveness
software supply chain security
communicating risk
asset mgmt
MDM
genAI code / IP concerns
sprawling identity
service catalog
vuln mgmt
RBAC
shifting left
ethical AI
availability
rolling out MDM to remote team
third party risk
secret rotation
siem costs
incident response
security posture
support tooling
no single pane of glass
dependency mgmt
EDR
zero trust
anti-abuse
IAM
tool sprawl
security data platform
SaaS app security
detection corpus
access mgmt
working with IT
model exfiltration
machine attestation
compliance
appsec
identity
vendors
cyber resilience
access control
password reset
third party review
design review
multi-party authorization
insider threat detection
risk prioritization
data governance
fixing vulns
group mgmt
verifying and demonstrating efficacy
privacy for AI
data security
support logs
business process inventory
HIPAA compliance
limited resources
vendor security
cloud guardrails
geopolitical risk
access approvals

top issues

access management

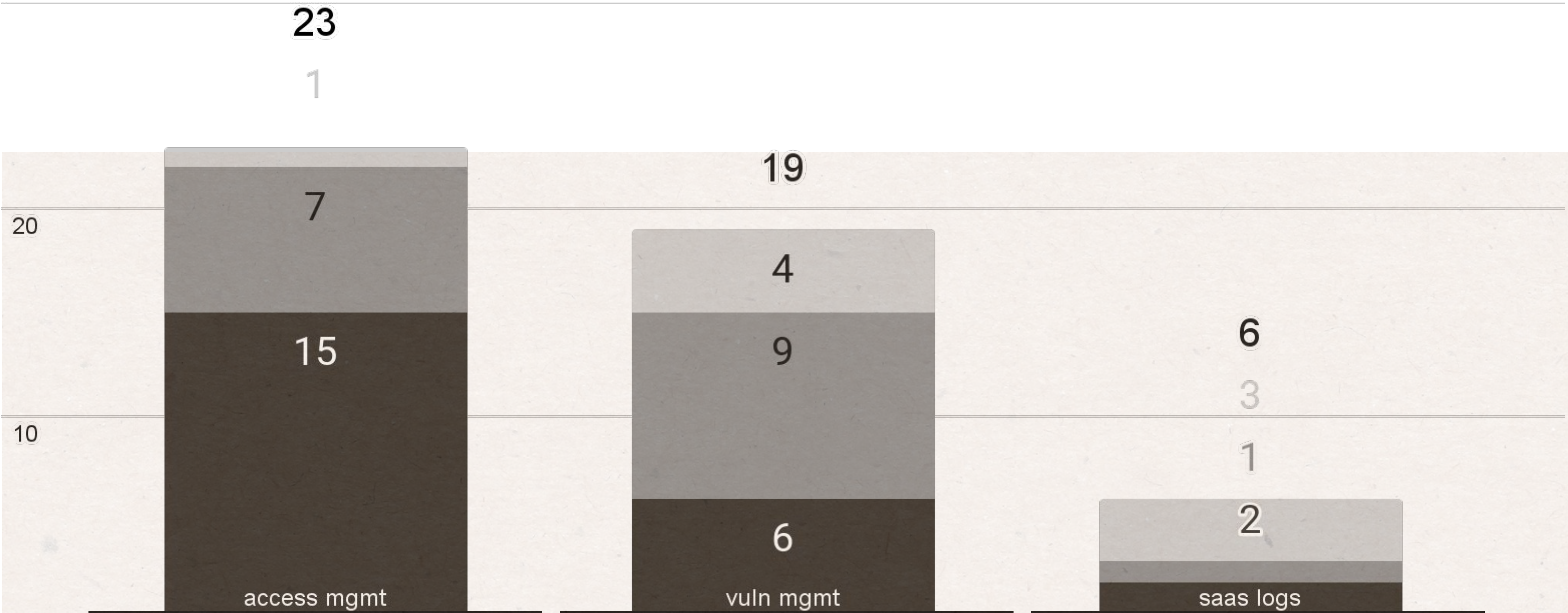
I can't provision appropriately scoped access, and so my team is overloaded with access request tickets.

vulnerability management

I have too many vulnerabilities to patch, so I need to prioritize these and ensure they are handled appropriately.

SaaS logs

When there's an incident, I can't easily pull the logs I need to find out what happened in my SaaS environments.



access management

vulnerability management

SaaS logs

access management

I can't provision appropriately scoped access, and so my team is overloaded with access request tickets.

access is done via tickets

- Highly manual
- Requires approval
- Insufficient context

We get 700+ access tickets a month — the only reason this isn't an issue is that they're handled by external IT support

Access ticket "approval is a pressure relief valve"

organic growth of entitlements

- Don't know what access someone has / should have
- Inconsistent between individuals
- Runaway groups

"Identity is a whole mess"

"Why do we have so many unused groups?"

corp and prod are separate

- Multiple systems for granting access
- Prod is not tied to IdP
- Also have NHI, shadow IT

"You're never going to be able to centralize all of your identity in one system"

"IAM is complicated and requires big integrations" for internal apps - and you hit limitations like group sizes

vulnerability management

I have too many vulnerabilities to patch, so I need to prioritize these and ensure they are handled appropriately.

move to managed base images

- Minimal container base images + VM golden images
- Continuously redeployed VMs
- Safer languages + reduced ecosystems

I'm looking for ways to "eradicate types of vulnerability", and this lets me remove a whole bunch.

need prioritization help

- Reachability
- Business context
- Exploitability
- Not just appsec

"Reachability is a problem for me." I want to know, "is the code used anywhere at all?"

"I can't prioritize across three silos"

no workflow

- Too many scanners
- Disjoint notifications (email, GitHub, Slack)
- Need to track SLAs

"The entire lifecycle of managing vulnerabilities feels off to me"

"Because we have FedRAMP, vulnerability management is a big thing"

"We are at the point for vulnerability management that we were in 2010 with EDR"

SaaS logs

When there's an incident, I can't easily pull the logs I need to find out what happened in my SaaS environments.

~~batteries~~ logs not included

- No logs
- No free logs

"We don't have a huge SaaS fleet … [but] we do a shit ass job"

It's "not possible to do an investigation in Slack"

logs aren't standardized

- No consistent format
- Manual work to normalize and ingest logs for new tools

"A lot of SaaS solutions are not set up in a way where their logs are useful for monitoring"

"Having a common SaaS format would be tremendous"

The vendors "don't have logs like I want"

a web portal is not an api

- No streaming - available via API or web portal
- Might need to email support in case of an incident

There's "currently a ton of integration pain"

cultural complications

vendor sprawl

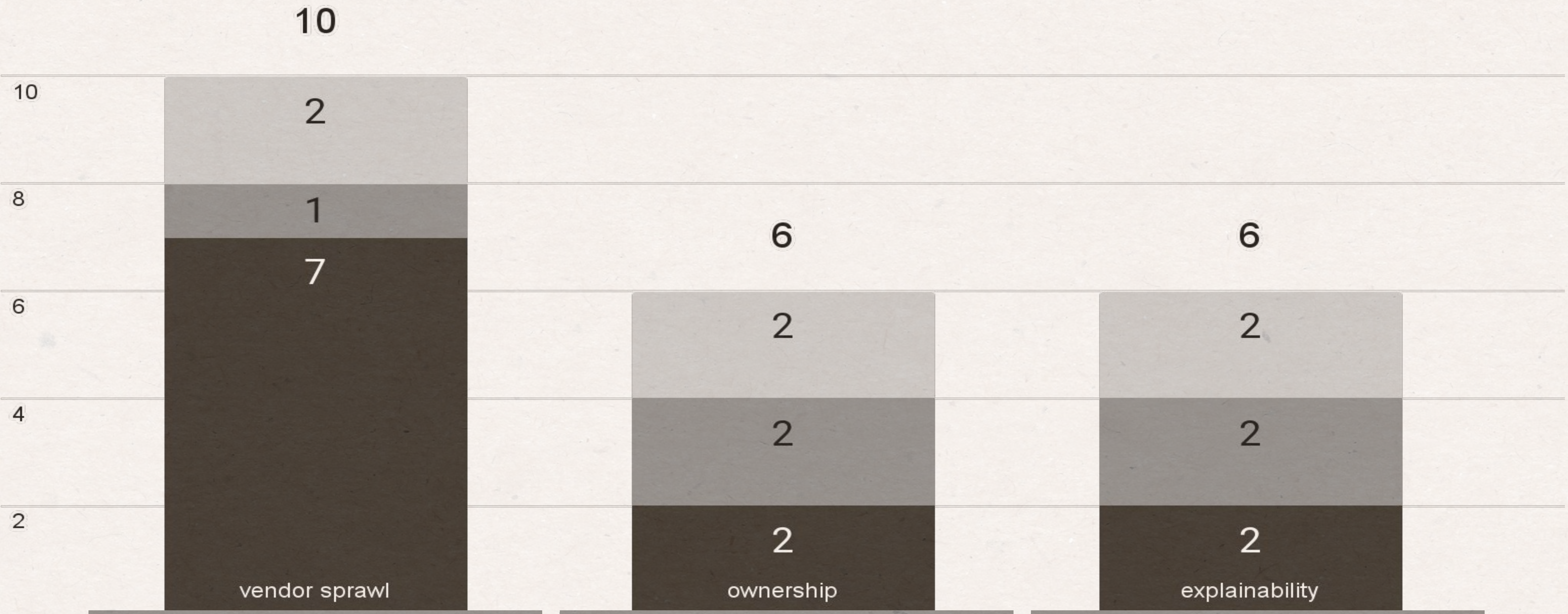
I have too many vendors, and they don’t always work well together.

ownership

I can’t keep track of who owns our ever-expanding set of services, assets, and apps.

explainability

I need to be able to communicate security risks and requirements effectively.



vendor sprawl

ownership

explainability

vendor sprawl

I have too many vendors, and they don't always work well together.

too much bullshit

- Too many similar vendors, with confusing marketing
- Incremental tools

"I fucking hate vendors"

"There's just so many vendors", I'm "inundated"

"They just keep trying to sell me stuff"

3rd party risk

- Every vendor is a new risk for my organization

"Vendor security is just a complete joke"

"I have to take on their security debt", so "in order for me to even consider a vendor... [I need] their CEO's phone"

no single pane of glass

- No single place to understand security posture
- Ad hoc reporting

"My biggest problem, bar none, is I have no single pane of glass... I just want a single place to see anything and everything"

"Everyone is doing one slice of the pie, everyone has a dashboard"

no glue

- Custom work to plug together solutions

I can't "waste time on integrating a new vendor"

"I don't want another Zapier for security logs"

ownership

I can't keep track of who owns our ever-expanding set of services, assets, and apps.

missing service catalogue

- Don't know who to ask for vuln mgmt + incidents
- Flexibility to name a group, not an individual

"One of our biggest challenges is attribution: who owns that thing?... This isn't just a security problem"

"Some systems didn't have an owner... nobody wanted to mess with them since they'd been around for so long"

incomplete asset catalogue

- Cloud resources + code
- Transition when people leave

It's "quite social and messy... more gardening than construction"

"I know a lot of people think asset management is solved", but it's still not usable — how do we roll up ownership of cloud assets?

SaaS ownership

- App management, including access management

"We have quite a few tools that don't have owners, that are scary"

explainability

I need to be able to communicate security risks and requirements effectively.

explaining risks to the board

- Missing common language

Quantifying and explaining risk is "an area of extreme importance" but very low maturity in the industry

I'm hesitant to put metrics in front of the board, and instead talk about risk generally

measuring effectiveness

- Existing tools
- New tools

"It's hard to prove you're getting what you think you're getting"

explaining effectiveness

- Being secure "enough"

This is "where I spend most of my time.. how do we demonstrate we have a good security program?"

communicating friction to the business

- Rolling out new controls
- Data / evidence

A CEO might think, "I'm worried you're adding friction to my barely profitable business"

tools

what are
you using

003

security tech stack for the 80%

cloud providers

aws 😕

Google Cloud 😕

Azure 🙁 *We thought "Microsoft would help get us into [government] markets... it has totally not happened"*

identity

okta 🙁 *"I hate Okta with all my soul... they're the Microsoft of identity"*

1Password 😊

mdm

jamf 🙁

Intune 🙁

edr

CROWDSTRIKE 😕

SentinelOne 😕

cspm

WIZ 😊 *Wiz "bailed me out"*

iac

HashiCorp Terraform 😕

observability

DATADOG 😕

data lake

snowflake 😕

fragmented tools

scanners

snyk Semgrep

VERACODE tenable sonarqube

CodeQL RAPID7

MEND Formerly WhiteSource trivy clair

Socket Dependabot

We have "a whole portfolio" of scanners

"I was very confused that every company [at Black Hat] was ASPM... they're all doing the same thing"

SIEMs

panther splunk>

sumo logic ELK

runreveal DATADOG Chronicle

"Nobody has come up with a Splunk replacement... there are a bunch of competitors, but no one seems to be able to knock them off the top of the stack"

There's "no turnkey solution available"

tools being built internally

security data lake

Operational data store for security and compliance information, e.g., on my corp and prod devices, cloud environments, etc — more than just historical SIEM logs. Used to find exceptions and verify controls and compliance.

on-demand access

Time-bound access to sensitive resources, like on-call access to prod, or support access to customer data — typically implemented by changing group membership. Some may have a more complex approval workflow.

"Unless you're a giant bank with a lot of money, I don't know how this is doable..."

vault interface

Front-end interface to HashiCorp Vault to provide an improved developer experience and restricted functionality; with pluggable back-end to multiple regional instances of Vault.

"Using Vault isn't intuitive... the tooling around it sucks"

ml in security

what about ml/ai

004

what about ml?

genAI governance

I want to ensure that only the teams who have been authorized to are using genAI, with only allowed data.

dlp

I need a better understanding of what data we are using in training, in order to prevent unauthorized data from being trained upon.

workload isolation

We need an efficient way to isolate different customers' code, models, or interactions with our model.

I just need to check, "are you using the enterprise version"

We don't want to send any data to these tools, even if the ToS says they won't use it

This is just data governance: "You need to know what you're protecting, and where it is"

"Next gen DLP doesn't really exist yet"

thank you