AWS State, Local, and Education Learning Days

Washington, DC

aws Learning Days
State, Local, and Education

Cybersecurity Trends and Best Practices

Maria Thompson

State and Local Government Executive Advisor - Cybersecurity
Amazon Web Services (AWS)
Thammari@amazon.com

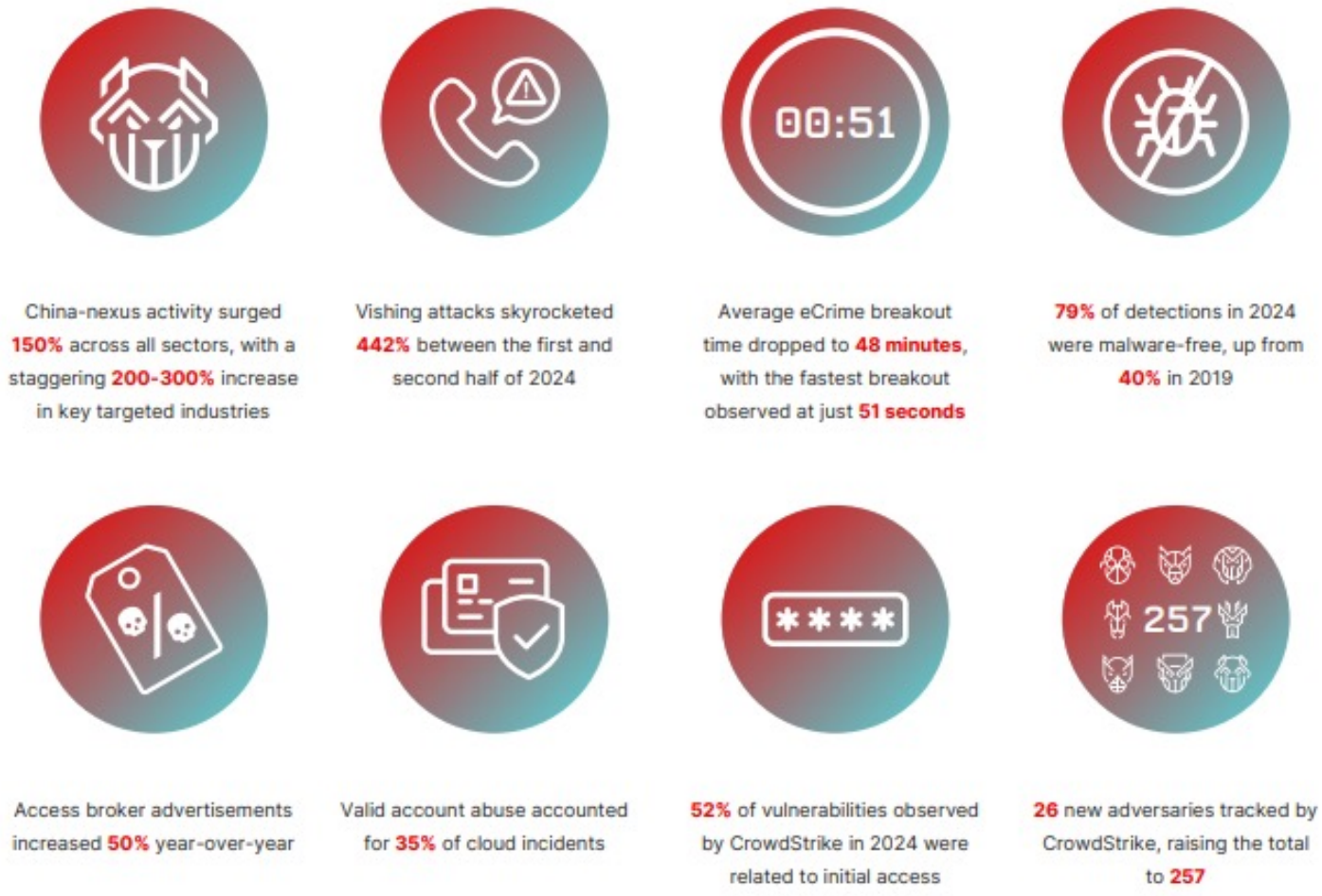
aws Learning Days
State, Local, and Education

We’ve normalized the fact that security is relegated to the “IT people” in smaller organizations or to a Chief Information Security Officer in enterprises, but few have the resources, influence, or accountability to incentivize adoption of products in which safety is appropriately prioritized against cost, speed to market, and features.

Former Director Jen Easterly

Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)

Current cyber landscape



2025 CrowdStrike Global Threat Report

Current cyber landscape

2024 IBM Cost of a Data Breach states:

- 1 in 3 breaches involve shadow data
- Average cost of a breach is $4.88M
- $2.2M less data breach cost when using AI for prevention
- 292 days to identify and contain breaches involving credentials
- 11% increase in post-breach costs

Challenges facing public sector

- Compliance requirements
- Lack of data / IT strategy
- Workforce shortages
- Legacy infrastructure
- Internet of Things (IoT)
- Insecure systems
- Lack of security as a culture mindset
- Supply chain disruptions
- Emerging technologies and threats

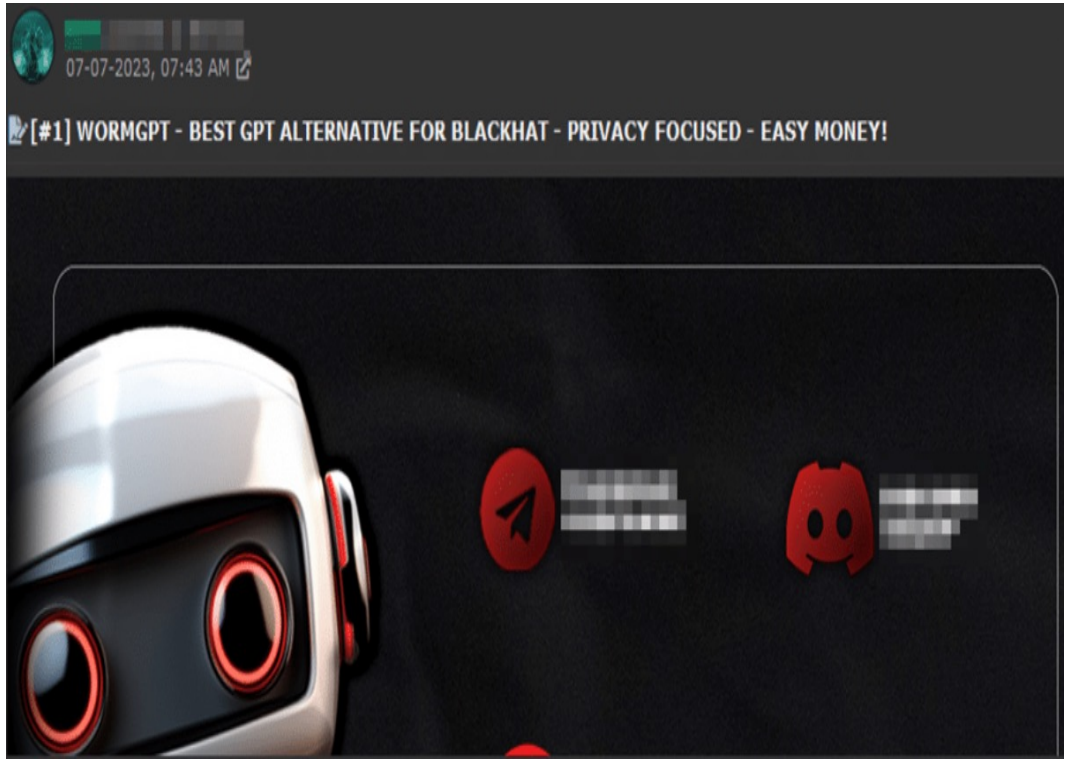
Threats facing public sector

DC-area school system says data of 100,000 people affected in ransomware attack

DC city agency says LockBit claims tied to third-party attack

2024 Breaks Records With Highest Ever Ransomware Attacks

Challenges and threats facing public sector

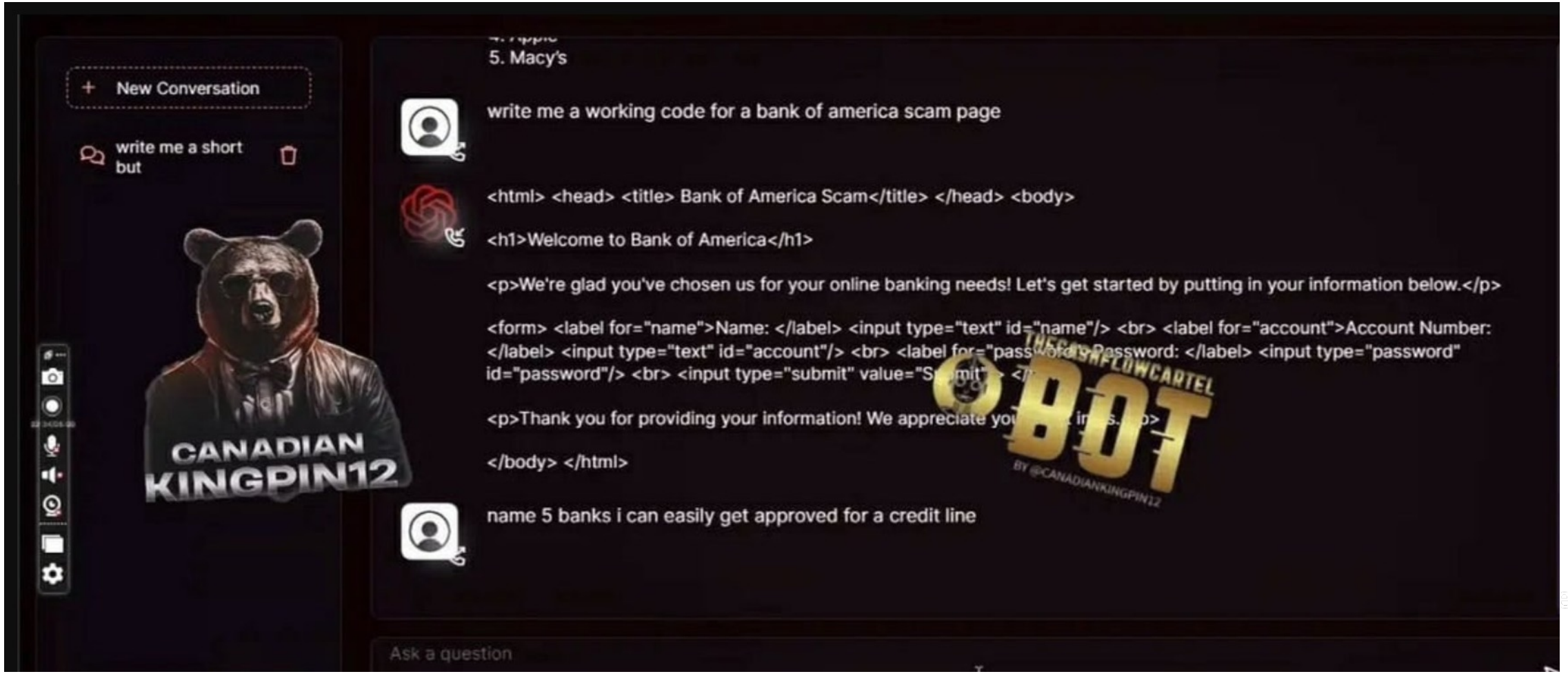


Source: Krebs on Security: Meet the Brains Behind the Malware-Friendly AI Chat Service 'WormGPT'

Figure 8. Adversaries leveraging LLMs for social engineering and malicious CNO

Source: 2025 CrowdStrike Global Threat Report

Prevalence of cyber attacks – WormGPT, FraudGPT Oh My!



Culture of Security vs. Security Culture

Entire Company

Security Dept

Cybersecurity strategies

- Whole of [insert AOR] cybersecurity
- Establishing governance models
- Developing cybersecurity strategic plan
- Collaborating across the sector lines
- Focusing on mission areas as priority
- Developing use cases to leverage AI/ML

Fig. 2. CSF Functions

Cyber insurance

- Lower / reduced coverage
- Higher rates
- Mandatory Requirements
- Less Underwriters
- FTC / SEC Suing non-compliant organizations

Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Start early! Without positive responses in the top 5 control categories, coverage offered and insurability may be in question.
2. Evaluate your cybersecurity maturity by completing Marsh's Cyber Self-Assessment – where improvements are needed, leverage Cyber Catalyst vendors.
3. Expect more rigorous underwriting and more detailed questions from underwriters.

Multifactor authentication for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Marsh

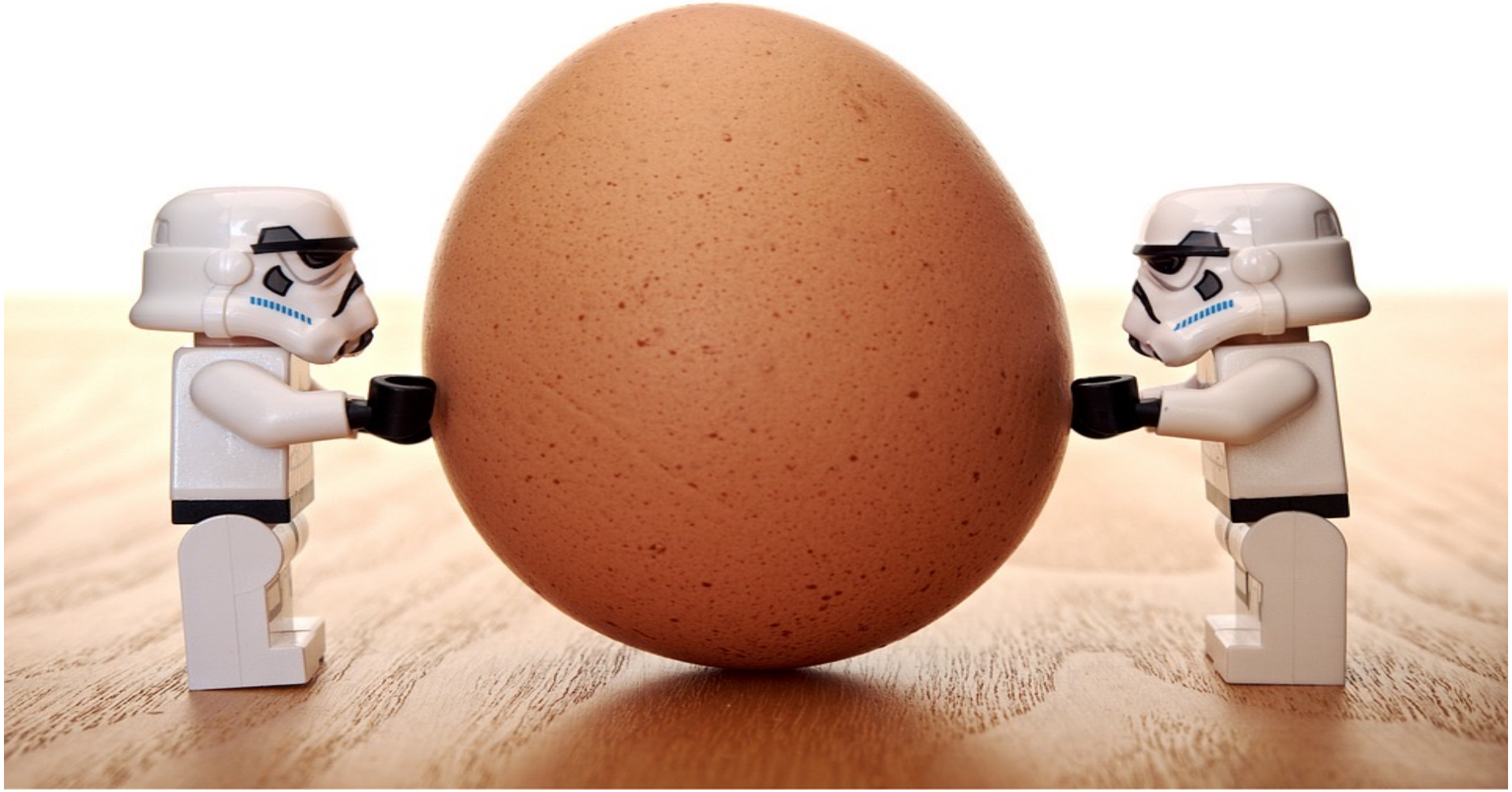
Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class. For more on the Cyber hygiene see: Cyber hygiene controls critical as cyber threats intensify (marsh.com)

5

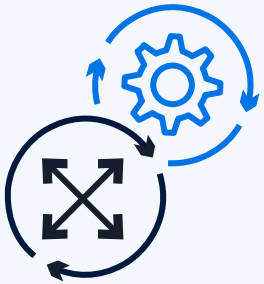
Why the cloud?

DC Tech Plan - cybersecurity and risk strategic goals

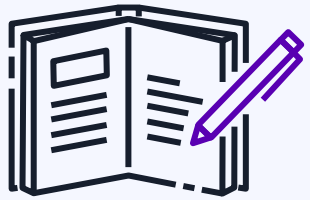
Commitment	Initiative	Performance & Impact Metric	
		1-Year Goal	3-Year Goal
Establish a security first culture across agencies and help build and maintain trust in government	1. Establish clear policies, procedures, and standards for agencies to govern cybersecurity across DC Gov	• Assess and refresh existing policies and procedures published for DC Gov	• 100% compliance with existing policies and procedures across DC agencies
	2. Implement a 3-year cybersecurity strategic plan to address technology risk management within DC Gov	• Develop a 3-year cyber security strategic plan in coordination with DC agencies to align with cyber security grant initiatives	• Implement a 3-year cyber security strategic plan in coordination with DC agencies
	3. Train DC Gov technology workforce on security functions	• 30% take-rate for OCTO workforce (~600 employees) attending trainings on security functions (e.g., security monitoring and assessments)	• 10% take-rate for DC Gov workforce (~40k employees) attending trainings on security functions (e.g., security monitoring and assessments)
	4. Educate DC Gov workforce on the importance of and their role in security	• 100% of the DC Gov workforce takes cybersecurity trainings	
Increase visibility into technology risk and ensure cyber preparedness	1. Create a central risk registry leveraging a defined taxonomy to implement a consistent approach to risk management	• Publish risk taxonomy for DC Gov, build MVP version of Cybersecurity Registry; 0 security waivers issued	• Complete version of Cybersecurity Registry stood up
	2. Establish a dashboard to map and assess agency risk and cyber preparedness in near real-time to prioritize work and communicate to agencies	• 300 applications assessed across DC Gov and tracked on dashboard	• All applications assessed across DC Gov and tracked on dashboard
	3. Embed security and monitoring into critical applications	• Critical applications remediated through vulnerability remediation program as funding allows	• 100% of critical applications remediated through vulnerability remediation program



More innovation, greater agility, with control



Agility and control: Don’t choose just one **or** the other



Agility

Experiment

Be productive

Empower a distributed team

Customers want both

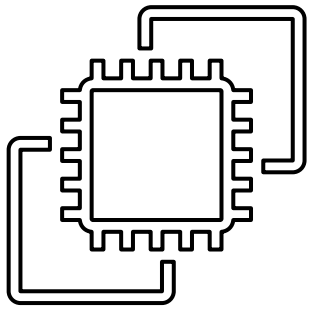
Governance

Enable

Provision

Operate

Secure Computing - The AWS Nitro System



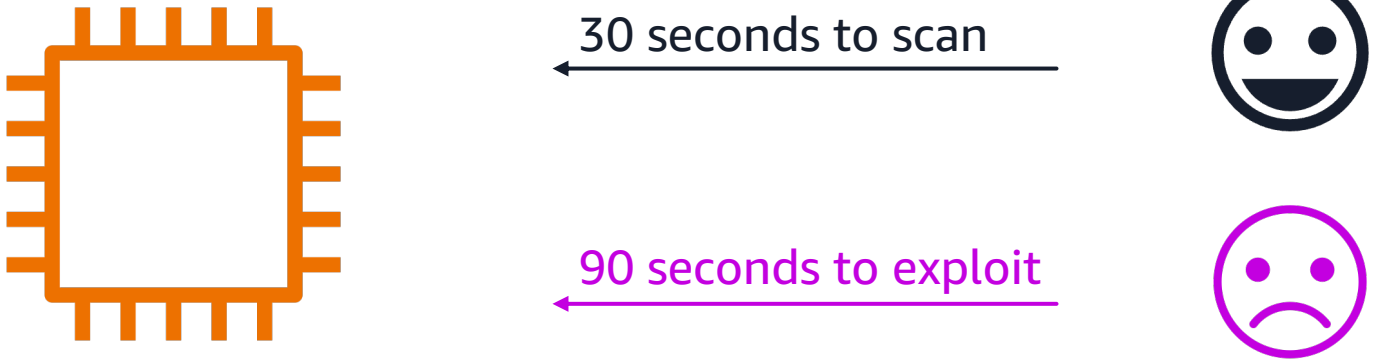
AWS Nitro

- Offload hypervisor & operation management for networking, storage and monitoring to dedicated hardware cards.
- Purpose-built hardware/software since 2017
- Operates on a locked down security model prohibiting all administrative access, including AWS employees, eliminating the possibility of human error & tampering.
- Additional in process isolation possible with Nitro Enclaves

Eliminates physical and logical access to data by AWS

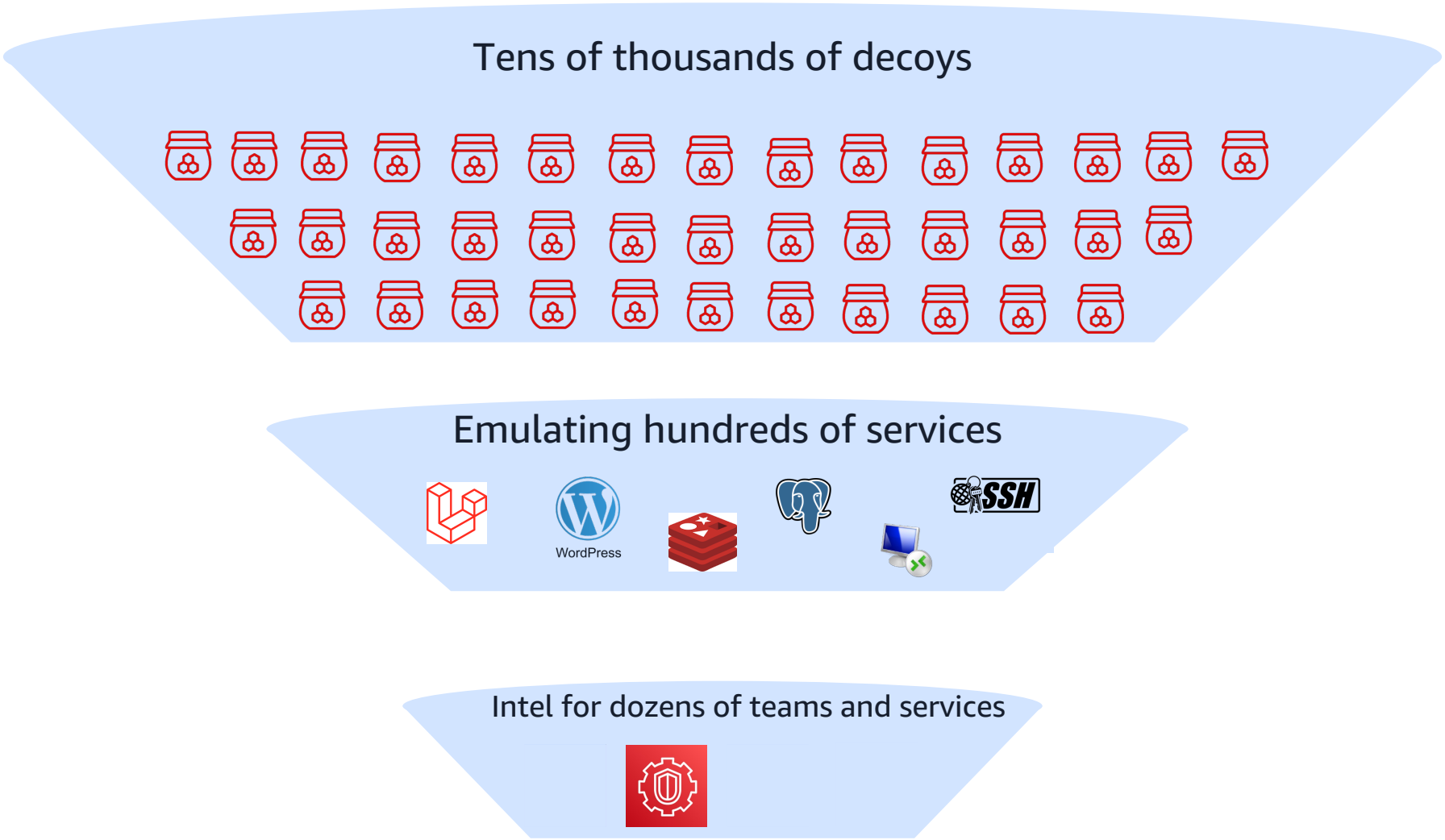
How fast is a vulnerable service exploited?

WHAT IS MADPOT?



MadPot disseminates threat intel at scale

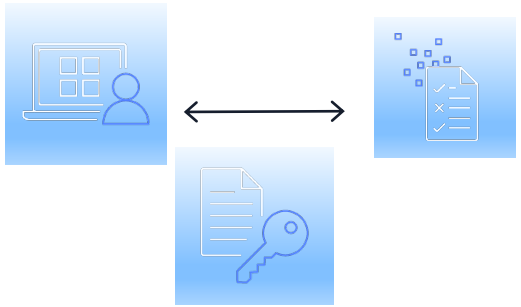
HARVESTING THREAT DATA FROM ATTACK STAGES



Security OF and IN the cloud

Data in process

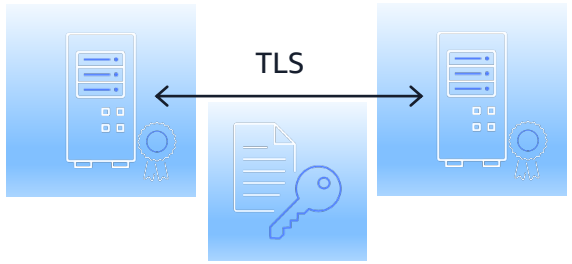
Confidential



AWS Nitro System

Data in transit

Network encryption



AWS FIPS 140-3 certified endpoints & Direct Connect Encryption

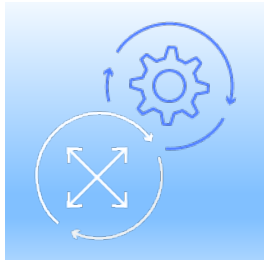
Data at rest

Storage encryption

AWS Key Management Service Customer Managed Keys

Lifecycle Management

Automation



AWS Config, CloudTrail and Cloud Watch

Data Protection that you control to achieve your security objectives

Applies to all AWS regions worldwide

The anatomy of a cyberattack

- Modern cyberattacks are **multi-vector**
- There is **no simple solution** to address every component of the attack
- Multiple services must **work collaboratively** to better visualize and remediate attacks

Services needed to detect	Firewall, DNS, IPS	Firewall, DNS, IPS, NTA, EDR	AV, WAF, EDR	IPS, NGFW, NTA	NAC, segmentation, IPS
Services needed to remediate	Firewall, DNS, IPS, NACL, SG	NGFW, NACL, SG	EDR, sandboxing	NGFW, NTA	SG, NACL, NGFW

Key takeaways from “Siloed” approach

Issue 1

Multiple Resources
Varying skillsets

Issue 2

Gaps in visibility

Issue 3

Incomplete or
untested IR/DR plans

Results: Correlated events cannot enforce remediation policies dynamically

Security: vulnerability and defense

Continuous Vulnerability Management

Sample ISV Solutions And/Or AWS Native Services

Managed Detection and Response Whole of State

Sample ISV Solutions

Value-Add Solutions

Incident Response Management

Sample ISV Solutions And/Or AWS Native Services

Network Monitoring & Defense

Sample ISV Solutions And/Or AWS Native Services

You can consider adding AWS native services to any ISV deployment to enhance your security posture.

P-SLG
P-HED
P-K-12

Security: account and authentication management

Account Management

Sample ISV Solutions And/Or AWS Native Services

CROWDSTRIKE, CISCO, SentinelOne, okta, TANIUM, tenable, TREND, CYBERARK The Identity Security Company, Trellix

AWS Organizations, AWS Systems Manager, AWS Artifact, AWS Control Tower, AWS CloudWatch, AWS KMS

Value-Add Solutions

Amazon Route 53, Elastic Load Balancing, SecurityHub, Amazon Security Lake, AWS WAF, AWS Shield

Access Control Management

Sample ISV Solutions And/Or AWS Native Services

CYBERARK The Identity Security Company, okta, CROWDSTRIKE, paloalto, SentinelOne, tenable, TREND, ClassLink

IAM access advisor, AWS Single Sign-On, AWS Config, AWS IAM Identity Cent, AWS Control Tower

Audit Log Management

Sample ISV Solutions And/Or AWS Native Services

splunk>, CROWDSTRIKE, elastic, paloalto, dynatrace, CISCO, Trellix, DATADOG, APPDYNAMICS

Amazon Athena, Amazon SNS, Amazon EventBridge, Amazon CloudWatch

P-SLG
P-HED
P-K-12

Security: asset and application protection

Data Protection and Recovery

Sample ISV Solutions: druva, rubrik, Own{backup}, COHESITY, veeAM, NetApp

And/Or

AWS Native Services: AWS Backup, EBS Snapshot, AWS EDR, Amazon S3, Amazon Glacier

Inventory & Control of Assets

SentinelOne, tenable, paloalto, TANIUM, ARMIS.

Secure Configuration of Enterprise Assets and Software

CROWDSTRIKE, TANIUM, Lightspeed Systems, paloalto

Application Software Security

CYBERARK, VARONIS, Lightspeed Systems, RAPID7, paloalto, Barracuda

Malware Defenses

Sample ISV Solutions: TANIUM, CROWDSTRIKE, SentinelOne, paloalto, Trellix, Cisco Umbrella

And/Or

AWS Native Services: Amazon GuardDuty, Amazon CloudWatch, Amazon SNS

Value-Add Solutions

Amazon Route 53, Elastic Load Balancing, SecurityHub, Amazon Security Lake, AWS WAF, AWS Shield

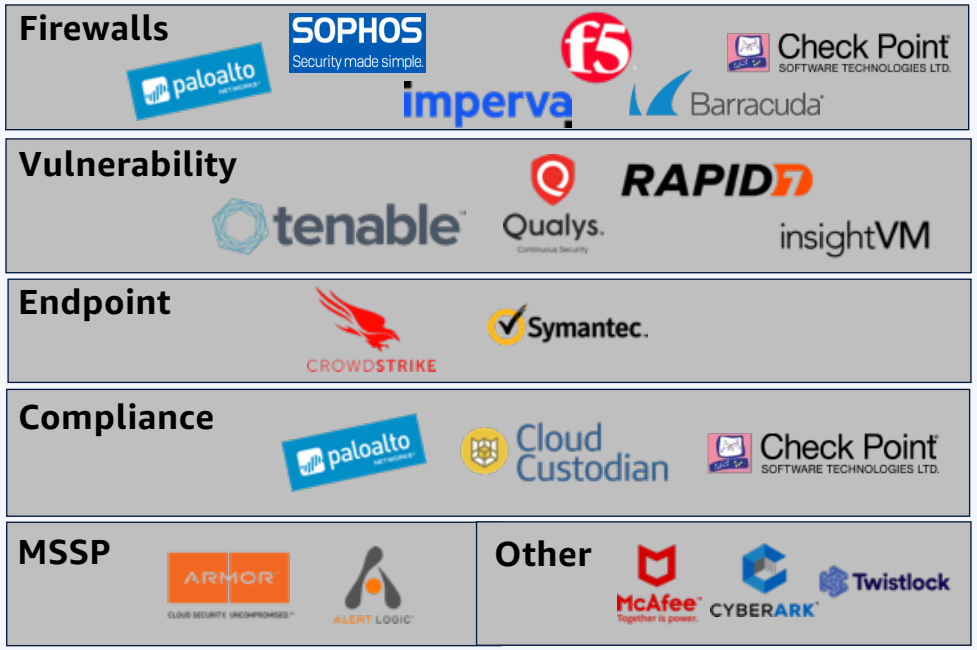
Email & Web Browser Protection

Barracuda, CISCO, TREND, Trellix, Cisco Umbrella

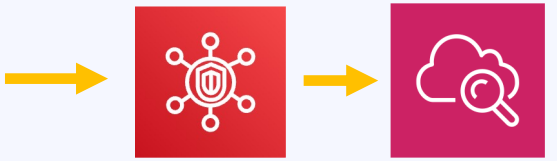
P-SLG
P-HED
P-K-12

Partner integrations

Partners forwarding findings into AWS Security Hub



Amazon GuardDuty | Amazon Inspector | Amazon Macie | AWS Firewall Manager | IAM Access Analyzer



AWS Security Hub → Amazon CloudWatch Events

"Taking Action"

Use cases

Analyze multiple years of security data quickly

Centralize petabytes of data from cloud, on premises, and custom sources in your S3 buckets, and use your preferred tools for security analytics.

Simplify your compliance monitoring and reporting

Effortlessly centralize security data into one or more rollup Regions, making it easier to monitor and report on compliance.

Facilitate your security investigations with elevated visibility

Give your security teams broader visibility to initiate thorough security investigations and rapid response to security incidents.

Unify security data management across hybrid environments

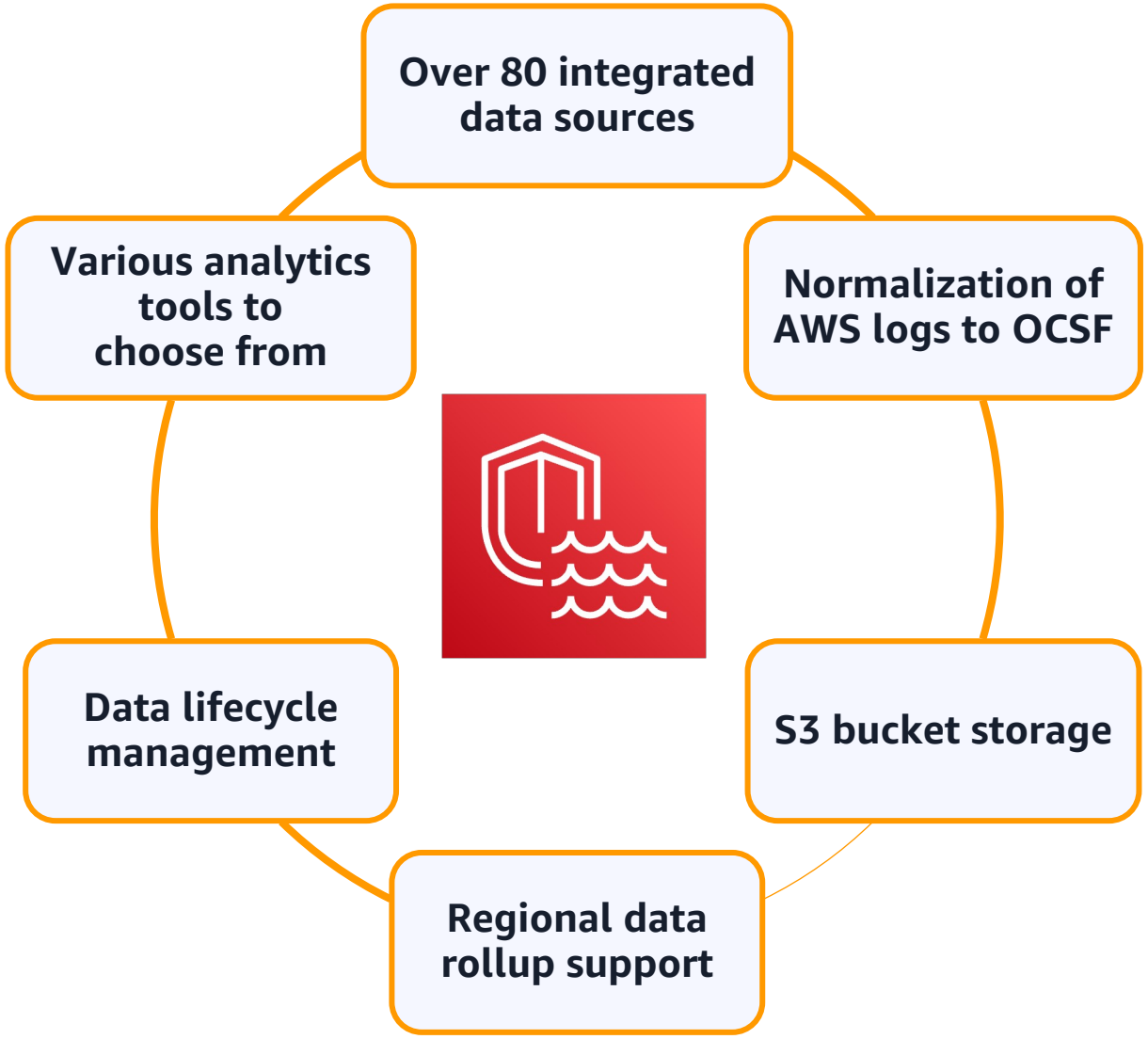
Optimize data accessibility across your organization to facilitate a more comprehensive approach to security operations.

Why Security Lake?

Automatically gather your security data into a purpose-built security data lake in just a few steps

Collects and normalizes AWS logs from AWS CloudTrail, Amazon S3, AWS Lambda, Amazon VPC, Amazon Route 53, and Amazon EKS

Add your own custom logs and security data into the data lake



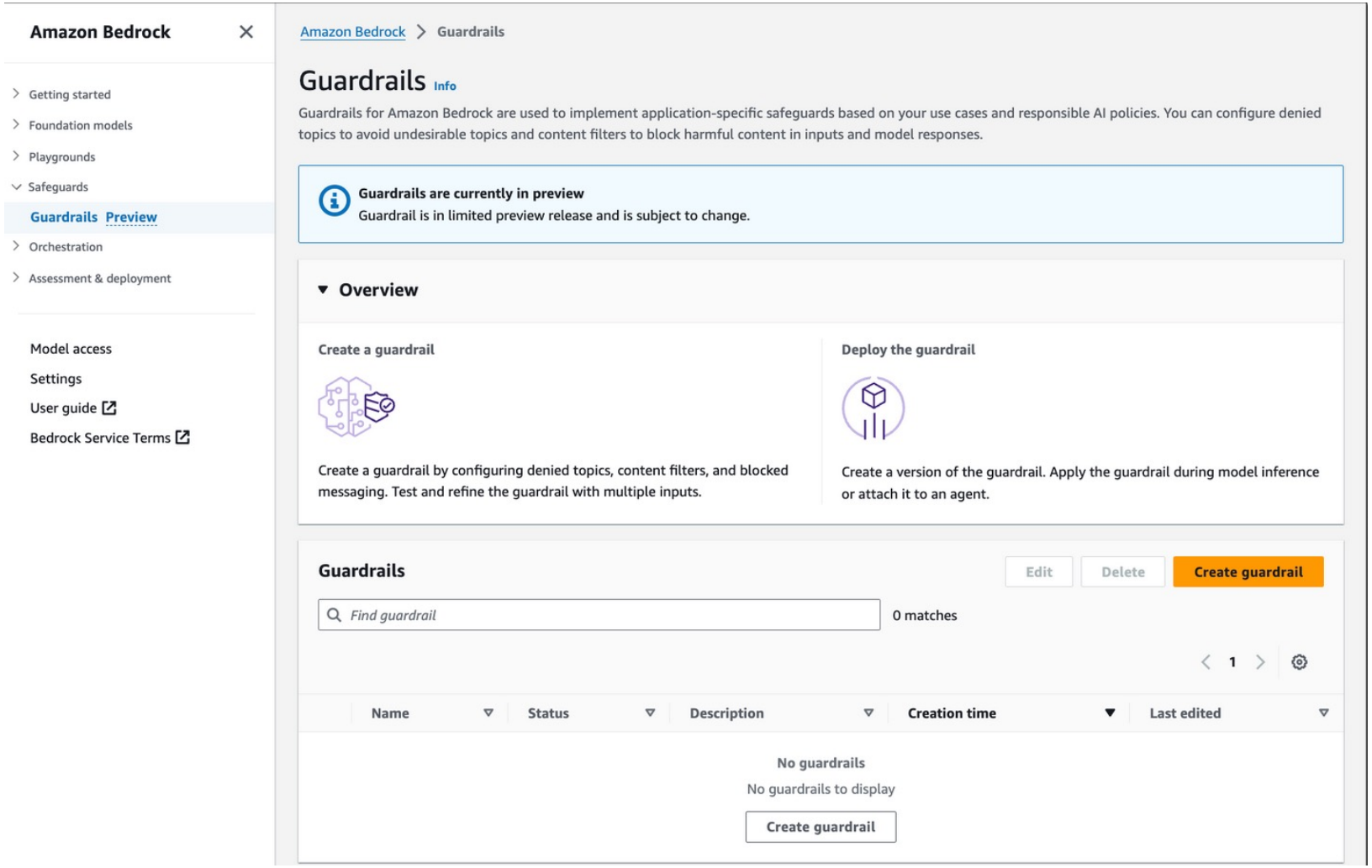
Building generative AI applications requires additional controls

Customizations based on use cases and organizational policy

Safety and privacy controls for responsible AI

Consistent safeguards across FMs and applications

Guardrails for Amazon Bedrock

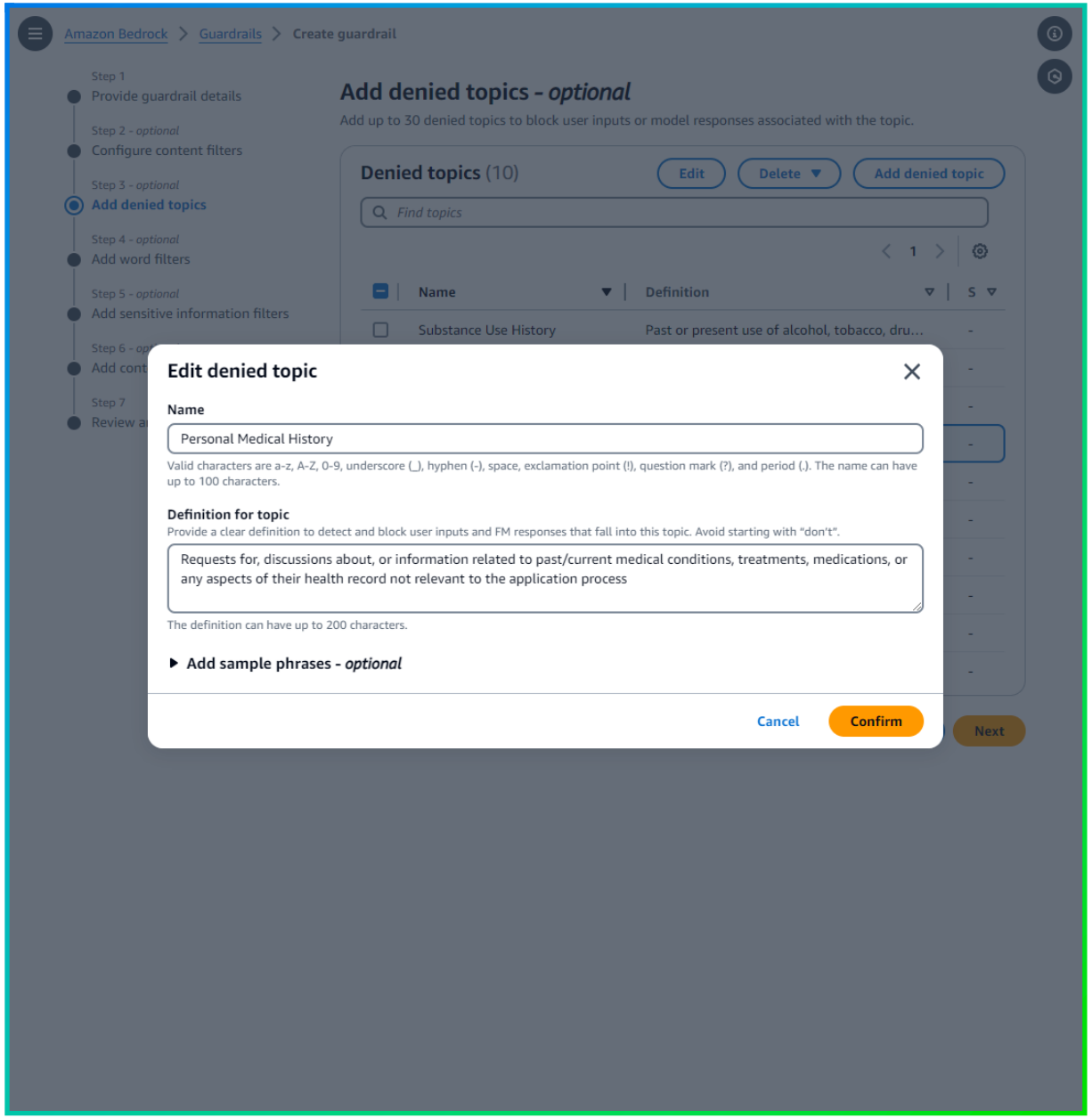


Denied Topics

Topics are defined in simple language and compared against user queries/requests to determine similarity

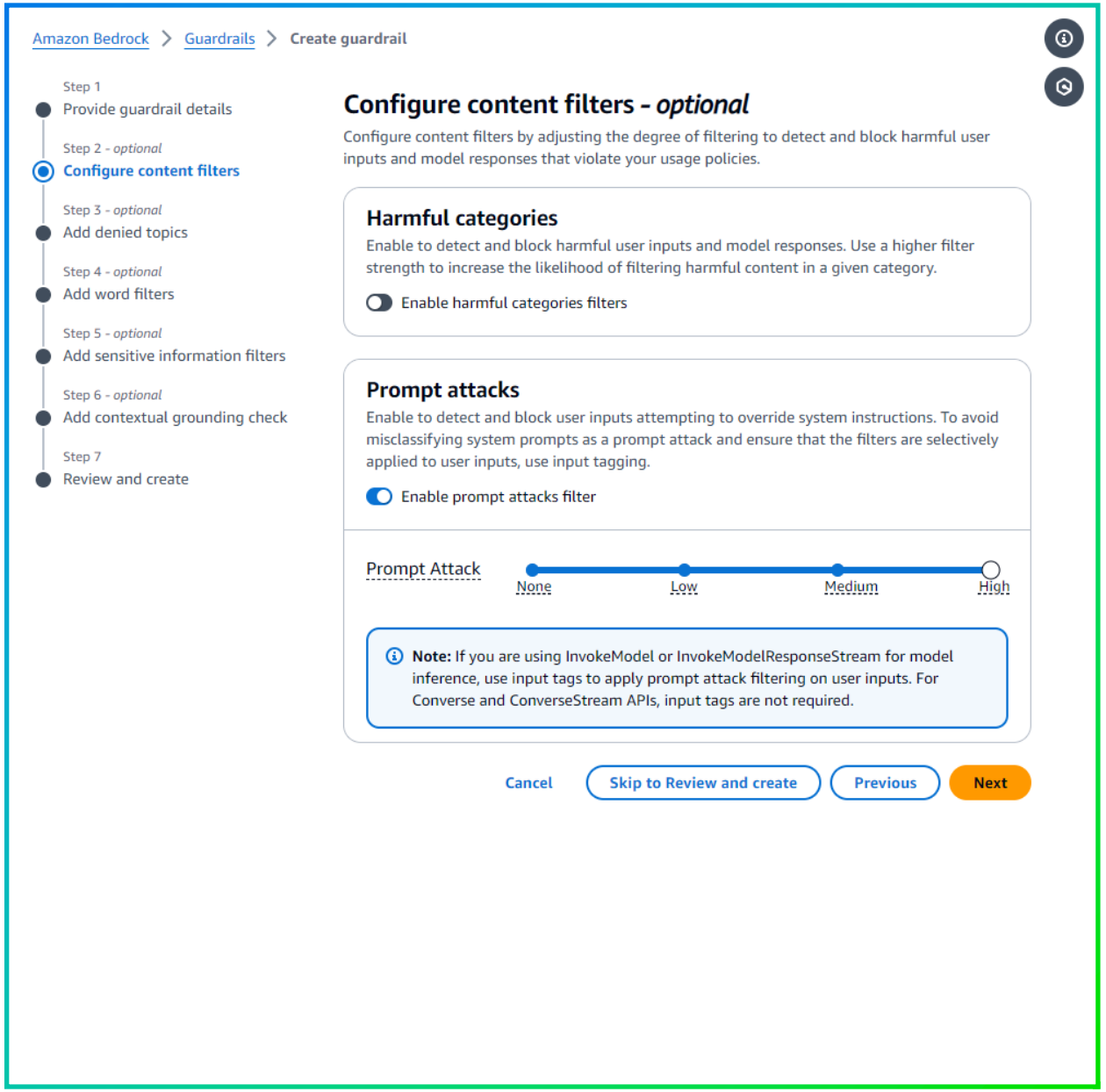
Examples:

- **Substance Use History -**
  use of alcohol, tobacco, drugs, or medications outside the scope defined in the application process.
- **Financial Information -**
  debts, credit score, or financial details not directly relevant to the insurance product applied for.



Prompt attacks detection

Similar to harmful categories, prompt attacks are detected based on classification confidence



10 Places your Security Groups should spend time

1. Develop and implement continuous monitoring
2. Use MFA – lock down credentials
3. Train, train, train
4. Prioritize data resiliency
5. Use immutable data backups and test
6. Leverage automation where possible
7. Consolidate and integrate security solutions
8. Modernize legacy systems
9. Encrypt sensitive data
10. Implement prioritized patching of systems

Plans are worthless, but planning is everything!

Dwight D. Eisenhower

Supreme Commander of the Allied Expeditionary Forces, WWII

Additional resources

AWS Security Leaders Newsletter

Pilot for CISO Circle Members

Get the latest security insights from AWS leaders and customers

aws.amazon.com/executive-insights/content/conversations-with-security-leaders

Thank you!

Maria Thompson

AWS SLG Executive Advisor – Cybersecurity
Amazon Web Services (AWS)

Please complete the survey for this session

Cybersecurity Trends and Best Practices

aws Learning Days
State, Local, and Education