2024 SAN FRANCISCO BSIDES
YOU CAN'T SPELL DYSTOPIA WITHOUT AI

Unlocking the Future

AI is the Key to CISOs Top Challenges

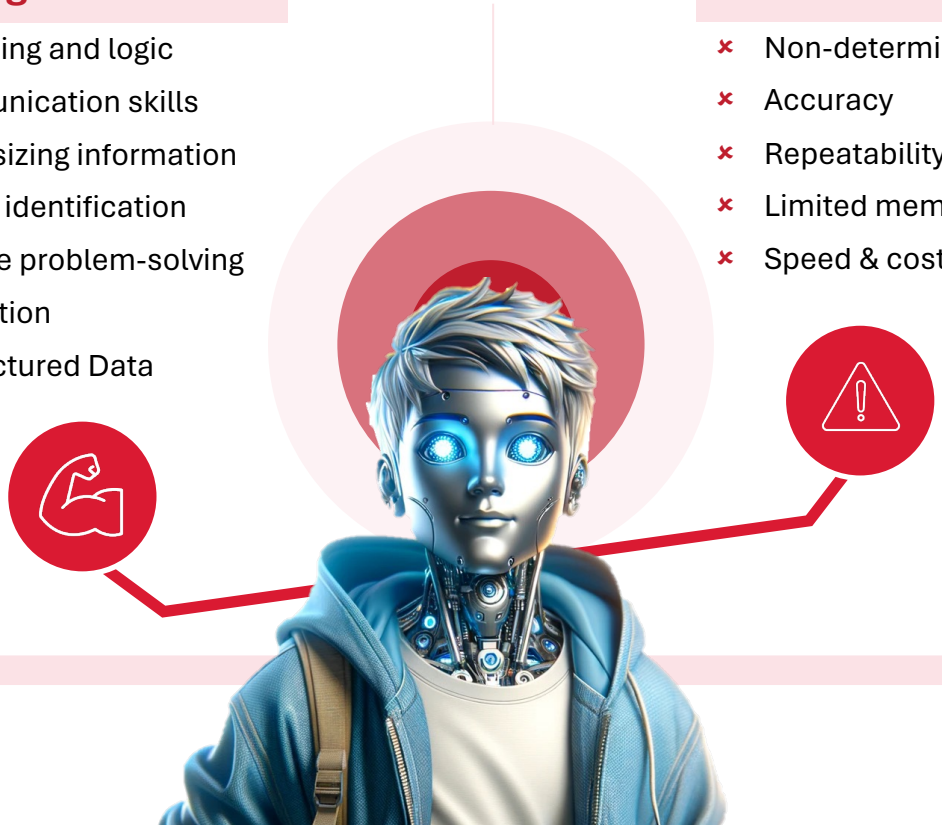
Some AI Fundamentals First

AI Strengths:

- ✓ Reasoning and logic
- ✓ Communication skills
- ✓ Synthesizing information
- ✓ Pattern identification
- ✓ Creative problem-solving
- ✓ Translation
- ✓ Unstructured Data

AI Limitations:

- × Non-deterministic behavior
- × Accuracy
- × Repeatability challenges
- × Limited memory retention
- × Speed & cost efficiency



> “Genius 13-year-old. Overconfident with short attention span and no street smarts”

What is Here Today but Coming Tomorrow

Expanded Context Awareness

Continuous Self-Improvement*

Localized Intelligence

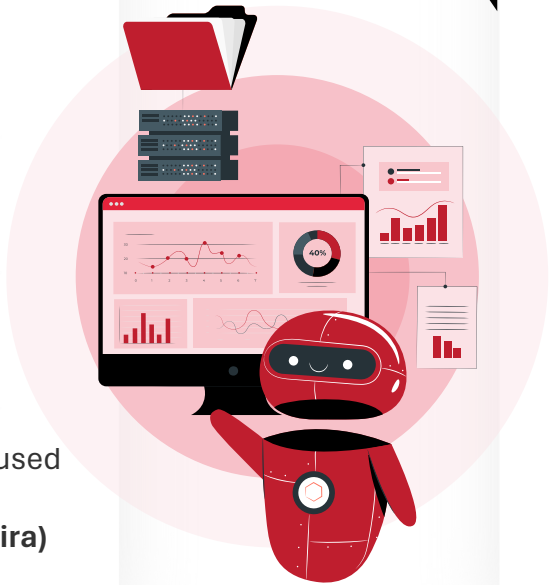
Deciding & Acting (Agents)

Low Cost & High Performing

AI's Impact on the Enterprise

Organization

- **All meetings and communication** will be analyzed and searchable
- **Self updating** documentation & wikis
- **Automated** management status reports
- Local agents (oracles) focused on each area of expertise **(identity, cloud, emails, Jira)**



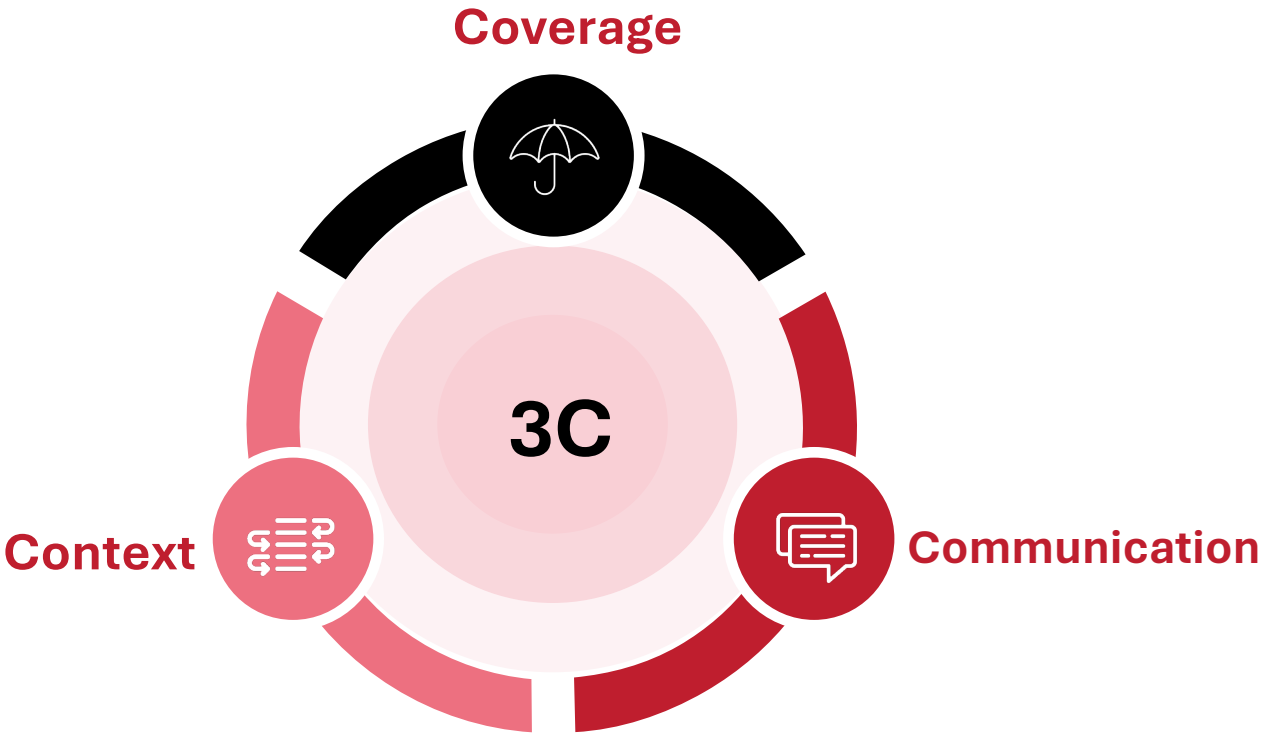
Engineering

- Code and Cloud will become **self documenting**
- Requirements-driven code generation (**requirements as code**)
- **Integrations** will be automatic
- Localized models will monitor systems & help remediate **(self healing)**

CISOs Top Challenges

CISOs top SECURITY challenges

Fundamental Underlying Issues: The three C’s



Context - Who? What? Where? Why? How?

Vulnerability Management

- Is it exploitable? If so by whom?
- Is there compensating controls?
- How hard/easy is it to remediate?
- Is it a critical system or area?
- Who owns the remediation?

Coverage – Width & Depth

Account Takeover (ATO)

Missing logs, fields/ Stopped logs

Thousands of vulnerabilities & alerts that need triaged

Configuration changes

Architecture Reviews

User/ System permissions

Communication – Most Important & Waste of Time

AI excels in the three C's.

Coverage

What would you have 10,000 smart junior security engineers do?

3C

Context

Oracles & Synthesization of the state of the organization

Communication

Communication is a translation challenge: ChatOps is back!


Today
vs
Tomorrow

Detection & Least Privilege

Info: A new outbound call to stripe.com was identified and is being allowed.

This is expected behavior and is considered low risk for the following reasons:

stripe

Stripe is a trusted provider & only outbound calls are allowed

Engineering documentation and discussions have identified Stripe being the new accepted payment provider

The Stripe libraries were introduced to code repo “payment-lib” on 3.3.2024

A **discussion with Cosmo who is the active contributor** to “payment-lib” occurred at 1:22pm PT 3.3.2024 via Slack to confirm the domain stripe.com is allowed outbound

Vulnerability Management & Coverage

An XSS issue was identified in the internal CIS system via the case commenting function.

Located at **xxx/comment/$id**
Total Exposure Time: **22 minutes**

Activity Report

3:35pm PT

The issue was identified via Nuclei assessment & **issue is rated as low risk due to internal system, limited authenticated users required & on a staging system**

3:42pm PT

The issue was introduced in the last push to staging

3:43pm PT

The code that has the vulnerability was found to be introduced by Josh Smith.

3:44pm PT

A fix with a PR was submitted and Josh was notified via Slack.

3:52pm PT

Josh has recognized the issue and accepted the PR

3:53pm PT

A new rule was added to semgrep and requirements doc was modified for this type of issue

Crown Jewel Alert

Your requested approval settings are High for any Crown Jewel Trust Zones.
A request for delete access for role ‘sp-report-gen’ on s3 bucket ‘bi-data-setec/tmp’.
Do you approve?

Recommendation is to grant access for the following reasons:

Request was made by Martin Brice who is Principal engineer of the ‘data-infra’ team who has ownership of this asset

Meetings with Martin & the business media team discussed cleaning up the discarded reports on a regular basis. 3.15.2024 (deeper summary here)

Jira ticket 2928 was filed with request for expanded permissions for regular clean-up activities.

Requirements document for sp-report added delete capability

We reached out to Werner Brandes head of security-engineering via Slack at 3.15.2024 who gives approval.

Thank You

Find me on Linkedin
Caleb Sima