# AGENDA

## The Future of IT & Cybersecurity
# CXO Think Tank

**Grace Beason**
Director of Governance, Risk and Compliance
Guidewire Software Inc

**Alex Cunningham**
CISO
Advisor360

**Brian Haugli**
CEO
SideChannel

**Mark Maybury**
VP, Commercialization, Engineering & Technology
Lockheed Martin
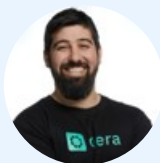
**Tony Parrillo**
VP, Enterprise IT Global Head of Security
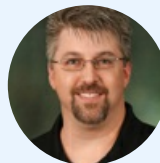Schneider Electric

**Gene Daigle**
Director Information Security
Lupl

**Larry Weber**
VP Product Marketing
Veracode

**Yotam Segev**
Co-Founder & CEO
Cyera US Inc.

**David Bullas**
Director of Sales Engineering
Authomize

**Matt Tesauro**
Distinguished Engineer/Director Security Evangelist - Global
Noname Security

**Sumit Nagpal Ph.D.**
Co-Founder/CEO/CTO
Cherish Health

**Ganesh Pai**
Founder & CEO
Uptycs

**Blake Atkinson**
Director of Infrastructure Security
Cloudflare

**Alon Levin**
VP of Product
Seraphic Security

**Shirish Ranjit**
Sr Enterprise Architect
Fortune 500 Private Sector

**Brian Haugli**
CEO
SideChannel

**Shirish Ranjit**
Senior Enterpris Architect
Staples Inc.

**October 05, 2022**

Eastern Time

## Welcome & Registration

### KEYNOTE PANEL

1:05 PM-2:00 PM

# Security Controls: Measuring Efficacy for the Business Growth

The industry is spending record amounts on cybersecurity tooling, but somehow CISOs still are at times left scrambling to respond to the vulnerabilities like Log4j. Assuming that these types of critical and far-reaching events are inevitable, how can CISOs further improve their organization's preparedness for future cyberattacks?

This panel will discuss potential strategies for determining the critical security controls - both technology and behavioral - that can minimize cyber-risks and give the organization the competitive advantage to grow and innovate. We will explore frameworks for measuring the efficacy of cybersecurity investments, and KPIs that show the board the investment is safeguarding the company's digital infrastructure for the long term.

### CHAIR

**Brian Haugli**
CEO
SideChannel

### PANELISTS

**Tony Parrillo**
VP, Enterprise IT
Global Head of
Security
Schneider Electric

**Mark Maybury**
VP,
Commercialization,
Engineering &
Technology
Lockheed Martin

**Ganesh Pai**
Founder & CEO
Uptycs

### KEYNOTE

2:00 PM-2:35 PM

# Application Security in a DevOps, Cloud and API World

Security teams are challenged to modernize application security practices in light of accelerating shifts to DevOps delivery models and rapid adoption of cloud-native application designs. Applications built on microservices (e.g. serverless, containers, APIs) and delivered continuously are outpacing application security teams ability to secure them. CISOs need to consider new skills, new touch points and new platforms to maintain a strong security posture in light of these trends and the speed at which they are re-shaping IT.

**www.cvisionintl.com**

**Matt Tesauro**
Distinguished
Engineer/Director
Security Evangelist -
Global
Noname Security

---

## Networking Break

---

**DISRUPTOR**

2:45 PM-3:00 PM

## Secure Your Browser - the Most Commonly Used and Vulnerable Application

In recent years, users have migrated from the office and are now working from everywhere and the resources the users need access to have also migrated from their desktops and data-centers to the cloud. The browser has become the de-facto tool for performing almost any action. Unfortunately, risks and threats to the browser are continuously on the rise, The browser is exposed to multiple types of threats and adversaries are increasingly targeting the browser to achieve their nefarious goals.
Join Seraphic VP of Product Management Alon Levin to learn about the threats to browsers and how to ensure secure browsing and prevention of policy infringements in the browser across all users, in all platforms and in every browser.
The session will review how security teams detect and mitigate browsers risks such as:
Browser vulnerability exploitation
Phishing
Intentional or unintentional data leak
Additional web-based attacks

**Alon Levin**
VP of Product
Seraphic Security

---

**PANEL**

3:05 PM-4:00 PM

## The Greatest Fears?

The biggest fear is not the technology, it is the potential of human error that could expose your organization to a cyberattack. The majority of CISOs agree that an employee carelessly falling victim to a phishing scam is the most likely cause of a security breach. Most

also agree that they will not be able to reduce the level of employee disregard for information security. How do we guard against human error without limiting employee efficiency and productivity?

**CHAIR**

**PANELISTS**

**Brian Haugli**
CEO
SideChannel

**Grace Beason**
Director of
Governance, Risk
and Compliance
Guidewire Software
Inc

**Sumit Nagpal Ph.D.**
Co-Founder/CEO/CTO
Cherish Health

**Blake Atkinson**
Director of
Infrastructure
Security
Cloudflare

---

**DISRUPTOR**

# Guarding the Doors: Navigating Risk From Third-Party Code

Open source libraries are widely leveraged by developers. In fact, 97 percent of the typical Java application is made up of open source libraries. But nearly 80 percent of developers never update third-party libraries after including them in codebase.
What does this mean for your applications? There is a good chance that your third-party libraries have undetected vulnerabilities. Scary, right?
The good news is that when alerted to vulnerabilities in open source libraries, developers tend to act quickly. This is especially true when developers understand how the vulnerability could impact their application.
Join us as we review our annual study on open source libraries, State of Software Security (SOSS) v12: Open Source Edition. We will explore the most popular open source libraries, how libraries are evaluated and selected, and how to eliminate risk by fixing vulnerabilities.

**PANELISTS**

**Larry Weber**
VP Product
Marketing
Veracode

---

# Networking Break

---

**DISRUPTOR**

# 5 Steps to Securing Identity and Access for Everything in the Cloud

Identity and Access are under attack. The only way to protect the identity layer from risks and threats is to continuously monitor identities, assets, access privileges, and activities across cloud environments.

Join Authomize Director of Sales Engineering David Bullas, to learn about the 5 steps you need to take to ensure that your Cloud Identity and Access is secure and in compliance with standards and regulations. The session will review how security teams detect and mitigate Identity and Access risks such as:

Excessive Access exposing what you build in AWS

Identity lifecycle risks including partial offboarding

IdP risks including password stealing and user impersonation

## PANELISTS



**David Bullas**
Director of Sales
Engineering
Authomize

---

**PANEL**                                                    `4:55 PM-5:50 PM`

# Cloud Data Security

According to Gartner, 79% of companies have experienced at least one cloud data breach during the pandemic. But the migration of critical business data to the cloud shows no sign of slowing. In fact, it's accelerating. Yet, despite powerful trends and mounting threats, traditional data security has simply not kept pace with the cloud. Security teams still struggle to even understand the reality of what sensitive data they have in the cloud and its associated risks. This is not a sustainable status quo. Data is increasingly a business most valuable asset. And until organizations can align around a shared Data Reality, cloud security will remain several steps behind intensifying security threats and tightening data regulations.
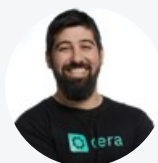
| CHAIR | PANELISTS | | |
|---|---|---|---|
|  |  |  |  |
| **Brian Haugli**<br>CEO<br>SideChannel | **Alex Cunningham**<br>CISO<br>Advisor360 | **Yotam Segev**<br>Co-Founder & CEO<br>Cyera US Inc. | **Shirish Ranjit**<br>Sr Enterprise<br>Architect<br>Fortune 500 Private<br>Sector |

---

# Closing Remarks                                            `5:50 PM-5:55 PM`

---

# Cocktail Hour                                              `5:55 PM-6:55 PM`

---