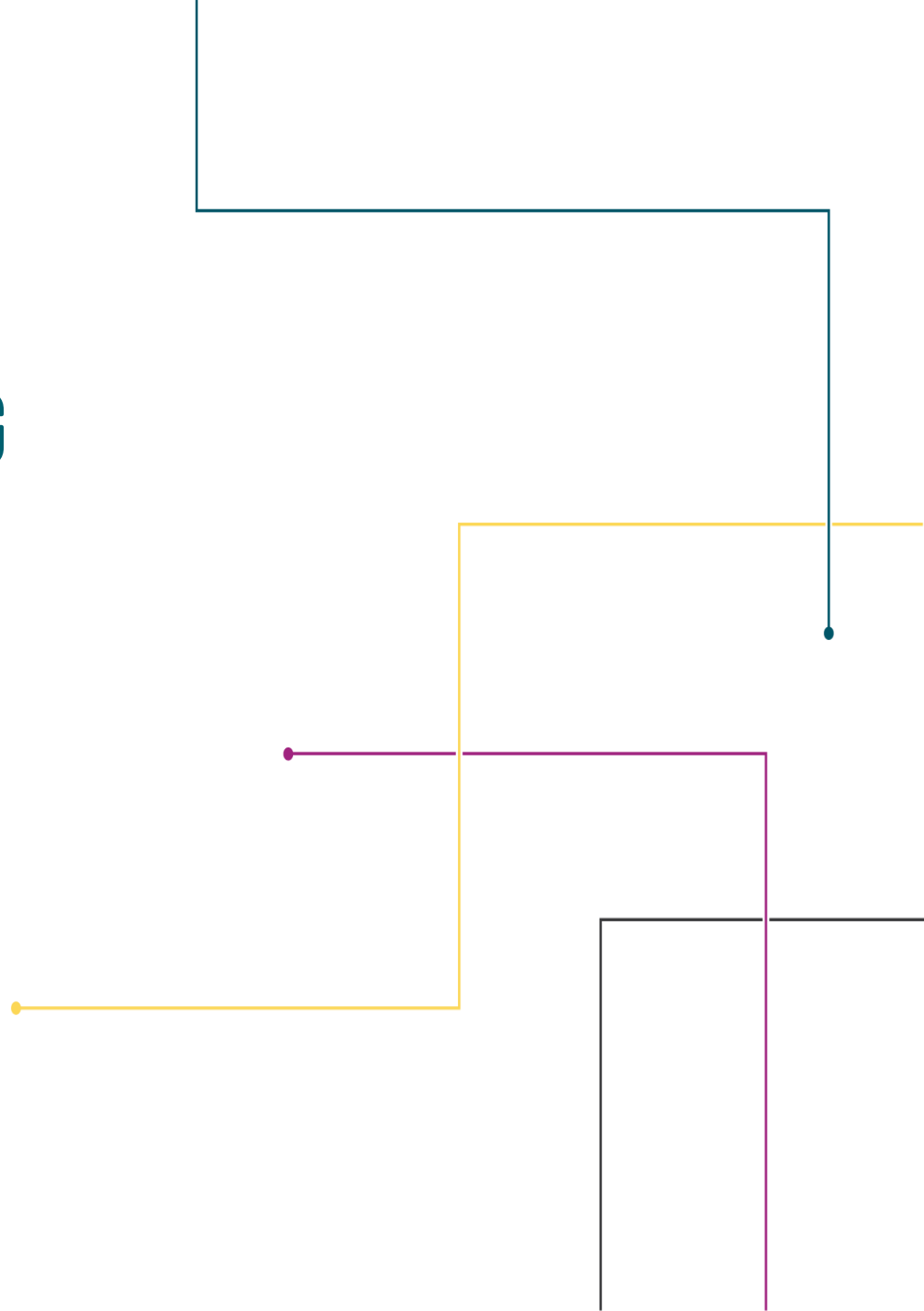




# ISOAG MEETING

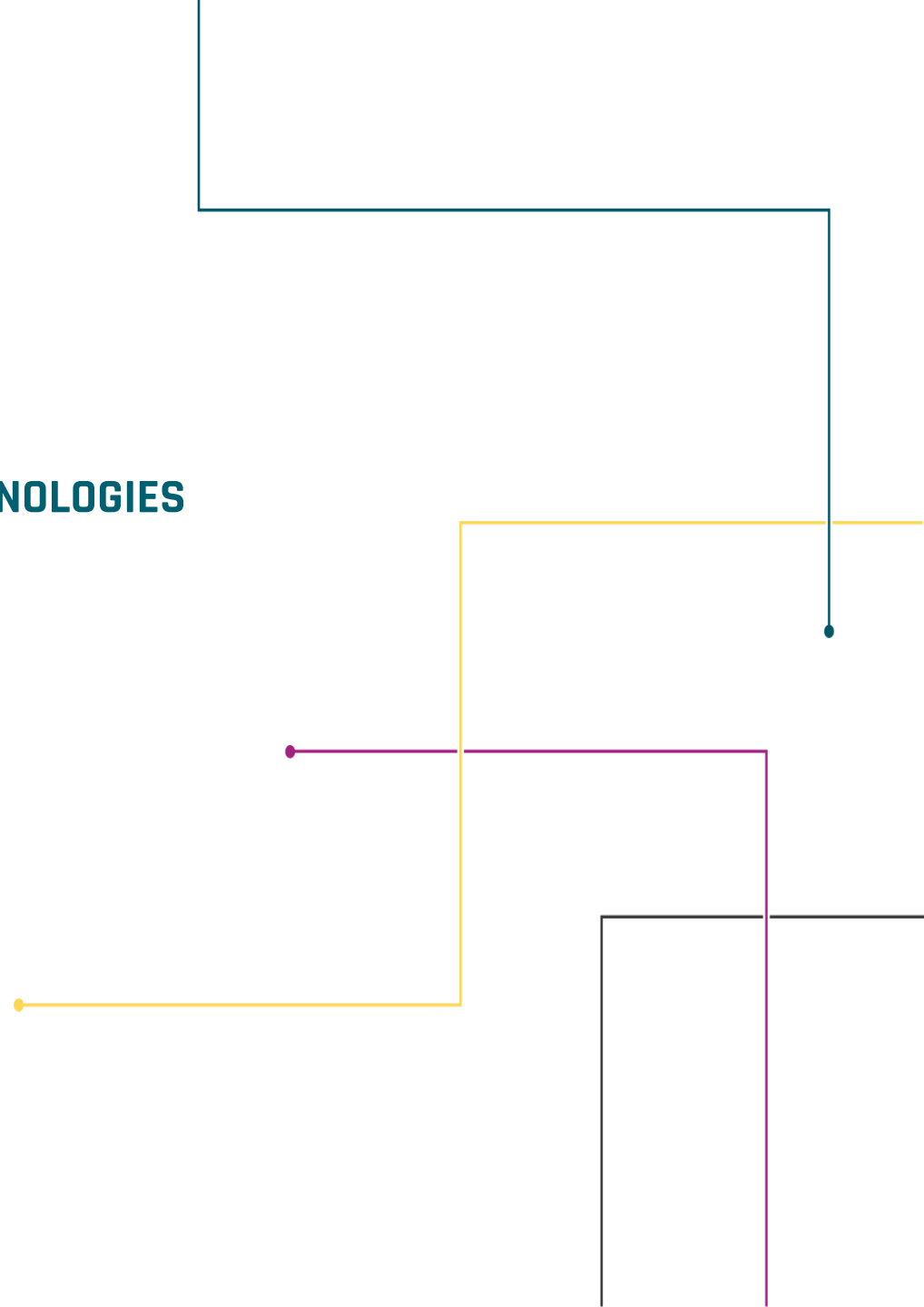
FEB. 3



# FEB ISOAG AGENDA




- **RICK SHAW, AWAREITY**
- **MICHAEL D'AREZZO, E PLUS TECHNOLOGIES**
- **DENNIS MOREAU, VMARE**
- **TINA GAINES, VITA**
- **UPCOMING EVENTS**
- **ADJOURNED**



# HACKERS: INCREASING ATTACKS AND TARGETING GOVERNMENT



Rick Shaw

 @Awareity  
@PreventionCoach

# Quick Background

---

- 20+ years helping clients prevent incidents and liabilities as well as analyzing data and lessons learned/risk management
- Started CorpNet Security in 1998 (white-hat hacking)
- Awareity won Grace Hopper Award from Virginia
- 20+ years researching post-incident reports and WHY
- Specializing in HOW hackers hack and HOW to prevent soaring numbers of breaches and costly consequences

# Questions to Get Started?

---

- Can you afford costs of being hacked?
- Can you afford consequences of being hacked?
- Why are so many information breaches happening?
- Why are so many information breaches successful?
- What do post-incident reports reveal about breaches?
- How do you prevent information breaches?
- How do you eliminate your gaps?

Cybersecurity

## **Hackers Have Infiltrated Many of Washington State's Agencies**

## **Why Apple Security Alert Means Users Must Update iPhones, iPads With iOS 14.4**

Three million users installed 28 malicious Chrome or Edge extensions



# Why Are Breaches Happening?

---

- Hackers exploit **unpatched** software, firmware, and people
- Information has value (sell it, share it, intelligence, etc.)
- Ransomware costs are expected to be \$20 Billion in 2021, up from around \$5 Billion in 2017



# Exploiting **Unpatched** Assets

---

- System Software/Firmware
- Firewalls
- Network and WiFi Devices
- Anti-Virus/Anti-Malware
- Mobile Devices
- Patch Management Software
- Other software, firmware, hardware, etc.



## Windows Update



You're up to date

Last checked: Today, 11:27 AM

Check for updates



## Google Chrome



Google Chrome is up to date

Version 88.0.4324.104 (Official Build) (64-bit)



## Current threats

No current threats.

Last scan: 1/27/2021 2:16 PM (quick scan)

0 threats found.

Scan lasted 26 seconds

34758 files scanned.

## Intrusion Detection Systems Explained: 13 Best IDS Software Tools Reviewed

## 17 Best Vulnerability Assessment Scanning Tools

## Top 11 BEST Patch Management Software Tools [UPDATED 2021 LIST]

# Exploiting **Unpatched** Assets (People)

---

What about your **PEOPLE** assets?

How are you patching your **PEOPLE**?

How are you checking latest version on **PEOPLE**?

What “tools” do you use for **PEOPLE**?

# Exploiting **Unpatched** Assets (People)

---

- Hackers Know **YOUR** People Are **YOUR** GAPS To **YOUR** “Data”
- Phishing attacks (emails)
- Social Engineering (phone calls)
- Remote Worker Issues (emails, phone calls, etc.)
- Text Scams (mobile devices, smishing, etc.)
- Social Media (deepfake videos and others)
- New attack methods are continuously being created

# Exploiting **Unpatched** Assets (People)

---

- Hackers Know **YOUR** People Are **YOUR** GAPS To **YOUR** “Data”
- Phishing attacks (emails)
- Social Engineering (phone calls)
- Remote Worker Issues (emails, phone calls, etc.)
- Text Scams (mobile devices, smishing, etc.)
- Social Media (deepfake videos and others)
- Hackers are exploiting “**unpatched people**”

# Exploiting **Unpatched** Gaps (People)

---

- Gaps in User Awareness
- Gaps in Ongoing Awareness
- Gaps in Changing Threat Awareness
- Gaps in Lessons Learned Awareness
- Gaps in Situational Awareness
- Gaps in Accountability of Awareness
- Other GAPS too...



# Exploiting **Unpatched** Gaps (People)

---

- Policy GAPS
- Best Practice GAPS
- Standards GAPS
- Compliance GAPS
- Technology GAPS
- Opinion GAPS
- GAPS, GAPS, GAPS...



# Exploiting **Unpatched** Gaps (People)

---

- Policy GAPS
- Best Practice GAPS
- Standards GAPS
- Compliance GAPS
- Technology GAPS
- Opinion GAPS
- **Global GAPIDEMIC**









Hi rick,

Your password will expire today  
You can keep using current details

**Keep Your Password**

Awareity Service!

---

**From:** Support <[noreply@awareity.com](mailto:noreply@awareity.com)>

**Sent:** Thursday, October 29, 2020 4:21 AM

**To:** Rick Shaw <[rick.shaw@awareity.com](mailto:rick.shaw@awareity.com)>

**Subject:** PHISHING EXAMPLE - (if you need it) Email Quarantine

Awareity has prevented the delivery of 39 new emails to your inbox ([rick@awareity.com](mailto:rick@awareity.com)) as of Thursday, October 29, 2020 because it identified these messages as spam. You can review these here and choose what happens to them. You can also get more information about quarantined messages by going to the Quarantine page in the Security and Compliance Center. You'll need to provide your work or school account to log in.

[View Emails](#)



Email Quarantine

## Zoom

Hi rick.shaw,

You received a video conferencing meeting:

**Topic**                **rick.shaw**

**Meeting ID**        874 7326 3120

**Time**                Jan 29, 2021 07:00 AM Eastern Time

[REVIEW Meeting](#)

Thank you for choosing Zoom.

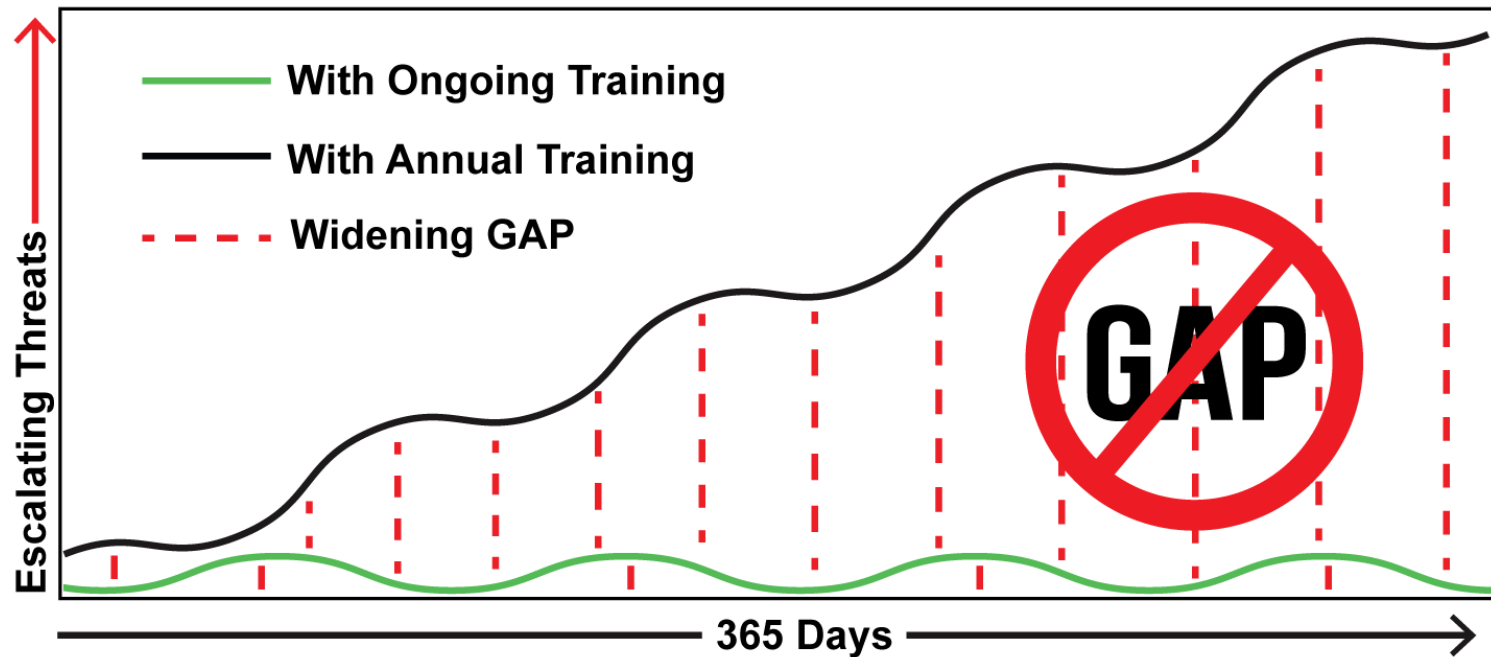
-The Zoom Team

Going Back to the Office	Your Password Is Expiring	Social Media Account Issues
Microsoft Invoice	Bank Account Hold	Coupon Scams
Organization Invoice	Credit Card Usage	Free Giveaways
Vendor Invoice	Olympics	Porn Threats
Emails in Quarantine	Super Bowl	Amazon Balance
Election Info	Super Bowl Commercials	Shipping/Delivery Notice
Covid-19 Health Info	World Cup	Celebrity News
COVID-19 Vaccine Info	Sporting Events	Politics
Pandemic Info	Hurricanes	Riots/Violence

New Job Info	Earthquakes	Police Reform
Voicemail Info	Volcanos	Fake Charities
Your Account Is Expiring	Tragedies (as they occur)	Deep Fake Videos
Investment Scams	Housing Scams	Overdraft Notice Scam
Lottery Scams	IRS Scams	Student Loan Scams
Ticket Scams	Negative Public Records	Business Email Compromise
Census Scams	Court Appearance Scam	ID Theft
Fake Websites	Infected Attachments	Many Others



# Exploiting **Unpatched** Gaps (People)



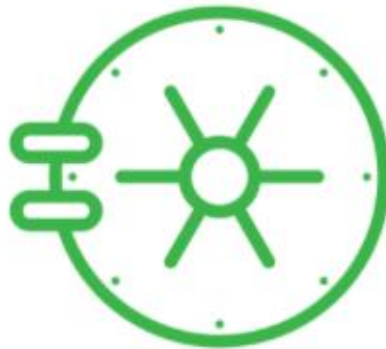
# Solution: Patching People

---





# Ongoing Awareness & Accountability Vault (AAV)



# THE VAULT

# Solution: Patching People (The Vault)

---

- Ongoing Awareness (situational, organizational, etc.)
- Updated Policies
- Updated Alerts
- Updated Attacks/Lessons Learned
- Updated based on GAP Assessments
- Ongoing “BOLO/Zero Day patches” for people
- Tracked/Measured Awareness at Individual Level



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All ✓ 's Are Needed for  
Certification.

- Module Instructions
- Information Risks
- Internet Security
- E-mail Security
  - Email Awareness
  - Email Risks
  - Phishing Attacks
  - Masquerading and Email Best Practices
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

## What Are the Most Common Phishing Attacks?

### VIDEO LESSON:

Please click play on the video below to view and listen to the lesson content.



**Email Security: Common Phishing Attacks**

# Email Security: Common Phishing Scams





(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All 's Are Needed for  
Certification.

(Organization) Awareness and Accountability Vault

Click on the title of the Policy/Document to review

= Reviewed Policy/Document  = Policy/Document to be Reviewed

Group by:  Sort by:   
Document Groups  Title

**ALERTS**				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">AAV Alerts</a>	2018 Q1	3/1/2018	Required Annually
<input type="checkbox"/>	<a href="#">Bad Rabbit Ransomware</a>	Release 10/27/2017	10/31/2017	Required
<input type="checkbox"/>	<a href="#">COVID-19 Cyber Crime ALERT</a>	Review examples of COVID-19 Cyber Crimes	3/30/2020	Required
<input checked="" type="checkbox"/>	<a href="#">COVID-19 Scams ALERT</a>	Review examples of COVID-19 Scams	3/30/2020	Required
<input type="checkbox"/>	<a href="#">COVID-19 Teleworking ALERT</a>	Resources for employees now teleworking.	3/30/2020	Required
<input checked="" type="checkbox"/>	<a href="#">Hackers Spread Ransomware V2</a>	NSA Tools Used to Hack	5/12/2017	Required
<input type="checkbox"/>	<a href="#">Netflix Hacked</a>	Risks with Third Party Service Providers	5/12/2017	Required Annually
<input type="checkbox"/>	<a href="#">New App allows hackers easy access to phone</a>	what employees need to know	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">New Assessment DUE Next Week!</a>	Please download the attached PDF, fill in active fields to complete survey, save as PDF and upload to the Survey IR in TIPS.	1/21/2015	Required Annually
<input type="checkbox"/>	<a href="#">News alert.</a>	example	11/8/2017	Not Required
<input checked="" type="checkbox"/>	<a href="#">Phishing ALERT</a>	Phishing Attempt - 03/30/2020	3/30/2020	Required

Emergency Preparedness/Emergency Response				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Active Shooter</a>	What to do if you find yourself in an active shooter situation	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Bomb Threat</a>	Please refer to the Bomb Threat Checklist (attached) for guidance on the information to be gathered.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Earthquake</a>	Drop, Cover, Hold on. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Fire</a>	Sound the alarm. Evacuate the building. Call for help. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Hazardous Materials Incident</a>	Procedures will depend on material and amount. Review the attached for proper procedures for any situation involving hazardous materials.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Power Outage</a>	Response information	12/19/2014	Required Annually

Employee Handbook				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Employee Benefits and Programs 2020</a>	What employee benefits and programs are available	12/19/2014	Required
<input type="checkbox"/>	<a href="#">Employee Complaint Process</a>	Complaint Process	2/3/2012	Required Annually
<input type="checkbox"/>	<a href="#">Work Life Balance &amp; Policies &amp; Programs</a>	How we can help with the Work Life Balance	12/19/2014	Required
<input type="checkbox"/>	<a href="#">Workers Compensation Policy</a>	Workers Comp	2/3/2012	Required Annually

Employee Safety/OSHA				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Emergency Call List</a>	Call List	2/3/2012	Required Annually
<input type="checkbox"/>	<a href="#">Inspection Guidelines</a>	Inspection Guidelines	2/3/2012	Required
<input type="checkbox"/>	<a href="#">NIOSH Risk Factors</a>	NIOSH Risk Factors	2/3/2012	Required Annually
<input type="checkbox"/>	<a href="#">Workplace Violence Policy v3</a>	Workplace Violence	2/3/2012	Required Annually

Employee Training				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Employee Onboarding</a>	Mission Statement, Corporate Overview and Employee Culture Training for All New Employees	12/26/2014	Required
<input type="checkbox"/>	<a href="#">Employee Onboarding</a>	Mission Statement, Corporate Overview and Employee Culture Training for All New Employees	12/26/2014	Required
<input type="checkbox"/>	<a href="#">Harassment Awareness Training</a>	This is mandatory training required periodically by the Organization. It is part of the duties of each faculty and staff member	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">HIPAA Compliance Training</a>	Proper HIPAA procedures and handling of health information	2/3/2012	Required Annually
<input type="checkbox"/>	<a href="#">OSHA Training</a>	OSHA Training	2/3/2012	Required Annually
<input type="checkbox"/>	<a href="#">PCI &amp; DSS Training</a>	Proper PCI & DSS procedures and handling of payment information	12/19/2014	Required Annually



Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All ✓'s Are Needed for  
Certification.

- Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

**(Organization) Awareness and Accountability Vault**

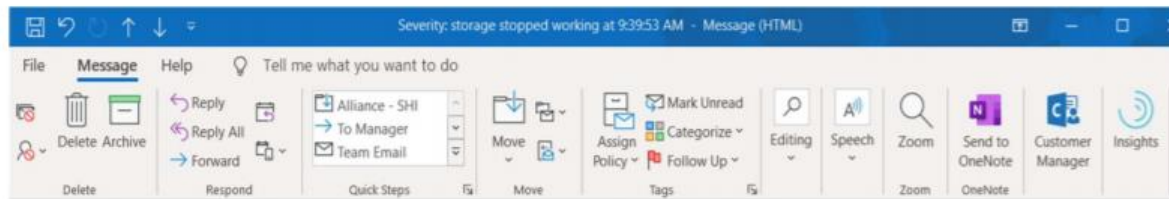
Click on the title of the Policy/Document to review

✓ = Reviewed Policy/Document  = Policy/Document to be Reviewed

Group by:  Sort by:

<b>**ALERTS**</b>				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">AAV Alerts</a>	2018 Q1	3/1/2018	Required Annually
<input type="checkbox"/>	<a href="#">Bad Rabbit Ransomware</a>	Release 10/27/2017	10/31/2017	Required
<input type="checkbox"/>	<a href="#">COVID-19 Cyber Crime ALERT</a>	Review examples of COVID-19 Cyber Crimes	3/30/2020	Required
<input checked="" type="checkbox"/>	<a href="#">COVID-19 Scams ALERT</a>	Review examples of COVID-19 Scams	3/30/2020	Required
<input type="checkbox"/>	<a href="#">COVID-19 Teleworking ALERT</a>	Resources for employees now teleworking.	3/30/2020	Required
<input checked="" type="checkbox"/>	<a href="#">Hackers Spread Ransomware V2</a>	NSA Tools Used to Hack	5/12/2017	Required
<input type="checkbox"/>	<a href="#">Netflix Hacked</a>	Risks with Third Party Service Providers	5/12/2017	Required Annually
<input type="checkbox"/>	<a href="#">New App allows hackers easy access to phone</a>	what employees need to know	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">New Assessment DUE Next Week!</a>	Please download the attached PDF, fill in active fields to complete survey, save as PDF and upload to the Survey IR in TIPS.	1/21/2015	Required Annually
<input type="checkbox"/>	<a href="#">News alert</a>	example	11/8/2017	Not Required
<input type="checkbox"/>	<a href="#">Phishing ALERT</a>	Phishing Attempt - 02/03/2021	2/3/2021	Required

<b>Emergency Preparedness/Emergency Response</b>				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Active Shooter</a>	What to do if you find yourself in an active shooter situation	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Bomb Threat</a>	Please refer to the Bomb Threat Checklist (attached) for guidance on the information to be gathered.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Earthquake</a>	Drop. Cover. Hold on. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Fire</a>	Sound the alarm. Evacuate the building. Call for help. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Hazardous Materials Incident</a>	Procedures will depend on material and amount. Review the attached for proper procedures for any situation involving hazardous materials.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Power Outage</a>	Response information	12/19/2014	Required Annually



### Severity: storage stopped working at 9:39:53 AM

**SI** System IT Notification <bursar@bluehills.reddfords.co.za>  
To Rick Shaw

Reply Reply All Forward  
Mon 3/30/2020 8:40 AM

You forwarded this message on 3/30/2020 9:03 AM.  
This message was sent with High importance.  
If there are problems with how this message is displayed, click here to view it in a web browser.



Hello [rick@awareity.com](mailto:rick@awareity.com),

We detected you have 4 undelivered incoming emails on Monday, March 30, 2020, this is because your account storage is full, your action is required for them to be released.

#### What you should do?

People trying to contact you will receive a message to this effect except you take action below to your portal to retrieve messages and choose what happens to them.

#### Restore Messages

awareity.com support for rick  
(c) 2020 Microsoft Corporation. All Rights reserved | Acceptable usage policy | Privacy Notice  
This email message, including any attached files, is for the sole use of the intended recipient(s) and may contain legally confidential and/or privileged information. If you are not the intended recipient, you are not authorised to copy or disclose all or any part of it without the prior written consent of Inspired Education Group. Opinions expressed in this email and any attachments are those of the sender and not necessarily the opinions of Inspired Education Group.



Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All ✓'s Are Needed for  
Certification.

- ✓ Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

Policy/Document List > Policy/Document Editor

\* Title:

\* Description:

Status:

Effective Date:

Reset Signed Policy/Document:  (Signed Policy/Document will change to Unsigned for all students)

Printable?

Required?  Annual?

Document Groups:

Policy/Document Text:

File ▾ Edit ▾ Insert ▾ View ▾ Format ▾ Table ▾ Tools ▾

Font Family ▾ Font Sizes ▾ Formats ▾ **B** *I*

A ▾ A ▾



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All 's Are Needed for  
Certification.

- Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

[Policy/Document List](#)> [Policy/Document Editor](#)> Department Assignment

In order to check or uncheck the Departments listed below, you will need to check or uncheck "All Departments."

Select	Dept/Group	Description
<input checked="" type="checkbox"/>	All Dept/Groups	
<input checked="" type="checkbox"/>	Administration	Administraton
<input checked="" type="checkbox"/>	Basic User	
<input checked="" type="checkbox"/>	Crisis Management	Crisis Management Personnel
<input checked="" type="checkbox"/>	Customer Service	Customer Service
<input checked="" type="checkbox"/>	Employee Assistance Programs	Employee Assistance Programs (EAP) Personnel
<input checked="" type="checkbox"/>	Human Resources	Human Resources Personnel
<input checked="" type="checkbox"/>	IT	IT
<input checked="" type="checkbox"/>	Legal Counsel	Legal Counsel
<input checked="" type="checkbox"/>	Nursing	Nursing
<input checked="" type="checkbox"/>	Occupational Safety and Health	Occupational Safety and Health Personnel
<input checked="" type="checkbox"/>	Onboarding	
<input checked="" type="checkbox"/>	Public Relations/Corporate Communications	Public Relations/Corporate Communications
<input checked="" type="checkbox"/>	Risk Management	Risk Management Personnel
<input checked="" type="checkbox"/>	Security	Security Personnel
<input checked="" type="checkbox"/>	Top Management	Top Management
<input checked="" type="checkbox"/>	Union Leaders	Union Leaders

NEXT

BACK

ADMIN





Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?


All 's Are Needed for  
Certification.

- Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

**Title:** Phishing ALERT  
**Description:** Phishing Attempt - 02/03/2021

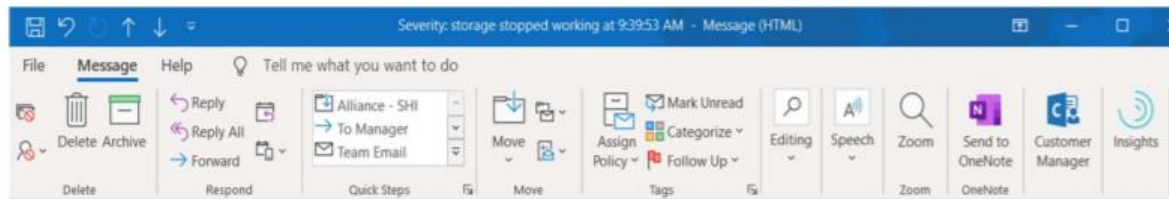
Please review this updated awareness to help ensure the safety of our organization's information and people.

Status	Document	Description
Not Read		Please click on the PDF icon to open and review the document(s), then carefully follow instructions listed.


If you understand and agree to comply with this policy, type **AGREE** in the box below and click the ACCEPT button.

ACCEPT

CANCEL




## Severity: storage stopped working at 9:39:53 AM

 System IT Notification <bursar@bluehills.reddfords.co.za>  
To Rick Shaw

 Reply  Reply All  Forward 

Mon 3/30/2020 8:40 AM

 You forwarded this message on 3/30/2020 9:03 AM.  
This message was sent with High importance.  
If there are problems with how this message is displayed, click here to view it in a web browser.



Hello [rick@awareity.com](mailto:rick@awareity.com),

We detected you have 4 undelivered incoming emails on Monday, March 30, 2020, this is because your account storage is full, your action is required for them to be released.

### What you should do?

People trying to contact you will receive a message to this effect except you take action below to your portal to retrieve messages and choose what happens to them.

### Restore Messages

awareity.com support for rick

(c) 2020 Microsoft Corporation. All Rights reserved | [Acceptable usage policy](#) | [Privacy Notice](#)

This email message, including any attached files, is for the sole use of the intended recipient(s) and may contain legally confidential and/or privileged information. If you are not the intended recipient, you are not authorised to copy or disclose all or any part of it without the prior written consent of Inspired Education Group. Opinions expressed in this email and any attachments are those of the sender and not necessarily the opinions of Inspired Education Group.



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All ✓'s Are Needed for  
Certification.


- ✓ Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

Title: Phishing ALERT

Description: Phishing Attempt - 02/03/2021

Please review this updated awareness to help ensure the safety of our organization's information and people.

Status	Document	Description
Read		Please click on the PDF icon to open and review the document(s), then carefully follow instructions listed.

If you understand and agree to comply with this policy, type **AGREE** in the box below and click the ACCEPT button.

Agree

ACCEPT

CANCEL



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018


Is Every Square Now a  
Checkmark?  
All ✓'s Are Needed for  
Certification.

- ✓ Module Instructions
- ☐ Information Risks
- ☐ Internet Security
- ☐ E-mail Security
- ☐ Human Factor Risks
- ☐ (Organization) Vault

Powered by Awareity

Title: Phishing ALERT  
Description: Phishing Attempt - 02/03/2021

Please review this updated awareness to help ensure the safety of our organization's information and people.

Status	Document	Description
Read		Please click on the PDF icon to open and review the document(s), then carefully follow instructions listed.

If you understand and agree to comply with this policy, type **AGREE** in the box below and click the ACCEPT button.

Agree

**Confirm** ✕

Click OK to confirm your acceptance of this Policy.



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All ✓'s Are Needed for  
Certification.

**(Organization) Awareness and Accountability Vault**

Click on the title of the Policy/Document to review

✓ = Reviewed Policy/Document  = Policy/Document to be Reviewed

Group by:  Sort by:

<b>**ALERTS**</b>				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">AAV Alerts</a>	2018 Q1	3/1/2018	Required Annually
<input type="checkbox"/>	<a href="#">Bad Rabbit Ransomware</a>	Release 10/27/2017	10/31/2017	Required
<input type="checkbox"/>	<a href="#">COVID-19 Cyber Crime ALERT</a>	Review examples of COVID-19 Cyber Crimes	3/30/2020	Required
✓	<a href="#">COVID-19 Scams ALERT</a>	Review examples of COVID-19 Scams	3/30/2020	Required
<input type="checkbox"/>	<a href="#">COVID-19 Teleworking ALERT</a>	Resources for employees now teleworking.	3/30/2020	Required
✓	<a href="#">Hackers Spread Ransomware V2</a>	NSA Tools Used to Hack	5/12/2017	Required
<input type="checkbox"/>	<a href="#">Netflix Hacked</a>	Risks with Third Party Service Providers	5/12/2017	Required Annually
<input type="checkbox"/>	<a href="#">New App allows hackers easy access to phone</a>	what employees need to know	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">New Assessment DUE Next Week!</a>	Please download the attached PDF, fill in active fields to complete survey, save as PDF and upload to the Survey IR in TIPS.	1/21/2015	Required Annually
<input type="checkbox"/>	<a href="#">News alert</a>	example	11/8/2017	Not Required
✓	<a href="#">Phishing ALERT</a>	Phishing Attempt - 02/03/2021	2/3/2021	Required

<b>Emergency Preparedness/Emergency Response</b>				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Active Shooter</a>	What to do if you find yourself in an active shooter situation	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Bomb Threat</a>	Please refer to the Bomb Threat Checklist (attached) for guidance on the information to be gathered.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Earthquake</a>	Drop. Cover. Hold on. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Fire</a>	Sound the alarm. Evacuate the building. Call for help. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Hazardous Materials Incident</a>	Procedures will depend on material and amount. Review the attached for proper procedures for any situation involving hazardous materials.	12/19/2014	Required Annually

- ✓ Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

(Organization)

Report Date: 1/31/2021 1:47:46 PM

Policy/Document Status - (grouped by user)

Sort by:

[\[Download this Report\]](#)  
[\[Print this Report\]](#)

User / Policy/Document Name	Policy/Document Agreed	Date/Time Acknowledged	Required For Cert	Required Annually	Dept/Group	Location	Unit Email	Supervisor Email
Admin, Awareity					Crisis Management		adminhelp@awareity.com	
Organization's Ethics Standards	No	--	Yes	Yes				
OSHA Training	No	--	Yes	Yes				
Password Policy 2020	Yes	1/14/2021 2:32:20 PM	Yes	Yes				
PCI & DSS Training	No	--	Yes	Yes				
Phishing ALERT	Yes	1/31/2021 1:45:37 PM	Yes	No				
Power Outage	No	--	Yes	Yes				
Protocol for Involving Law Enforcement	No	--	Yes	Yes				
Protocols to Address Emergencies and Incidents that Generate Heightened Concern	No	--	Yes	Yes				

User Activity Report

Report Date: 1/31/2021 1:57:20 PM

Reporting Period: Earliest through 01/31/2021

Sort by:

[\[Download this Report\]](#)  
[\[Print this Report\]](#)

**User:** Admin, Awareity **Email:** adminhelp@awareity.com  
**Organization:** (Organization) **Dept/Group:** Crisis Management  
**Location:** **Unit:**

Date/Time	Activity Type	Additional Info
1/31/2021 1:42:21 PM	policyfile-userread	Policy ID: 1476 - CIT ID: 925 - FilePath: /Content/36000/1585584978-Phishing Example - Microsoft - Restore Messages.pdf - MD5: 1a01aac9d0d859d44bf90251cba24a48
1/31/2021 1:45:37 PM	policyagree	Policy: 1476

## (Organization)

Report Date: 1/31/2021 1:54:07 PM

Policy/Document Status - (grouped by policy/document)

Sort by:

[\[Download this Report\]](#)

[\[Print this Report\]](#)

Policy/Document Name / User	Policy/Document Agreed	Date/Time Acknowledged	Required For Cert	Required Annually	Dept/Group	Location	Unit	Email	Supervisor Email
Phishing ALERT									
Admin, Awareity	Yes	1/31/2021 1:45:37 PM	Yes	No	Crisis Management			adminhelp@awareity.com	
Crisis , Management1	No	--	Yes	No	Crisis Management			crisis_management@awareity.com	
EAP, Personnel1	No	--	Yes	No	Employee Assistance Programs			eap_personnel@awareity.com	
Guard, Security	No	--	Yes	No	None			security's@awareity.com	
Head, Department	No	--	Yes	No	Administration			demo@awareity.com	
Human, Resources1	No	--	Yes	No	Human Resources			human_resources@awareity.com	
Legal, Counsel1	No	--	Yes	No	Legal Counsel			legal_counsel@awareity.com	
Occupational , Safety and Health1	No	--	Yes	No	Occupational Safety and Health			support@awareity.com	
Olvey, Keira	No	--	Yes	No	Human Resources			keira.olvey@awareity.com	
Police, Local	No	--	Yes	No	Administration			policeorg.com@awareity.com	
Price, Sandra	No	--	Yes	No	Administration			sandraprice@archstl.org	



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All ✓'s Are Needed for  
Certification.

- ✓ Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

### (Organization) Awareness and Accountability Vault

Click on the title of the Policy/Document to review

✓ = Reviewed Policy/Document  = Policy/Document to be Reviewed

Group by:  Sort by:

**ALERTS**				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">AAV Alerts</a>	2018 Q1	3/1/2018	Required Annually
<input type="checkbox"/>	<a href="#">Bad Rabbit Ransomware</a>	Release 10/27/2017	10/31/2017	Required
<input type="checkbox"/>	<a href="#">COVID-19 Cyber Crime ALERT</a>	Review examples of COVID-19 Cyber Crimes	3/30/2020	Required
✓	<a href="#">COVID-19 Scams ALERT</a>	Review examples of COVID-19 Scams	3/30/2020	Required
<input type="checkbox"/>	<a href="#">COVID-19 Teleworking ALERT</a>	Resources for employees now teleworking.	3/30/2020	Required
✓	<a href="#">Hackers Spread Ransomware V2</a>	NSA Tools Used to Hack	5/12/2017	Required
<input type="checkbox"/>	<a href="#">Netflix Hacked</a>	Risks with Third Party Service Providers	5/12/2017	Required Annually
<input type="checkbox"/>	<a href="#">New App allows hackers easy access to phone</a>	what employees need to know	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">New Assessment DUE Next Week!</a>	Please download the attached PDF, fill in active fields to complete survey, save as PDF and upload to the Survey IR in TIPS.	1/21/2015	Required Annually
<input type="checkbox"/>	<a href="#">News alert</a>	example	11/8/2017	Not Required
✓	<a href="#">Phishing ALERT</a>	Phishing Attempt - 02/03/2021	2/3/2021	Required

Emergency Preparedness/Emergency Response				
	Document Title	Description	Eff. Date	Cert. Status
<input type="checkbox"/>	<a href="#">Active Shooter</a>	What to do if you find yourself in an active shooter situation	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Bomb Threat</a>	Please refer to the Bomb Threat Checklist (attached) for guidance on the information to be gathered.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Earthquake</a>	Drop. Cover. Hold on. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Fire</a>	Sound the alarm. Evacuate the building. Call for help. More information attached.	12/19/2014	Required Annually
<input type="checkbox"/>	<a href="#">Hazardous Materials Incident</a>	Procedures will depend on material and amount. Review the attached for proper procedures for any situation involving hazardous materials.	12/19/2014	Required Annually





(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?



All  's Are Needed for  
Certification.

- Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

**Title:** COVID-19 Teleworking ALERT  
**Description:** Resources for employees now teleworking.

The following file(s) represent or augment the body of this policy.

Status	Document	Description
Read		Please click on the PDF icon to open and review the document(s), then carefully follow instructions listed.
Read		Please click on the PDF icon to open and review the document(s), then carefully follow instructions listed.

If you understand and agree to comply with this policy, type **AGREE** in the box below and click the ACCEPT button.

ACCEPT

CANCEL



(Your Logo Here)

Awareity Admin

Cert Due On:  
03-07-2018

Is Every Square Now a  
Checkmark?

All 's Are Needed for  
Certification.

- Module Instructions
- Information Risks
- Internet Security
- E-mail Security
- Human Factor Risks
- (Organization) Vault

Powered by Awareity

**Title:** Password Policy 2020

**Description:** Password Guidelines

The following file(s) represent or augment the body of this policy.

Status	Document	Description
Read		Please click on the PDF icon to open and review the document(s), then carefully follow instructions listed.

[Please click here to answer the mandatory questions for this document/training.](#)

If you understand and agree to comply with this policy, type **AGREE** in the box below and click the ACCEPT button.

ACCEPT

CANCEL

# Questions to Get Started?

---

- Can you afford costs of being hacked?
- Can you afford consequences of being hacked?
- Why are so many information breaches happening?
- Why are so many information breaches successful?
- What do post-incident reports reveal about breaches?
- How do you prevent information breaches?
- How do you eliminate your gaps?

# Game-Changer is Patching People (Vault)

---

- Easy and immediate awareness at the individual level
- Excellent for at-work or remote workers
- Excellent for contractors, vendors, other third-parties
- Provides REAL TIME measurability, accountability, etc.
- Provides audit-ready and legal-ready documentation
- Automated notifications for immediate and annual updates
- VITA Approved / SHI Contract / Clients say it best...

**What our clients are saying:**

*“AN EASY TO MANAGE AND EFFECTIVE ONLINE TOOL WHICH HAS GREATLY REDUCED THE TIME WE SPEND DELIVERING, TRACKING, AND RESPONDING TO USER TRAINING AND COMPLIANCE. ADDITIONALLY, WE ARE VERY PLEASED WITH THE TIMELY AND EXPERT SUPPORT WE RECEIVED FROM THE AWAREITY STAFF.”*

*“WE HAVE BEEN UTILIZING AWAREITY’S PLATFORM FOR OVER FIVE YEARS AND EVERY YEAR WE FIND MORE AND MORE WAYS TO UTILIZE IT TO SAVE MONEY AND IMPROVE OUR EMPLOYEES’ AWARENESS.”*

*“TRAINING ADDS VALUE AS IT MAKES COUNTY EMPLOYEES AWARE OF ONGOING DANGERS/PITFALLS AND PROVIDES HELPFUL SUGGESTIONS AS TO HOW THE AVERAGE USER CAN ENHANCE SECURITY BY PUTTING THESE SUGGESTIONS INTO PRACTICE.”*

# Awareity Contact Information

---



Rick Shaw – Prevention Specialist

402.730.0090

[Rick.Shaw@Awareity.com](mailto:Rick.Shaw@Awareity.com)

[Info@Awareity.com](mailto:Info@Awareity.com)

[www.Awareity.com](http://www.Awareity.com)

 @Awareity  
 @PreventionCoach





# Lessons Learned: SolarWinds Security Incident

**Mike D'Arezzo**  
Director of Security Services  
February 3<sup>rd</sup> 2021

© 2021 ePlus inc. Confidential and Proprietary.

# Today's Agenda

---

Level Set: What Happened?

What can we do?

How can we stop it from happening again?

Finishing the chapter

Q&A





# Identified Issues



Government | Customer Portal | Partners | Events | Contact Us | English ▾

PRODUCTS > SOLUTIONS > SUPPORT > COMMUNITY > **FREE TRIALS**

CONTACT SALES ONLINE QUOTE 

SolarWinds asks all customers to upgrade immediately to Orion Platform version 2020.2.1 HF 2 to address a security vulnerability.   
More information is available [here](#).



## Identified Issues

- Do we have the SolarWinds Orion product installed here?
- Are we connected to anyone through our network that may have Orion?
- Are we using any vendors/ suppliers that may have been impacted by SolarWinds?



## Identified Issues

- Attacker replaced the upgrade executable for SolarWinds Orion early summer 2020
- The Orion product allows a company to digitally sign a product and ensure its source and identity
- This allows an attacker access to the product through a backdoor DLL and gives the ability to escalate privileges in the Orion environment
- The Orion product requires escalated privileges in order to sign applications and this may be a Domain Admin account in cases



## Identified Issues - breakdown

- The product hack creates a backdoor in around 18,000 companies and gov't agencies
- The hack spread to FireEye which gave attackers access to tools they use for penetration testing and red team engagements
  - Many of their tools took advantage of vulnerabilities not entirely disclosed
  - A lot of vulnerabilities published immediately as a result – Many were critical!
- The attack may also have allowed attackers to Microsoft's Core Source Code



## Identified Issues – Security Lessons

- Security practices at SolarWinds are in question right now
- Asset Management
- Third Party Risk Management
- Product/ Supply Chain Risk Management
- Incident Response Plan



## Identified Issues – Security Lessons

- Security practices at SolarWinds are in question right now
  - Password security
  - Multifactor Authentication for publicly exposed resources or privileged accounts
  - Privileged access to third parties



# Identified Issues – Security Lessons

## - Asset Management

- “Know Thyself”
- Hardware, Software, and Data Asset Management
- Criticality and Risk



# Identified Issues – Security Lessons

## - Third Party Risk Management

- Who do you work with today?
- What do they do for you?
- What impact will they have on your operations?





# Identified Issues – Security Lessons

## - Product/ Supply Chain Risk Management

- Is there impact within your supply chain?
- Do you have redundancy built into your supply chain?
- What is your recovery/ return to normal operations plan?



# Identified Issues – Security Lessons

## - Incident Response Plan

- Do you have one created?
- When was the last time the plan was tested?
- Do you improve it when an opportunity is identified?

# Why ePlus for Security?

- ✓ **Leading technology integrator**
  - ✓ 1400 security customers
  - ✓ 19-year track record, including 3 security acquisitions
- ✓ **Breadth of engineering talent and expertise**
  - ✓ Dedicated engineering resources, logging 80,000 hours of client work per year
  - ✓ 400 security certifications, capturing technical and industry leadership
- ✓ **Broad solutions portfolio**
  - ✓ Security Advisory Services, focused on GRC and Assessment Offerings
  - ✓ Advanced Integration Services
  - ✓ Managed Security Services
  - ✓ Financing
- ✓ **Strong Industry Relationships**
  - ✓ Partnerships with 135+ security vendors
  - ✓ Active participation on 10 industry councils





# ePlus Forward-Focused Solutions



## CLOUD

- ✓ Business-aligned Cloud Strategy
- ✓ Enterprise Cloud Foundation
- ✓ Multi-Cloud Readiness
- ✓ Accelerated Cloud Adoption
- ✓ Optimized Cloud Deployments



## DATA CENTER

- ✓ Data Center Modernization
- ✓ Hybrid Cloud Data Protection
- ✓ Application & Data Insights
- ✓ End-User Computing



## NETWORKING

- ✓ Software Defined Networking
- ✓ SD-WAN
- ✓ Service Provider Networking
- ✓ Mobility / Wireless
- ✓ Connectivity



## COLLABORATION

- ✓ Voice & Video Calling
- ✓ Real-Time Messaging & Meetings
- ✓ Video Conferencing
- ✓ Contact Center



## AI/EMERGING

- ✓ Artificial Intelligence
- ✓ Data Science
- ✓ Machine Learning

## SECURITY

- ✓ Threat Prevention & Detection
- ✓ Data Protection
- ✓ Security Operations & Analytics
- ✓ Security Managed Services
- ✓ Security Advisory Services

## SERVICES

- ✓ Assessments
- ✓ Consulting
- ✓ Professional Services
- ✓ Managed Services
- ✓ Enhanced Maintenance Support
- ✓ Staffing Solutions
- ✓ On Demand Services
- ✓ Integration Services
- ✓ Training

## FINANCING

- ✓ Equipment
- ✓ Consumption Structures
- ✓ Services
- ✓ Vendor Programs
- ✓ Software
- ✓ Device-as-a-Service



# Why ePlus

*In today's constantly changing, complex tech landscape, organizations need a partner that can solve short-term challenges with sustainable solutions that ensure long-term success.*



## **“Do what it takes” dedication**

Long-term view and enduring commitment extending well beyond the transaction



## **Industry-leading consultative expertise**

Capability to help customers better understand their evolving business environment



## **Comprehensive offerings**

Transformative technology to deliver measurable business outcomes



## **Proven processes & methodologies**

Up-front assessments, followed by design and architecture, deployment and implementation, managed services, professional services, and staffing



## **Highly-accessible, consumption-based solutions**

Enable future success and better position our customers for tomorrow's needs

# The Sun Will Come Out!

- We have survived and will continue to survive
- We survive as a species because of our adaptability
- “This too shall pass” – Persian adage



# Questions & Answers

Thank you

Mike D'Arezzo  
[mdare@eplus.com](mailto:mdare@eplus.com)

LinkedIn





# ISOAG

DevSecOps, Cloud Native  
Applications, Zero Trust and Security  
AI:

## Security Transformation at the Intersection

January 2021

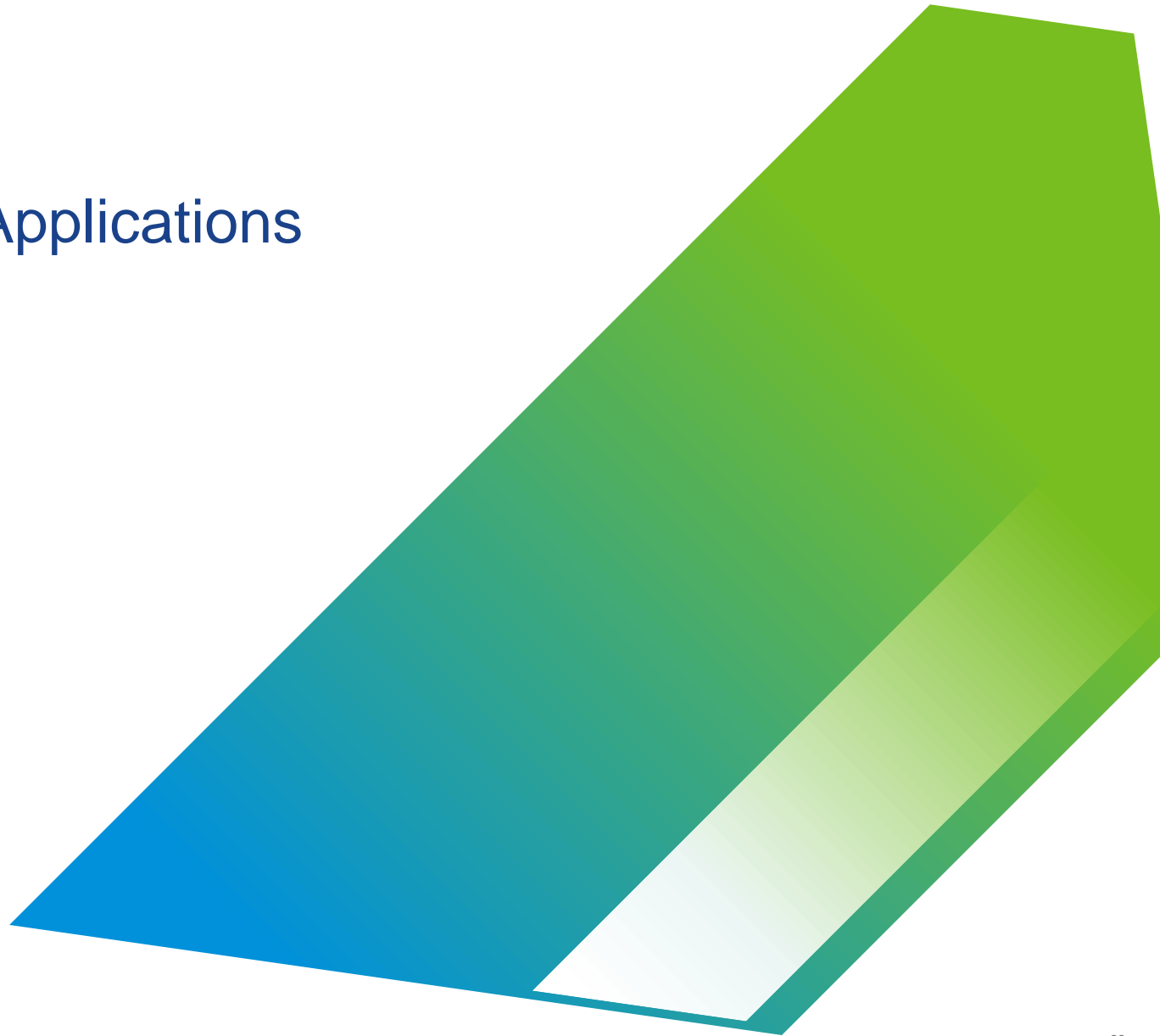
Dennis Moreau, PhD  
Sr Engineering Architect  
Advanced Technology Group  
VMware Office of the CTO



- Cloud Native Architectures, DevSecOps, Zero Trust and Security AI have not been “silver bullets” in isolation ... and are unlikely to be in the future
- At the intersection between these innovations, truly interesting things begin to happen
- The hosting platform is in a position to connect these mutually beneficial technologies
- Some examples of evolution in this direction
  - Standards
  - Public Clouds

# Cloud Native Applications

## CNA Security



# CNA: Comparison

## Conventional Applications Architecture

Large software artifacts

Complex interaction/attack surface

Evolved code base

Large trust boundary, large segments

Impact: Largest existing application footprint

## Cloud Native Applications Architecture (reference architectures)

Many small, more easily grok'd parts

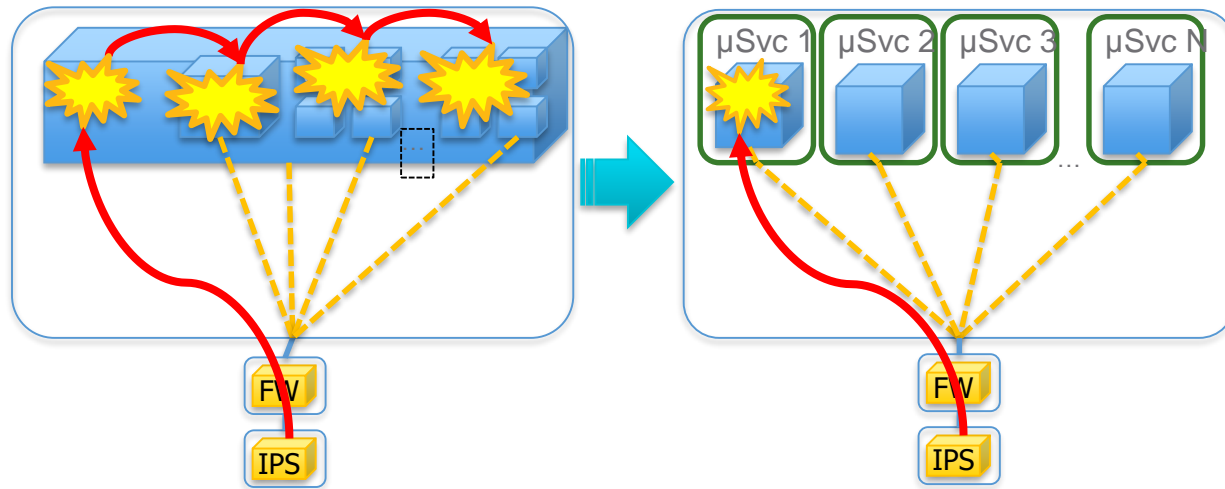
Defined interactions (api) / sharing points (services)

More frequently updated/fixed code base

Can be isolated/segmented at the container, micro-service, function... level

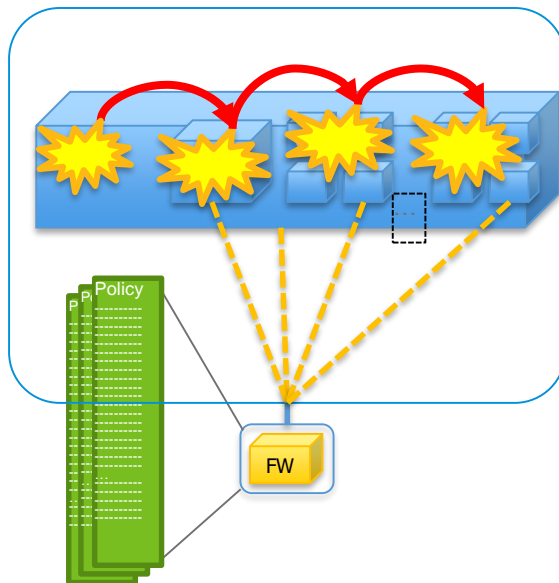
Impact: Fastest growing; over 50% of cloud

# CNA: Aggressive Compartmentalization around Components

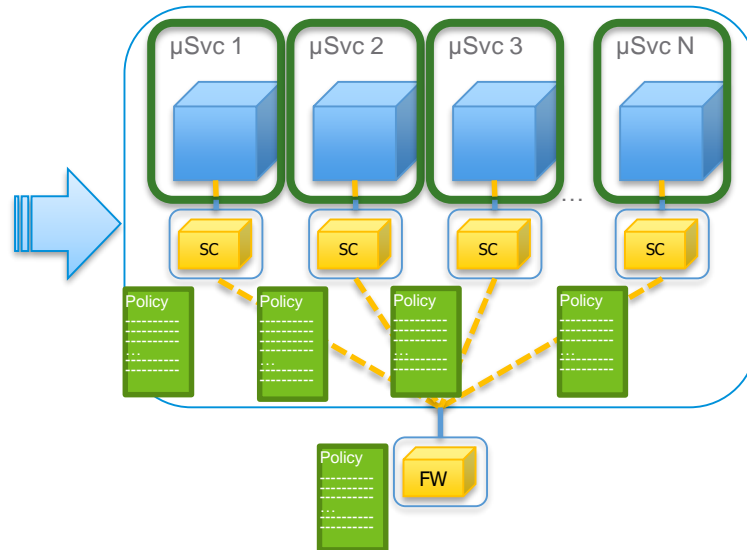


Containment and Protection

# CNA: Granular Policy Simplification and Consistency



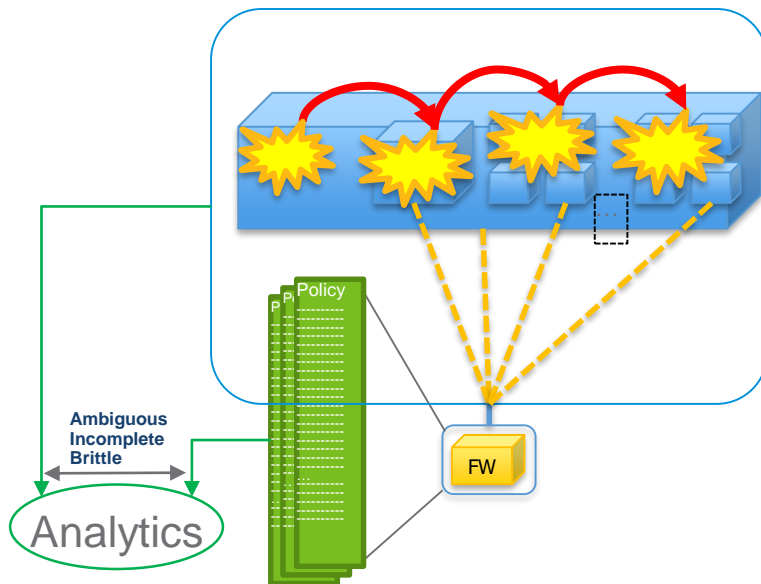
Policy sets large  
Policy sets mixed focus  
Policy sets hard to change  
Dynamics complex & fragile  
Lateral movement invisible



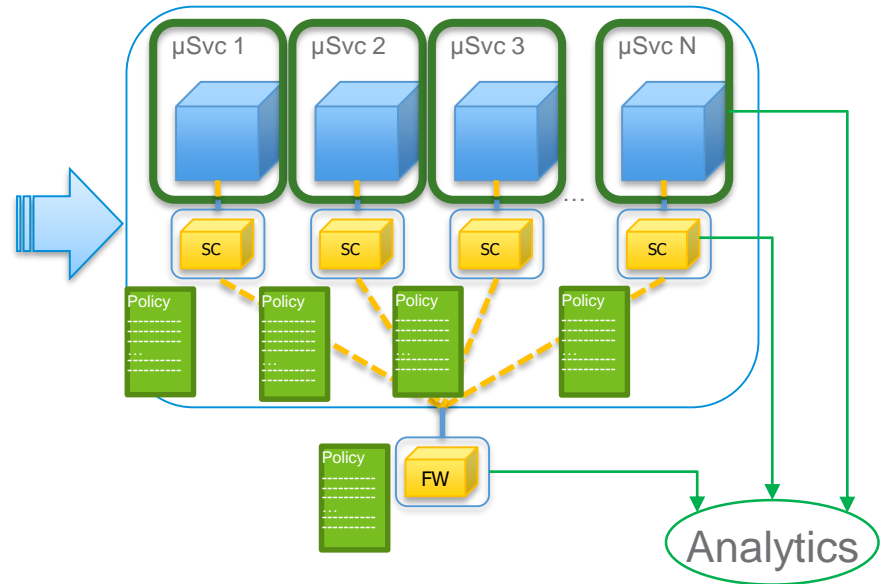
Policy sets much smaller  
Policy focused on one Svc/Abstraction  
Policy sets easy to change  
Dynamics are integral  
Lateral movement visible and restricted

SC := Service Mesh Side Car

# CNA: Improved Actionability, Explain-ability ... Dynamics



- Policy sets large
- Policy sets mixed focus
- Policy sets hard to change
- Dynamics complex & fragile

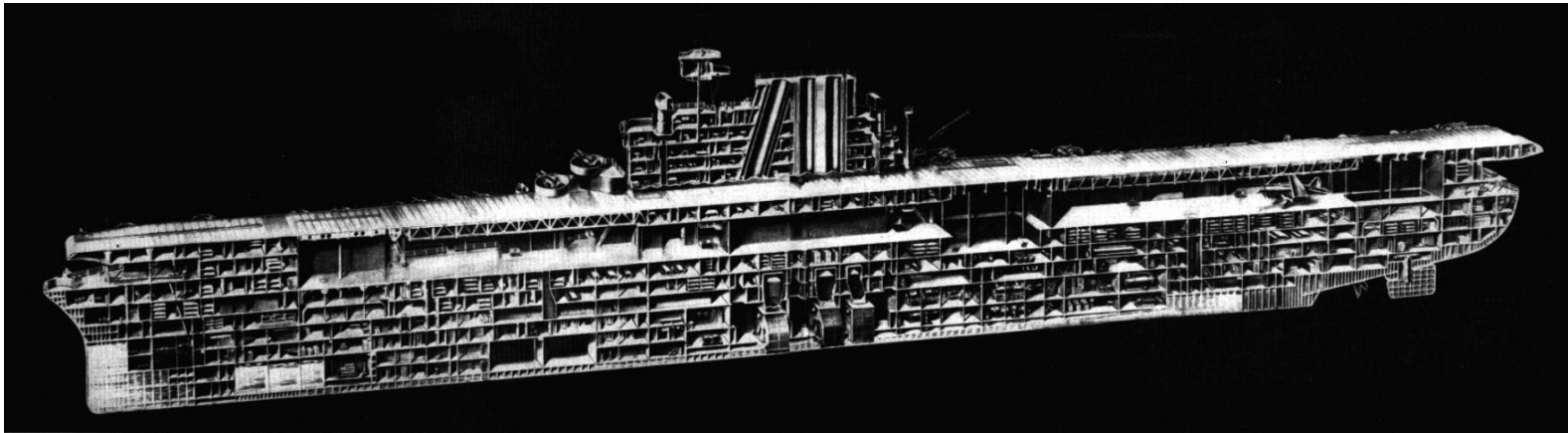


- Policy sets much smaller
- Policy focused on one Svc/Abstraction
- Policy sets easy to change
- Dynamics are integral

SC := Service Mesh Side Car

## CNA security resilience comes from:

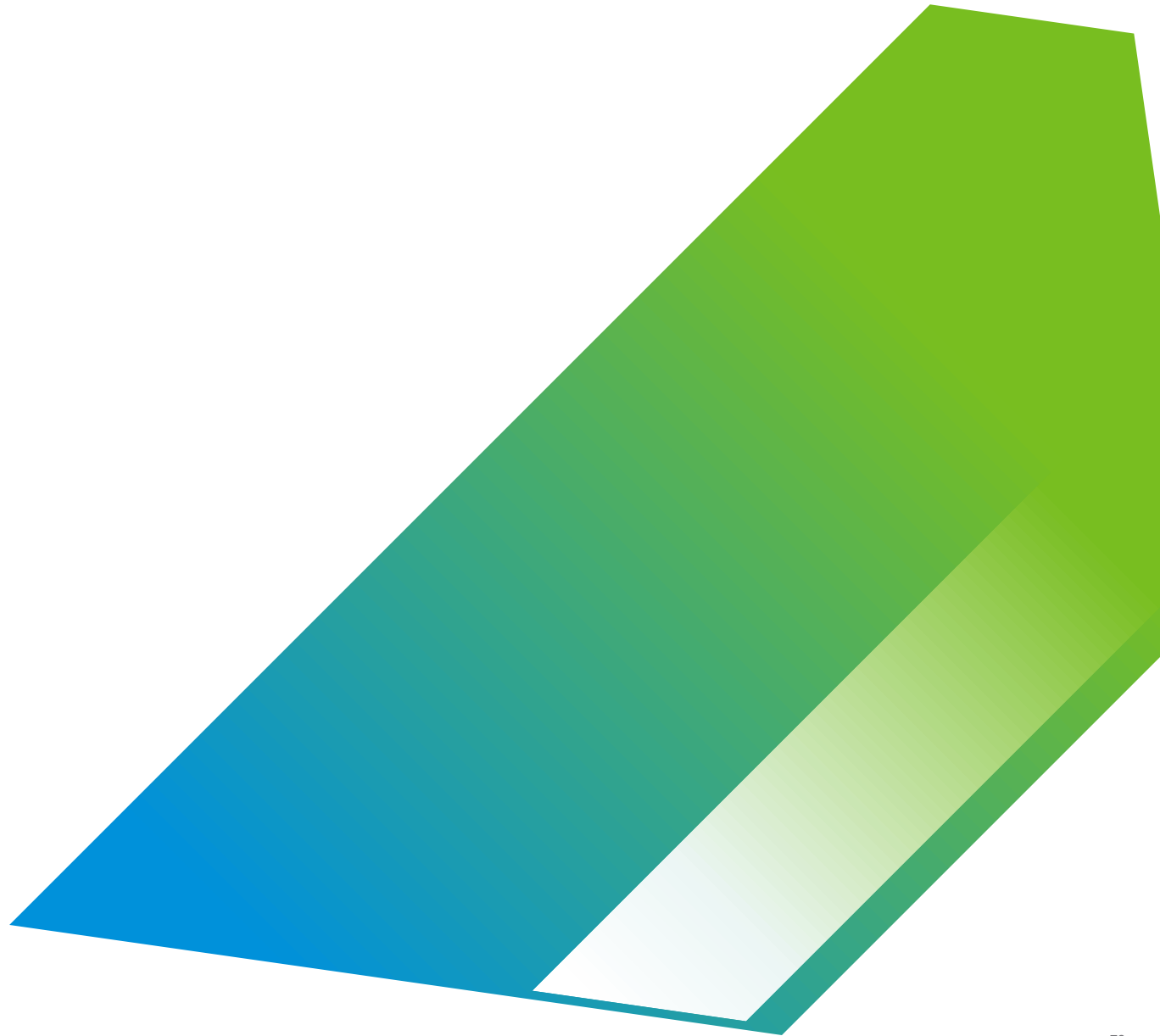
Distributed, Decoupled, Dynamic components ... each of which can have its own state, isolation, policy, instrumentation, development/fix lifecycle, ...



Challenge: But, where does all that API policy for all those policy enforcement points come from???

# DevSecOps

Shifted-Left Security





# DevSecOps for and in cloud

DevSecOps as a Service (certified : AF Platform One)

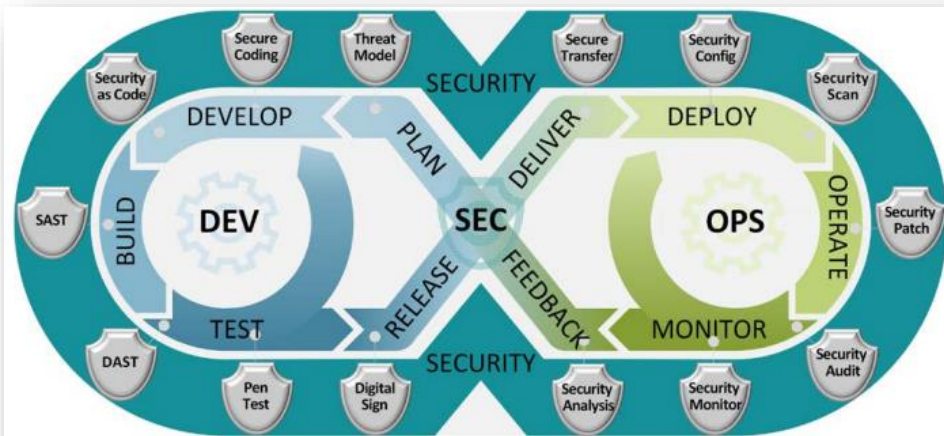


Figure 3: DevSecOps Software Lifecycle

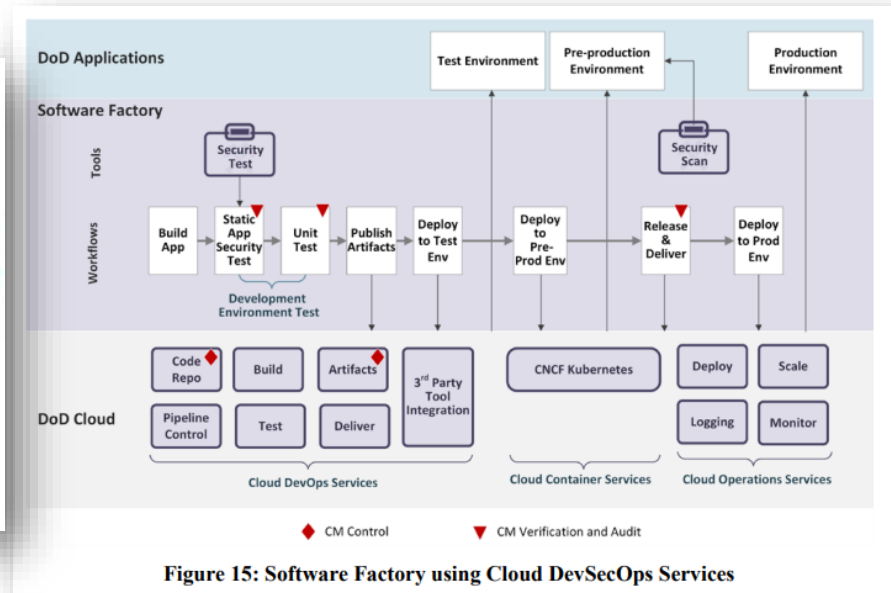


Figure 15: Software Factory using Cloud DevSecOps Services

Page 18:

<https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0%20Public%20Release.pdf?ver=2019-09-26-115824-583>

# devSecOps – Infrastructure vs Application – Continuity - Context

## Beyond DoD

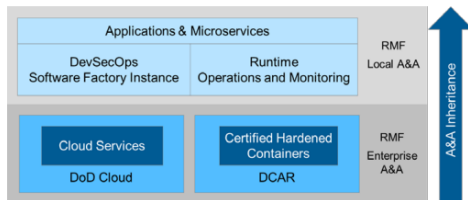


Figure 7: Assessment and Authorization Inheritance

Table 2: Roles of Authorizing Officials in DevSecOps

Capability	Authorizing Official
DoD Enterprise Hardened Containers	Enterprise AO (e.g., Defense Information Systems Agency (DISA))
DevSecOps software factory instances	Enterprise AO (e.g., DISA, Military Department (MilDep) CIO)
Continuous Process Improvement / Continuous Authorization of DevSecOps software factory instances	Specialty or Local AO (e.g., Program executive Officer (PEO))
AO for mission applications	Specialty or Local AO (e.g., PEO)

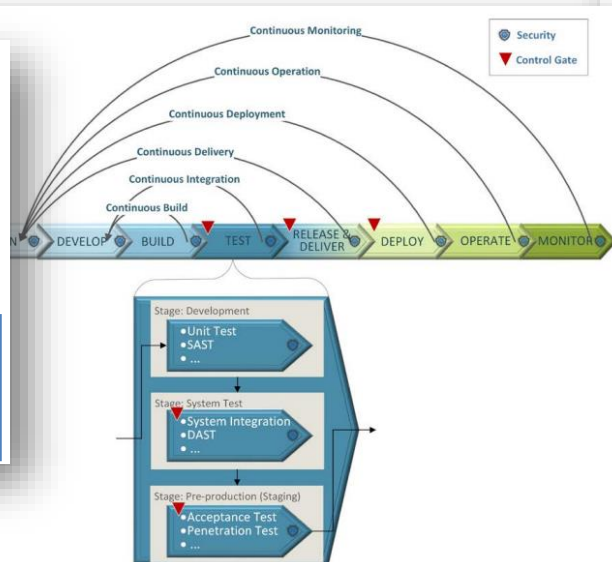


Figure 5: Application DevSecOps Processes

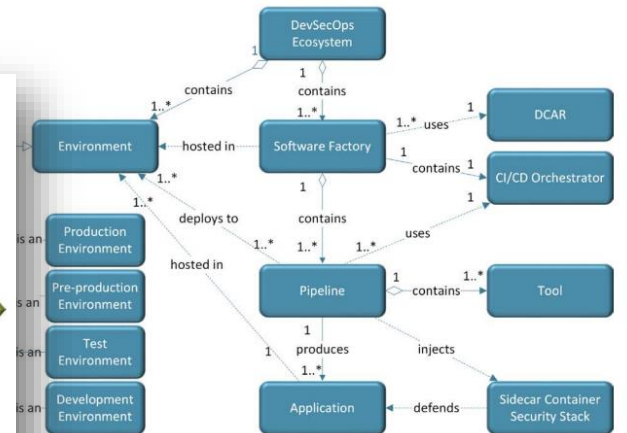


Figure 2: Conceptual Model

### 2020 Analyst Projections

- By 2023 85%-95% of all development projects will adopt DevSecOps practices. (approx. 42% today)
- By 2023 20%-30% of all development projects will be following DevSecOps from design thru production. (approx. 12% today)

<https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html>

### DoD Reference Design

[https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0\\_Public%20Release.pdf?ver=2019-09-26-115824-583](https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583)

### Anchore:

<https://blog.executivebiz.com/2020/06/anchore-gets-dod-certification-for-hardened-devsecops-software/>

API Desc, Test, Dep...

# Enter DevSecOps

Context from the Left

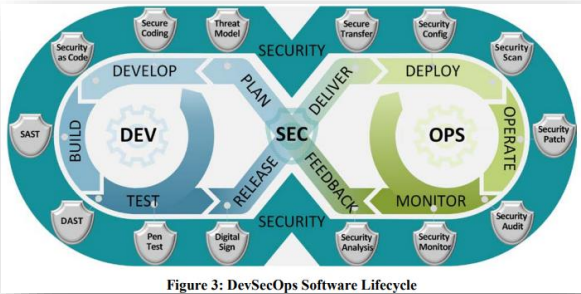
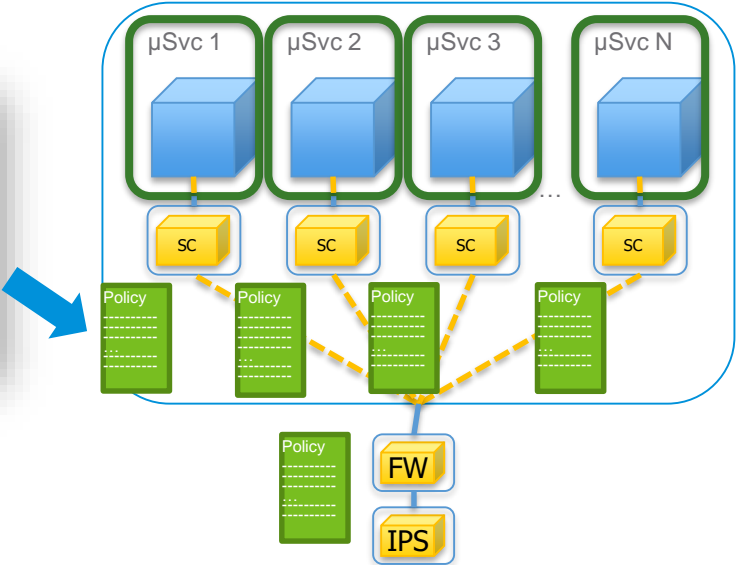


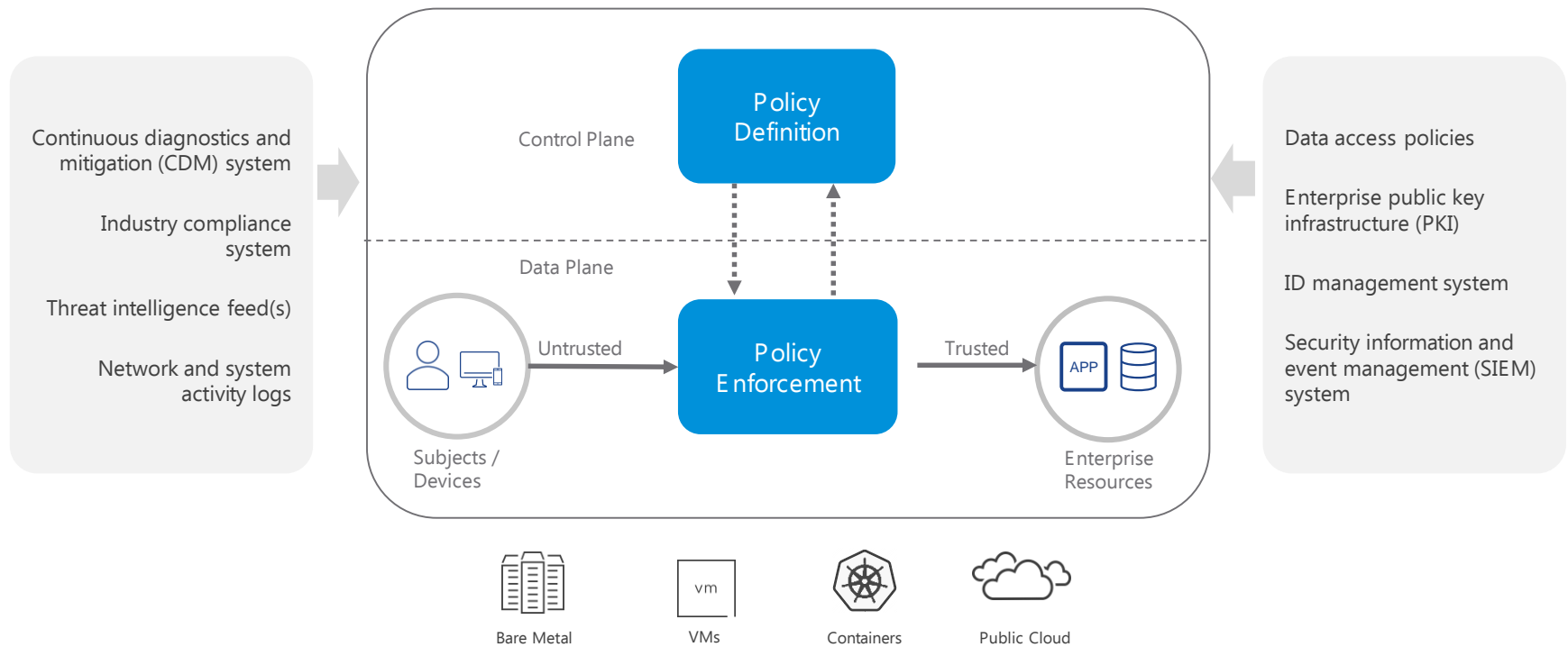
Figure 3: DevSecOps Software Lifecycle



# Zero Trust: Aligning the Security Portfolio

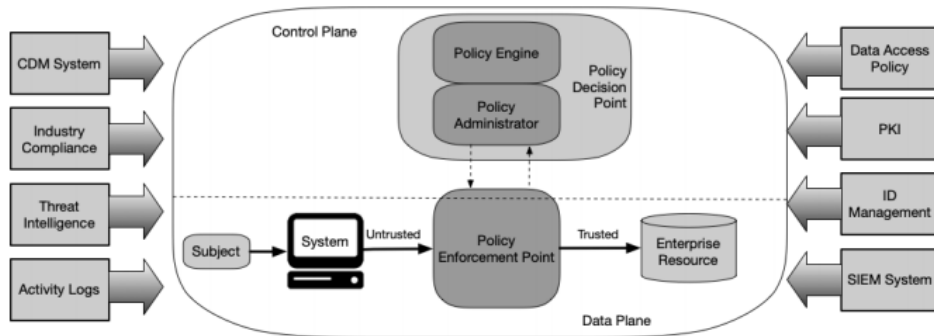
Suppose we can give the right level of policy to the granular isolation boundaries in a CNA, ... there are still multiple-modalities of security to align

# NIST ZTA: One way to enable simpler more resilient security policy

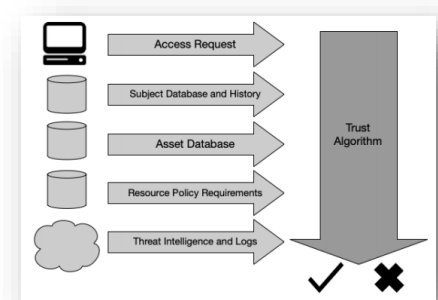
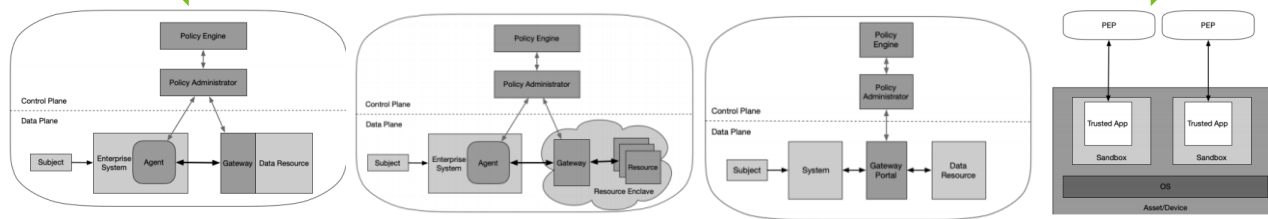


Ref: NIST SP 800-207 - Zero Trust Architecture – pp 9, 14-17

# ZT System Components

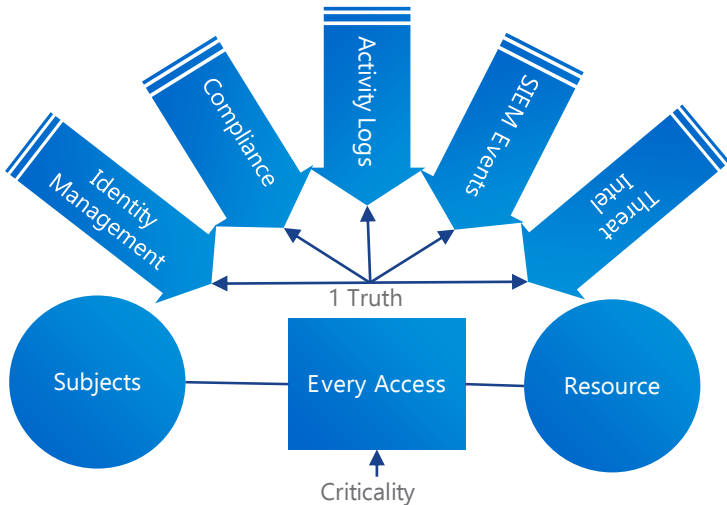


- Continuous diagnostics and mitigation (CDM) system
- Industry compliance system – (template)
- Threat intelligence feed(s) – (signature)
- Network and system activity logs & ML
- Data access policies – (intent policy rules)
- Enterprise public key infrastructure (PKI)
- ID management system – (intent roles)
- Security information and event management (SIEM) system – (detection rules, correlation rules, & action rules)



# Platform Enabled Security Portfolio Alignment

## What is Zero Trust? And why use it?



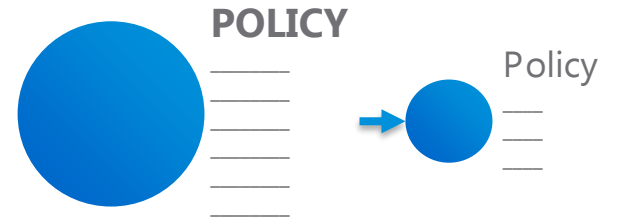
### How Do I Deploy Zero Trust (NIST)

1. Identify All Subjects
2. Identify All Resources
3. Identify Criticality and Bus. Process
4. With 1, 2 & 3 Define ZT Policy
5. Deploy Policy (mapping for E2E)
  - Minimize Granularity
  - Enforcement is Continuous

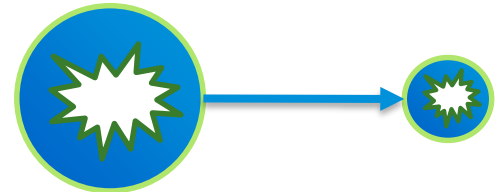
For this effort we extend ZT End to End



Smaller More Aligned Policy sets



Smaller Attack Surface & Blast Radius



Easier To Update Policy Sets



More Mobile Policy

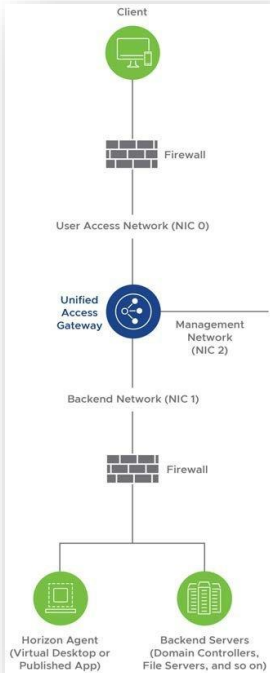


Reference: NIST SP 800-207 - Zero Trust Architecture – pp 37

# Zero Trust Reference Architecture – (not the only approach)

## Security Architecture – Automatable, Normalized, Cross Platform

VMware



<https://techzone.vmware.com/resource/zero-trust-secure-access-traditional-applications-vmware>

Amazon AWS

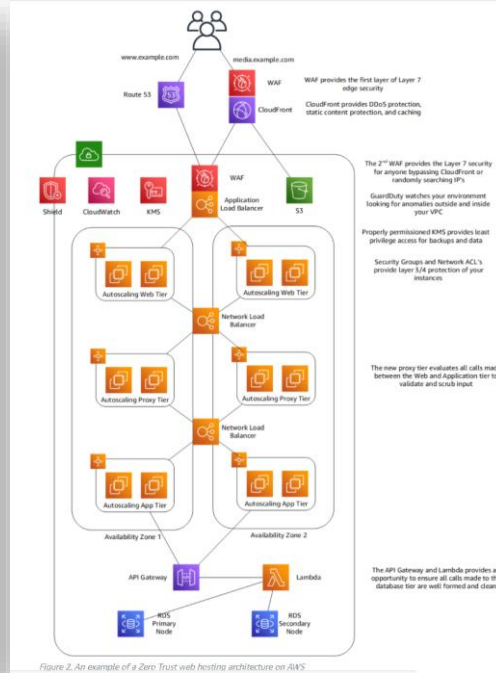
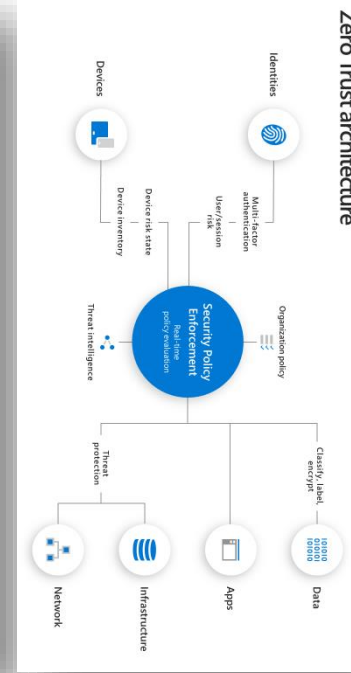


Figure 2. An example of a Zero Trust web hosting architecture on AWS

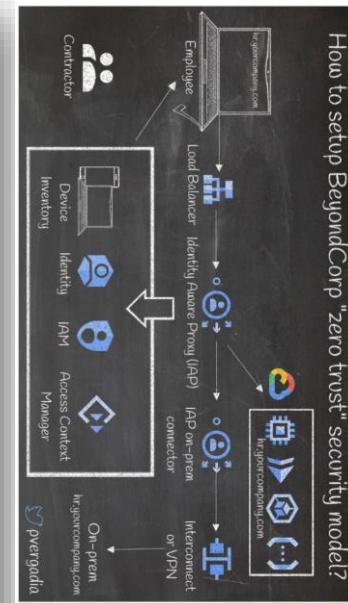
<https://aws.amazon.com/blogs/publicsector/how-to-think-about-zero-trust-architectures-on-aws/>

Microsoft Azure



<https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft>

Google



<https://cloud.google.com/blog/products/application-development/13-popular-application-architectures-for-google-cloud>



# Enter Zero Trust

Context from below

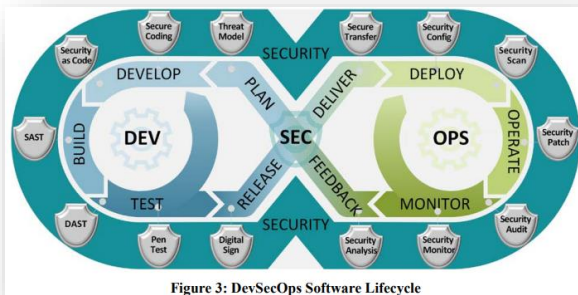
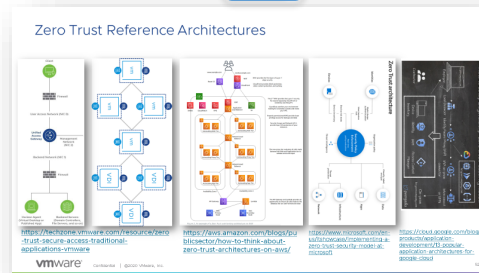
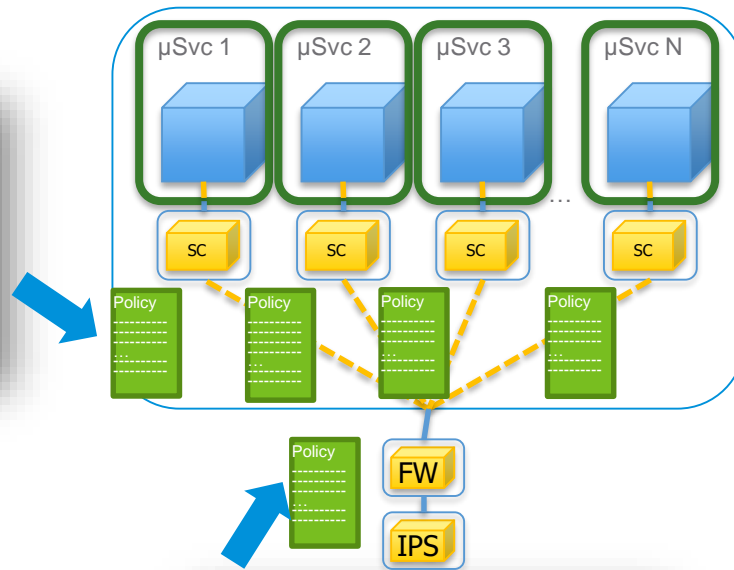


Figure 3: DevSecOps Software Lifecycle



# Security AI

System and Service Guard Rails address key  
Security AI barriers ... today

## Leveraging Platform Metadata

### Alignment: Leveraging Platform Metadata

#### Compartmentalization:

- Containment
- Classification (Intention vs. Observation)
- Protection



#### Trusted Communication:

- Sources
- Destination
- Dependency



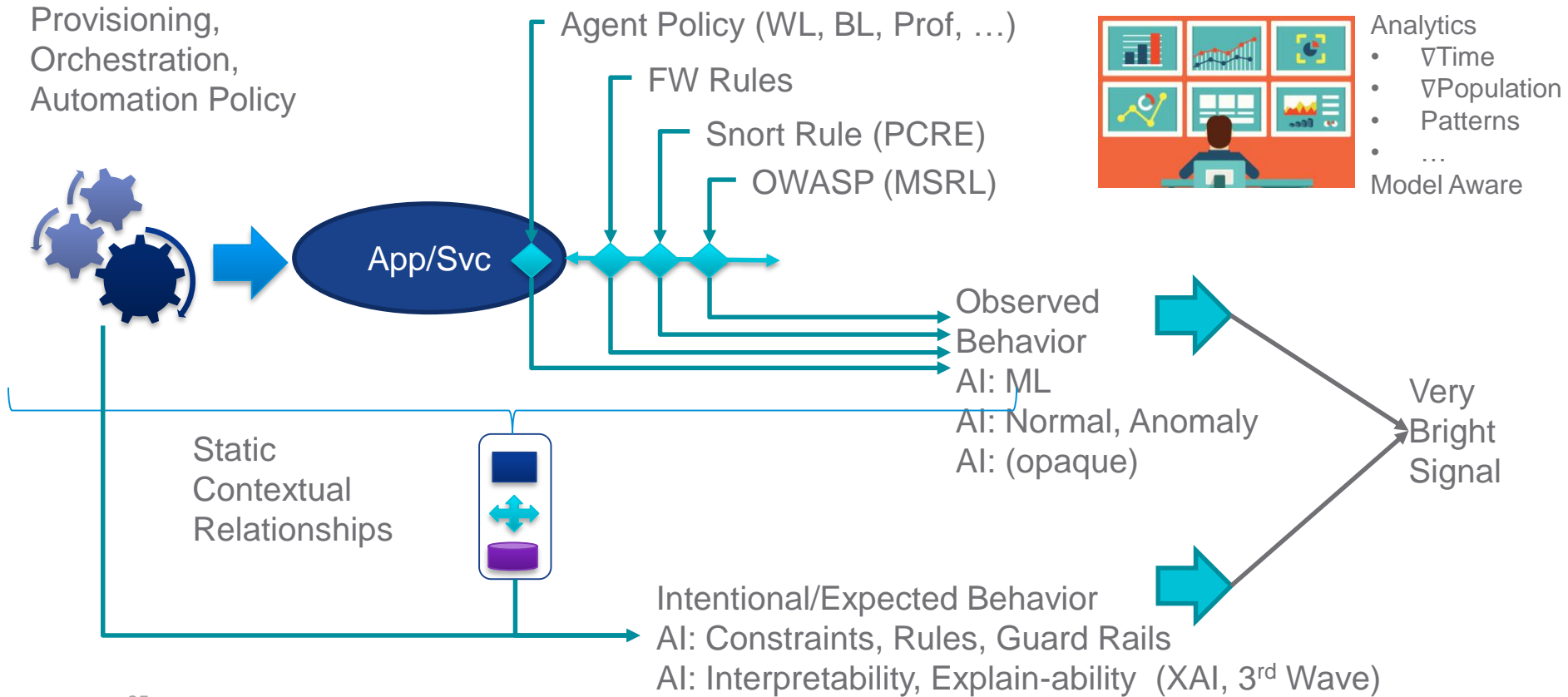
#### Controls Policy:

- EP & NW Instrumentation
- Aligned, Contextual, Actionable



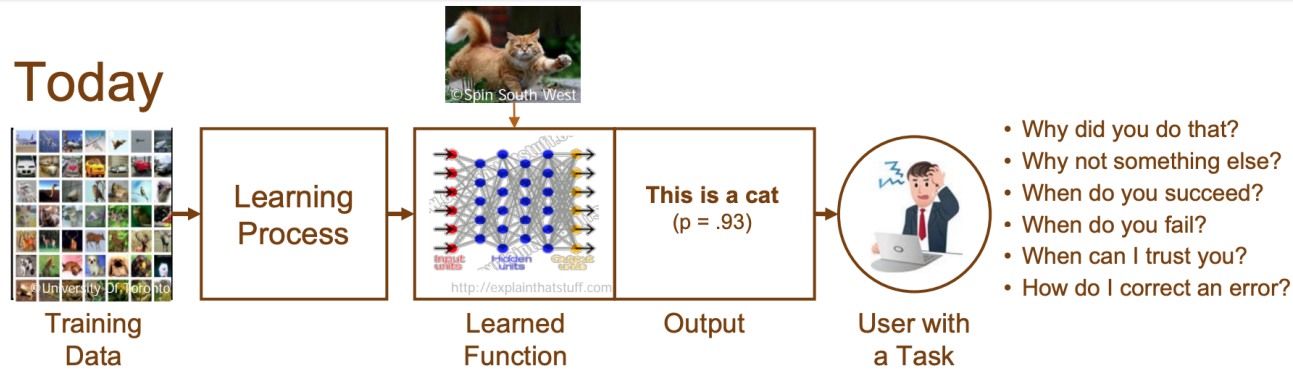
# Policy, Behavior and Analytics in Context

## Policy, Behavior and Analytics in Context

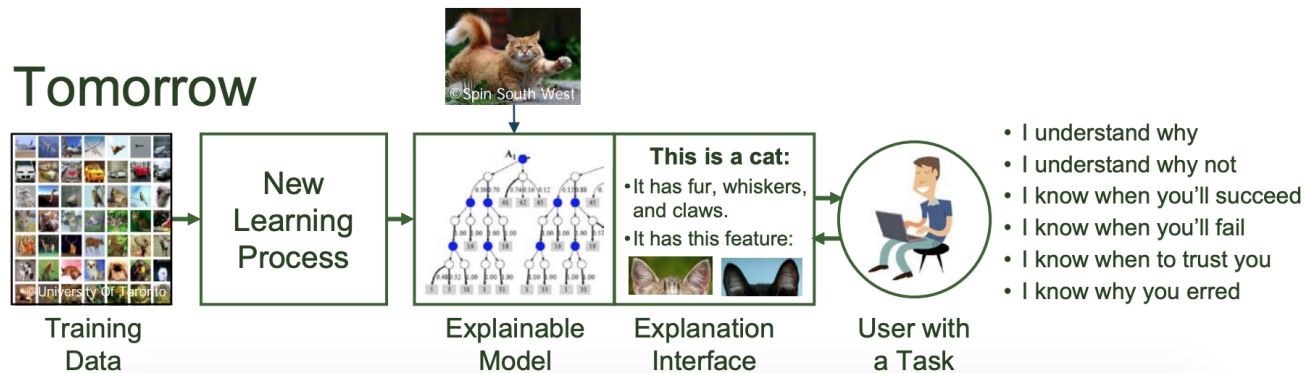


# Directional: Explainable AI

## Today



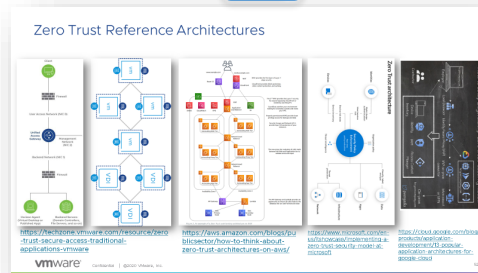
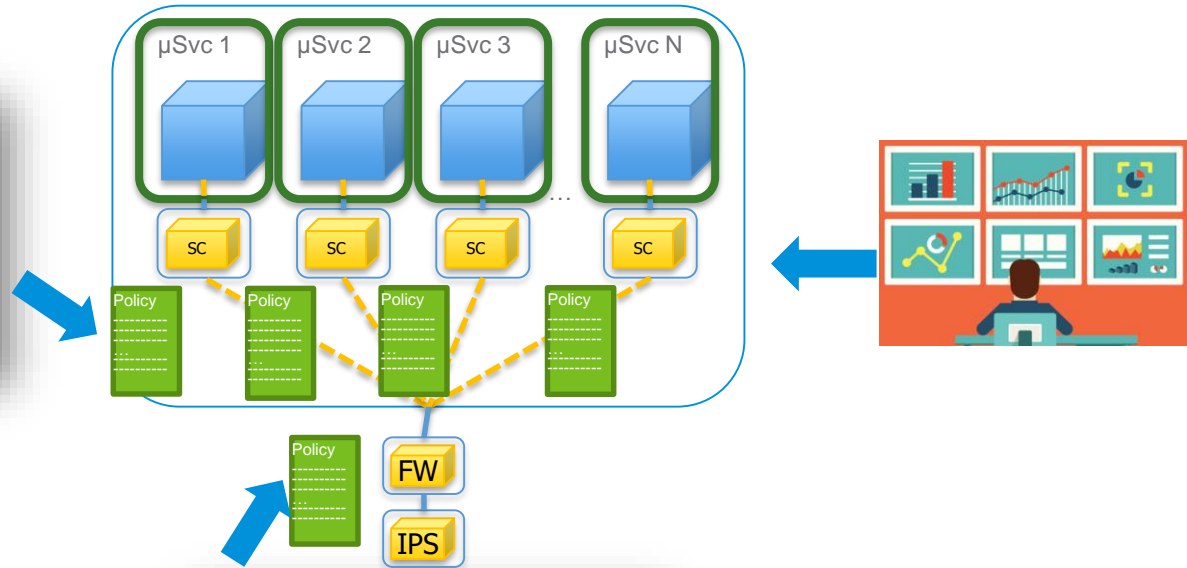
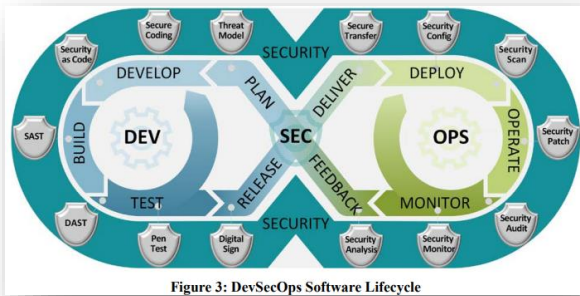
## Tomorrow



<https://lawtomated.medium.com/explainable-ai-all-you-need-to-know-the-what-how-why-of-explainable-ai-dcf2287a9f6c>

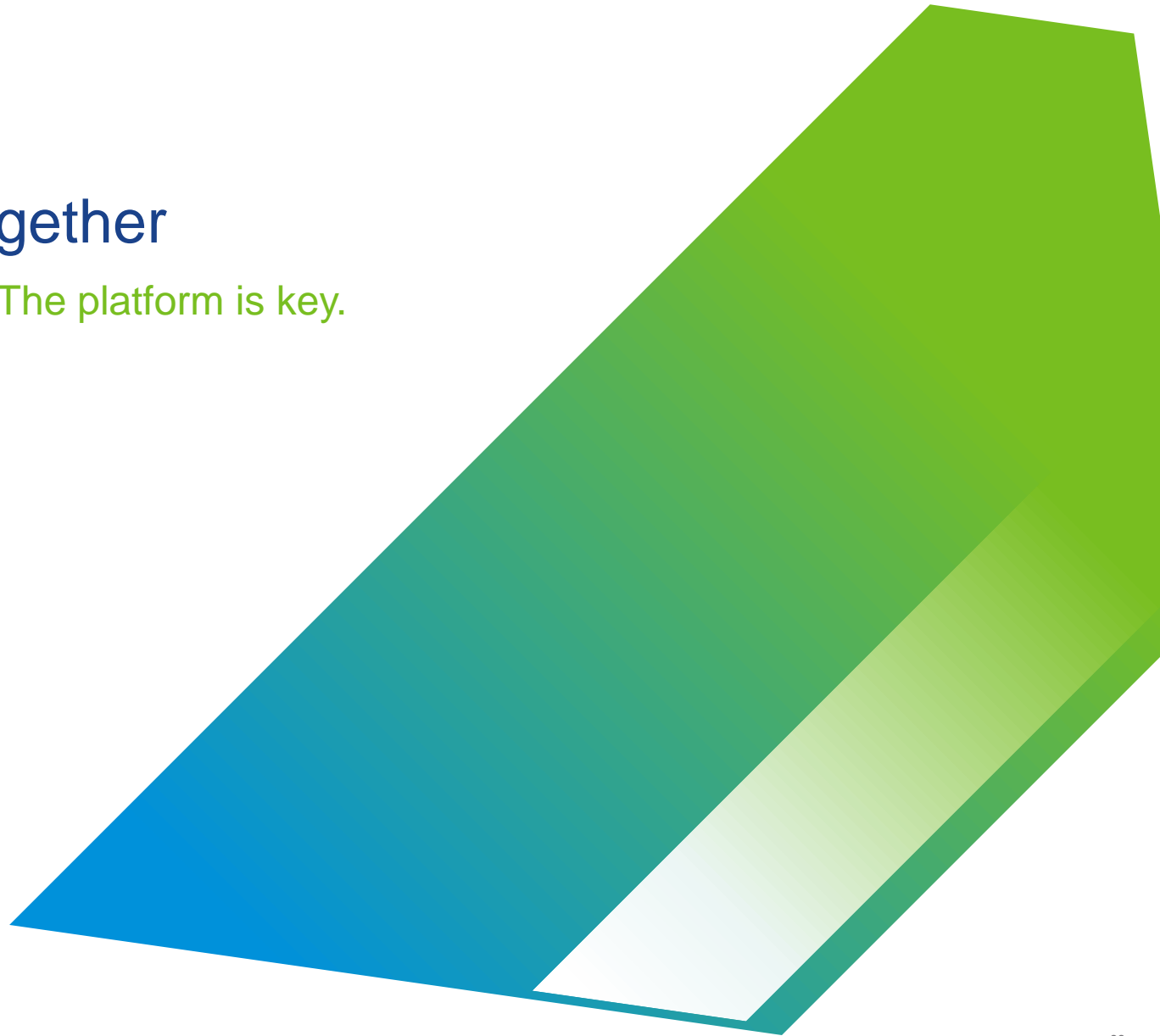
# Enter AI (XAI)

## Context from the Right

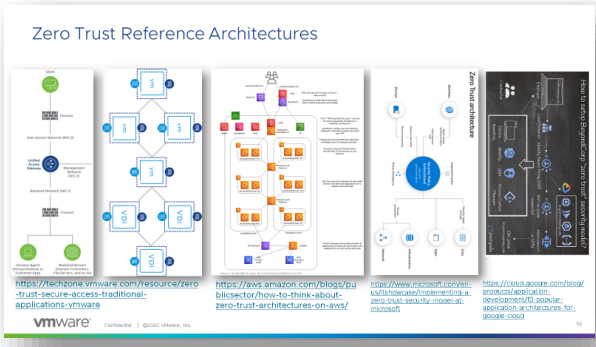
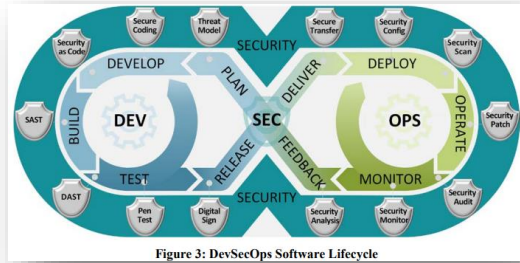
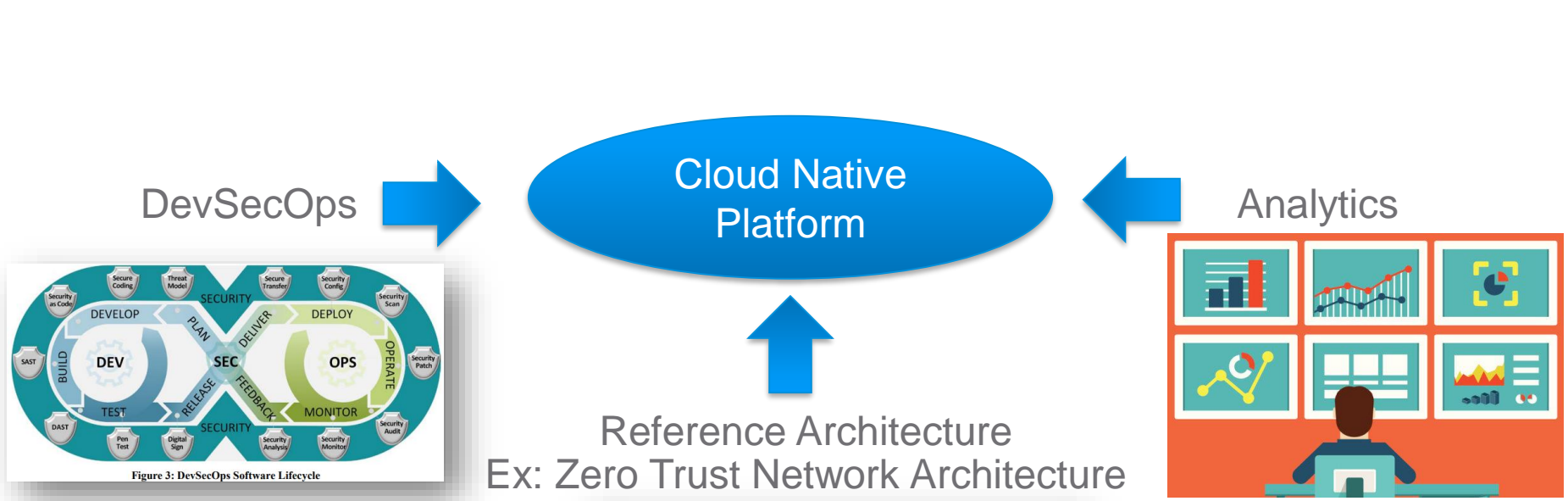


# Putting it all together

Connecting the dots. The platform is key.



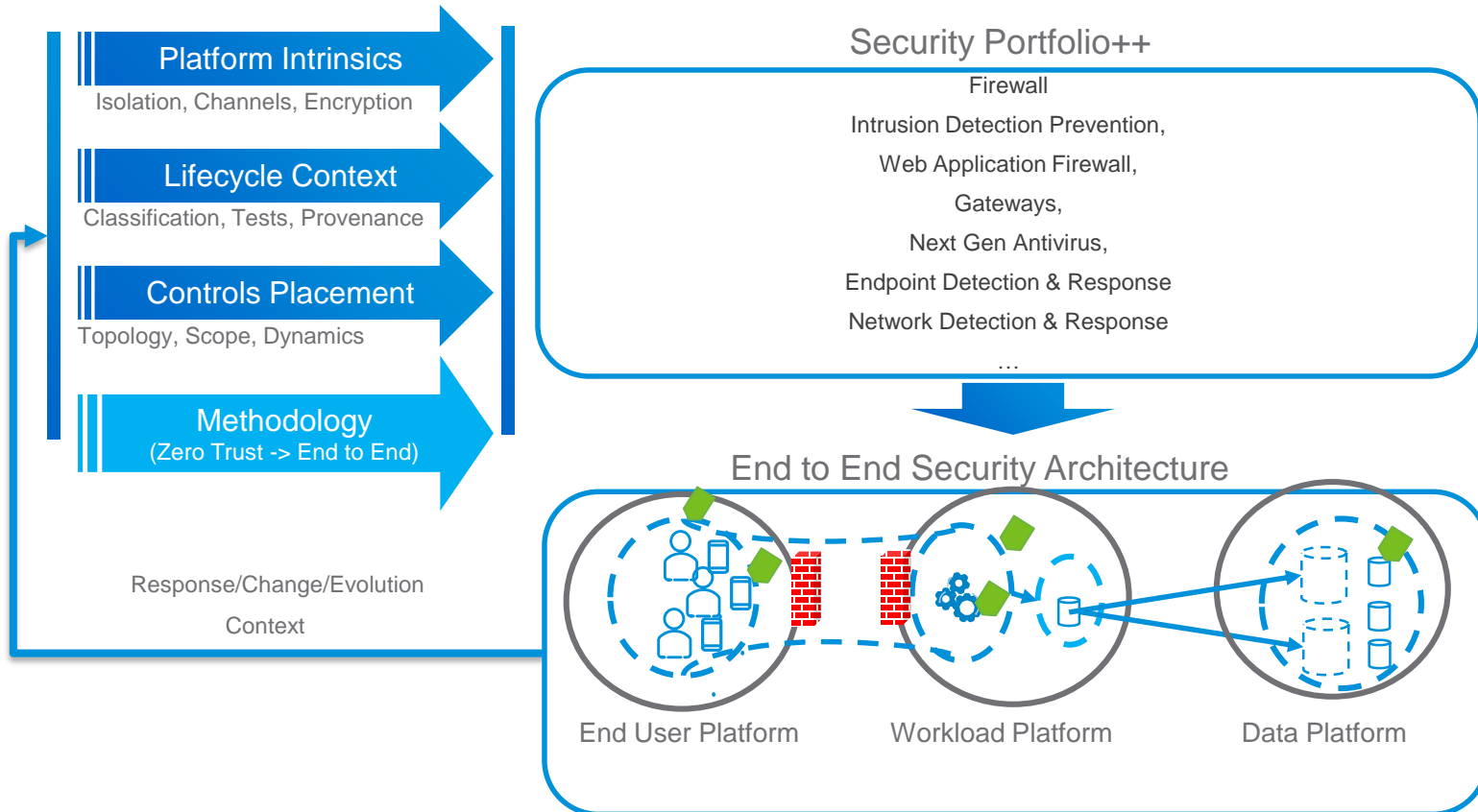
# Only the Hosting Platform Connects all the Pieces





# System Policy and Guardrails

## The Role Of the Platform



# End to End ZT: Aligning Policy across Hosting Contexts

Directional

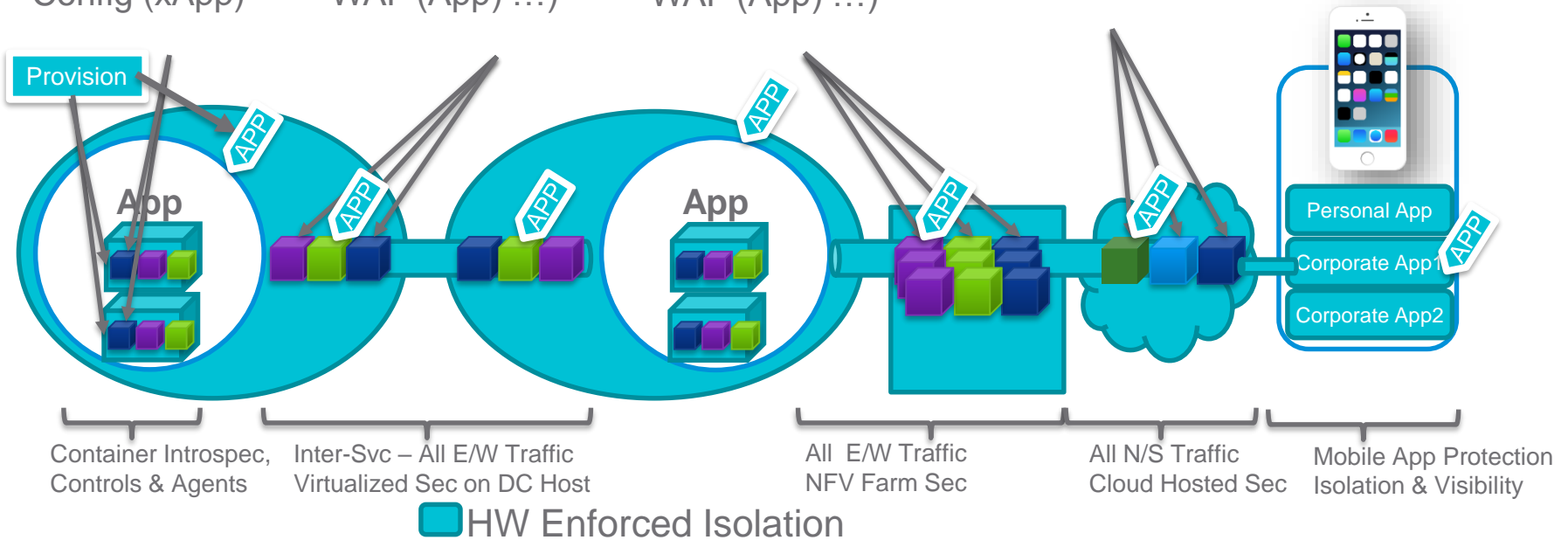
Endpoint Security  
 AV (App)  
 EDR (App)  
 Profile App)  
 Config (xApp)

Service insertion  
 FW (App)  
 IPS (App)  
 NGFW (App)  
 WAF (App) ...)

Service Chaining  
 FW (App)  
 IPS (App)  
 NGFW (App)  
 WAF (App) ...)

Hosted Protection  
 WAF (App)  
 CASB (App)  
 vDDoS (App(s))

Device Policy  
 DLP (App)  
 CASB (App)  
 Access Profile (App)



# What is Happening Now

Connecting the dots. The platform is key.



# NIST: Zero Trust Extension

<https://www.nist.gov/programs-projects/trustworthy-networks-things>

## Trustworthy Networks of Things



News and Announcements  
Associated Products

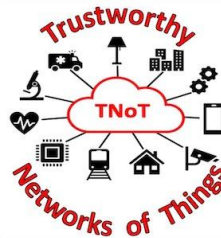
### Summary

NIST is working with industry to design, standardize, test and foster adoption of network-centric approaches to protect IoT devices from the Internet and to protect the Internet from IoT devices.

### DESCRIPTION

Our work focuses on network-centric approaches to improve the security and robustness of large scale deployments of IoT devices.

- The research and development of software-defined networking technologies in support of IoT security.
- The design and IETF standardization of [Manufacturer Usage Description \(MUD\)](#) technologies to enable a scalable and automated means to enforce device specific access control within network switches and routers.
- The design and standardization of technologies to securely "on board" IoT devices on to networks and to provision credentials to local devices.
- The application of automated model checking techniques to verify the security properties of emerging IoT security protocols.
- Research on the application of [zero trust architecture](#) to IoT environments.
- Research on the use of [DNS-based Authentication of Named Entities \(DANE\)](#) as a trust infrastructure for constrained IoT environments.



<https://www.nist.gov/system/files/documents/2021/01/21/Agenda%20SOZTA%20Jan%202027%202021%20DRAFT%20v8.pdf>

## DevSecOps and Zero Trust Architecture in Multi-Cloud DRAFT

**Tetrate**  
*MC: Dr. Michaela Iorga, Senior Security Technical Lead, NIST*

**NIST**  
National Institute of Standards and Technology  
U.S. Department of Commerce

**Wednesday, January 27, 2021**

11:00 am [25] 8:00 am [PST]	<b>Kickoff Keynote</b> <b>Varun Talwar</b> , CEO, Tetrate
11:25 am [20] 8:25 am [PST]	<b>DevSecOps: Benefits and Vision</b> <b>Dr. Ronald Ross</b> , Fellow, NIST
11:45 am [25] 8:45 am [PST]	<b>NIST IR 8313 – Attribute-based Access Control for Microservices-based Applications using Service Mesh</b> <b>Ramaswamy Chandramouli</b> , Senior Scientist, NIST <b>Zack Butcher</b> , Founding Engineer, Tetrate
12:10 pm [15]	<b>Break</b>
12:25 pm [25] 9:25 am [PST]	<b>Zero Trust: Past, Present, and Future</b> <b>Zulfikar Ramzan</b> , Chief Technical Officer, RSA
12:50 pm [25] 9:50 am [PST]	<b>Air Force (AFLCMC/HNCP) Platform One</b> <b>Nicolas M. Chaillan</b> , Chief Software Officer, Air Force Co-Lead, DoD Enterprise DevSecOps Initiative
1:15 pm [25] 10:15 am [PST]	<b>Using Mesh Architecture to support ZTA and DevSecOps</b> <b>Adam Zwickley</b> , Engineer, Tetrate
1:40 pm [55]	<b>Lunch (Breakouts Rooms)</b>
2:35 pm [45] 11:35 am [PST]	<b>Demo: Identity Provisioning in a Service Mesh</b> <b>Ignasi Barrera</b> , Founding Engineer, Tetrate <b>Demo: Federated Sharing of Disparate Database Resources</b> <b>Joshua Roberts</b> , Computer Scientist, NIST
3:20 pm [25] 12:20 pm [PST]	<b>Blockchain-based Secure Software Assets Management (BioSS@M)</b> <b>Andrew Weiss</b> , Lead Architect and Technical Advisor, UMBC
3:45 pm [25] 12:45 pm [PST]	<b>Transitioning to the Mesh</b> <b>Kevin Paige</b> , CISO, Flexport
4:10 pm [15]	<b>Break</b>
4:25 pm [45] 1:25 pm [PST]	<b>Panel: Ask the Experts</b> Join us for an exhilarating fireside chat with adopters and experts of cutting-edge technologies such as ZTA, multi-cloud, service mesh and DevSecOps. Get engaged with our guests by bringing forward your concerns and questions.  <b>Moderator:</b> <b>Dr. Michaela Iorga</b> , Senior Security Technical Lead, NIST <b>Adopters:</b> <b>Andre' Mendes</b> , Chief Information Officer (Acting), DoC <b>Sorin Nastea</b> , Associate Director of Informatics Architecture, FDA <b>James Younger</b> , DHS <b>Experts:</b> <b>Nicolas M. Chaillan</b> , Chief Software Officer, Air Force <b>Zack Butcher</b> , Founding Engineer, Tetrate
5:10 pm [10]	<b>Closing Remarks – Matthew Scholl</b> , Chief, Computer Security Division, NIST

# ISACA Organization – 200,000 Practitioners - 1 Vocabulary

ISACA

Home / Enterprise / Enterprise Credentialing

## CREDENTIALING

More Than 200,000 Practitioners and Managers Have Earned ISACA Certifications.

Among the world's most trusted information systems and cybersecurity professionals serving enterprises worldwide.

### Certify Your Team

Our globally recognized credentials include:

6 Certifications:

- CISA
- CRISC
- CISM
- CGEIT
- CSX-P
- CDPSE

Additionally, ISACA also offers:

- COBIT
- CSX
- CYBER SECURITY AUDIT
- IT RISK FUNDAMENTALS

- 8+ Cyber-skills-affirming certificates for cybersecurity practitioners.
- 2 Certificates that confirm the cybersecurity know-how of practitioners in any field of information systems:
  - CSX Cybersecurity Fundamentals Certificate
  - Cybersecurity Audit Certificate
- 2 Certificates that prove ability to implement effective IT governance and maximize the value of information and technology assets:
  - COBIT® 2019 Foundation Certificate
  - COBIT 2019 Design & Implementation Certificate

See how certifying can really energize your organization.

Audit  
Risk  
Cybersecurity  
Compliance

- Certification
- CPE
- Platform

## CMMI & CMMC

Accelerate Your Path to Cybersecurity Maturity Model Certification

The Department of Defense's (DoD's) Cybersecurity Maturity Model Certification (CMMC) is foundationally built, in part, on the CMMI model and methodology. ISACA is actively working with the DoD, the CMMC Accreditation Body (AB) and other stakeholder organizations to advance the success of the CMMC ecosystem and help improve the cybersecurity posture and resilience of the defense industrial base (DIB).

### Are you overwhelmed on your path to CMMC?

The CMMC Defense Federal Acquisition Regulations (DFARS) requirement is now law and the government is starting to rollout contract requirements for CMMC in upcoming contracts. We can jump start your CMMC efforts with our gap analysis.

Our **three-step gap analysis program** will simplify and accelerate your preparation. **Contact us** today to schedule!

- 1 Facilitated Assessment**  
A CMMC-trained Lead Assessor facilitates **interactive review** in a workshop-like format, leveraging the CMMC spreadsheet characterization and tracking tool as an information-gathering framework with your team.
- 2 Gap Analysis Roadmap**  
We **provide a visual roadmap** to help you prioritize and systematically address CMMC gaps, based on 30+ years of similar best practice experience with CMMI.
- 3 Customized Report**  
We provide you with **actionable results** you can use to make your prioritized CMMC improvements. We note process strengths and weaknesses categorized by CMMC domains to target clear and sustainable improvement.

# ISACA Auditor CPEs

“Zero Trust” in all Content

Dashboard showing a list of CPE courses and conferences, including:

- GRC Governance, Risk and Control (GRC) Conference (3 - 11 August 2021)
- ISACA Conference Europe 2021 | IT Conference
- What Background Makes a Good CPO?
- CPE on Demand: All Access - 34 podgth sessions
- ISACA Virtual Training Week November: AI and Machine Learning
- ISACA Virtual Training Week November: Challenge Communication in Challenging Communication Parameters, Negotiation & Conflict Management
- ISACA Virtual Training Week November: Data Analytics
- CSM Online Review Course
- CSA Online Review Course
- Latin America CACS 2021 Conference
- ISACA Conference North America 14-18 May 2021
- VIRTUAL - Cloud Computing for Auditors: March
- Denver Training Week: CISA Bootcamp
- Denver Training Week: CISM Bootcamp
- Denver Training Week: CDPSE Bootcamp

## CPE on Demand: Security

Online Course

Online courses can be accessed from the Learning Access tab of your MySACA account.

Format	CPE	Duration
Online	5.5	5.5 hours

Member Price:	\$385.00
Non-Member Price:	\$485.00
Your Price:	\$385.00

[Add to Cart](#) [View Shopping Cart](#)

The CPE on Demand: Security collection provides timely, valuable insights for IT Audit, Security, and Risk professionals, and enables you to learn on your schedule while earning up to 5.5 ISACA CPEs. Access to the entire collection of recordings - each recorded at ISACA's North America CACS 2020 Conference - is unlimited for a 90-day period and includes downloadable presentation decks.

Session titles include:

- Securing 5G: Data Risk Management for the Future of Wireless Technology
- Extending Zero-Trust to the Endpoint: Security Anywhere
- Effective Automation for Third Party IT Security Risk Management
- The Holistic CSO: 7 Critical Factors to Success
- Effective Reliance on Other Assurance Partners - IT Audit and Information Security

Product Code: LMS\_NAC20S  
[Hide Full Description](#)

## CPE on Demand: All Access

Online Course

Online courses can be accessed from the Learning Access tab of your MySACA account.

Format	CPE	Duration
Online	37	37 hours

Member Price:	\$1,850.00
Non-Member Price:	\$2,000.00
Your Price:	<a href="#">Log In To View Your Price</a>

[Log In](#)

The CPE on Demand: All Access collection provides timely, valuable insights for IT Audit, Security, and Risk professionals, and enables you to learn on your schedule while earning up to 37 ISACA CPEs. Access to the entire collection of recordings - each recorded at ISACA's North America CACS 2020 Conference - is unlimited for a 90-day period and includes downloadable presentation decks.

Session titles include:

- Privacy Assurance - Growing Need for Tools
- Difficult Clients and Ficing Problem Relationships
- Compliance leading the way during a Pandemic
- The Current Landscape of Cybersecurity and Privacy Laws
- Integrate Enterprise SoD Rules with Identity and Access Management
- Agile, DevOps and Compliance
- Machine Learning Monitoring Compliance and Governance
- Industry 4.0 - Future-Proofing Your Career
- Transforming IA with Lean & Agile Techniques
- The Virtual CSO: The Future of Cyber Strategy?
- Securing 5G: Data Risk Management for the Future of Wireless Technology
- Extending Zero-Trust to the Endpoint: Security Anywhere
- Effective Automation for Third Party IT Security Risk Management
- The Holistic CSO: 7 Critical Factors to Success
- Effective Reliance on Other Assurance Partners - IT Audit and Information Security
- Shifting to the Offensive - Enabling your Teams for Cyber Threat Hunting
- From Surviving to Thriving as an "Only" in Cybersecurity
- Supply Chain Threats in E-commerce
- How Hackers Profit from Common Cloud Services
- COVID-19 Cyberattacks
- Point in Time Assessments Are Over - A Technical Approach to Addressing 3rd Party Risk
- Effective Automation for Third Party IT Security Risk Management
- Getting Granular with Vendor Risks: Adding Business Context & Mapping Data Flows
- Risk Managed Partnerships: Being/Finidng A Secure Partner
- 9 Objectives to Manage Pandemic Risk
- COBIT 2019 Spotlight - Governance and Management in a High Velocity Environment
- The NIST Cybersecurity Framework Best Practices
- Your Cloud Environment Passed the SOX audit, but is it Really Secure?
- What Does It Take for Integrated Risk Management to Slick?
- Managing Risk and Building Resilience in the New Normal
- 39 Ways to Work with The Board
- Transform Your Data: The Journey to Realize Your RPA And Data Analytic Dreams
- See What You've Been Missing! A View Through Audit Analytics
- Fighting Fraud with Data Analytics and IA

Product Code: LMS\_NAC20ALL

# ISACA: Global Definition








## Transform From Trust to Zero Trust at Asia CACS 2020

Author: ISACA  
Date Published: 23 November 2020



---

This year, the COVID-19 pandemic and its resulting physical distancing requirements have made the idea of congregating with other professionals to explore industry topics and insights seem like a thing of the past. Yet the ISACA® community can still gather virtually to share insights and experiences through the online-only Asia CACS 2020 virtual conference. Asia CACS, taking place 11-12 December 2020, is designed to teach participants how to go from "Trust to Zero Trust."

The conference will have 3 parallel tracks available, exploring the following topics:

- Track 1: Assurance**—The assurance path will include discussions about alignment to trust principles in safeguarding an organization, zero trust policy and its management, and how to audit a zero trust model.
- Track 2: Defense**—This track will explore zero trust architecture, the role of microsegmentation in zero trust and access management in trust verification.
- Track 3: Oversight**—The oversight track will focus on governance of the zero trust model, risk management in a zero trust framework and performance measurement in adherence with zero trust security vs. traditional security models.

Participants who attend can earn up to 14 continuing professional education (CPE) credits throughout the 2-day conference. An additional 7 CPE credits will be available to earn through the available pre-conference workshops.

To learn more about Asia CACS 2020 and register for the conference, visit the [ISACA Asia CACS Conference](#) page of the ISACA website.

## CACS Global Auditor Guidance

## Zero Trust Definition – A Model

### Zero Trust Maturity Model

It is quite challenging to identify a maturity model for zero trust because there is no one size that fits all. Every organization is unique, operating in different industries with varied compliance requirements. As discussed, business priorities define the zero trust architecture and migration priorities. Figure 4 shows the effort to develop a yard stick that generally satisfies the basic requirements. It provides indicative information that can be used for assessment.

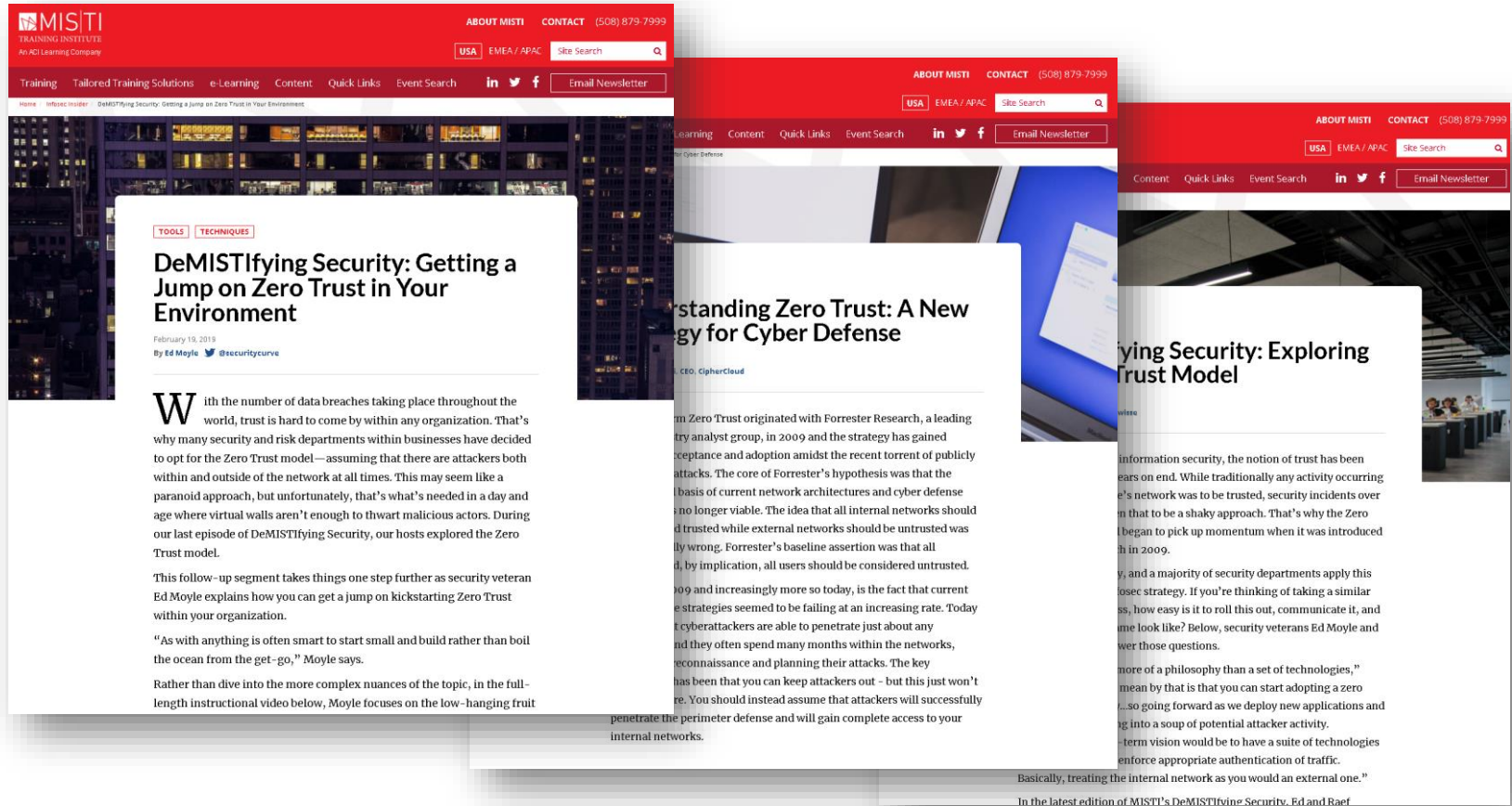
**Figure 4—Zero Trust Maturity Model**

Zero Trust Elements	Initial	Developing	Defined	Managed	Optimizing
Data	Data sources and workflows are not formally documented. Access is granted on perimeter device controls.	Data sources, workflows and classification scheme are documented. Data are classified and labeled manually.	Automated content-based data classification, labelling and protection is in place.	ML for classification, labelling and protection is used. Data loss prevention (DLP) is governed by workflows and potential attack vectors.	Periodic review of ML algorithm configuration is undertaken to ensure alignment with business priorities.
Communication	No documented policy for securing communications. Network traffic is encrypted for outgoing with static traffic filtering.	Formal network security policy is in place. Traffic is encrypted, but not consistently applied. Servers and clients are in separate network segments.	All traffic is secured based on protect surface. Network segmentation is in place within the server's network segment. Logs are maintained and reviewed.	Logs are aggregated centrally and reviewed for trend analysis. Deeper dynamic microsegmentation is in place based on protect surface.	Continuous analytics through ML are used to identify attack vectors and improvements in network security.
User	Basic IAM, auditing at the system level and isolated single sign-on system (SSO) are used.	IAM with MFA, enterprise level SSO, auditing at system level with some integration to central logging repository are in place.	Automated IAM integrated with enterprise-wide systems is in place, including session management, reauthentication, reauthorization and user activity logging	IAM integrated with other components such as device management, threat intel and mitigation, ML, and rapid incident response tools is used.	ML capability is used for session management based on various threat vectors. Periodically review reports from IAM and fine-tune IAM configurations and integration.
Devices	Devices are secured by antimalware, active directory group policies. Only authorized devices can connect to the enterprise network.	A device management tool is in place, which ensures a device's compliance with established policies before it is connected to the enterprise network.	Devices are protected through endpoint detection and response (EDR) technology with real-time threat intel and mitigation. Non-enterprise devices can connect to a separate network segment with limited Internet connectivity.	Access control is managed through the user and device compliance status. Continuous device monitoring for anomaly detection is used.	Proactive threat hunting, investigation and mitigation leveraged on ML and advanced analytics is employed.
Infrastructure	Manual processes for managing permissions across servers and virtual machines (VMs) are used. Applications are open to any authorized user in the network.	Automated privileged access management integrated with session workflow management is in place. User to application access is secured based on defined workflows. Cloud access security brokers (CASBs) are used.	Unauthorized deployments are identified and alerts are triggered. Workloads are monitored for anomalies. Every workload has an application tag.	User and resource sessions are tagged and continuously monitored. Applications are secured through least privileges, SSO and user sessions are continuously monitored.	Dynamic least privilege rules are coupled with AI to provide granular control across all workloads.

### Zero Trust Adoption Trend

A 2020 zero trust progress report surveyed more than 400 cybersecurity decision-makers, ranging from technical executives to IT security practitioners and representing a balanced cross-section of organizations of varying sizes across multiple industries. According to one survey report, confidence among security professionals is mixed. Fifty-three percent have confidence, whereas 43 percent are still doubtful in applying a zero trust model in their architecture. This mixed reaction can be understood by the fact that 40 percent of zero trust implementations resulted in an increase in budget, whereas 45 percent of budgets remained the same, and only 15 percent of organizations witnessed a decrease in their budget. Seventy-two percent of organizations plan to assess or implement zero trust capabilities in some capacity in 2020 to mitigate growing cyber risk.<sup>11</sup>

# MISTI: Just Getting Started





EN

From January 2019 to April 2020

## Emerging trends

ENISA Threat Landscape

**06\_Reduction of false positives.** This long waited promise is key in the future of the cybersecurity industry and in the fight against the alarm fatigue.

**07\_Zero-trust security strategies.** With an increasing pressure on IT systems from new business requirements such as remote working, digitalization of the business model and data sprawl, zero trust is seen by many decision makers as the solution de facto to secure corporate assets.

**08\_Enterprise cloud migration errors.** With many businesses migrating their data to cloud-based solutions, the number of configuration errors will increase exposing data to a potential breach. Cloud service providers will address the issue by implementing systems that identify these type of errors automatically.

**09\_Hybrid threats.** New *modus operandi* adopt virtual and physical world threats. The spread of disinformation or fake news for example, is a key fixture of the hybrid threat landscape. The EUvDisinfo™ is a flagship project of the European External Action Service's East StratCom Task Force established to address the disinformation threat.

**10\_The attractiveness of the cloud infrastructure as a target will grow.** The increasing reliance on public cloud infrastructure will surge the risk of outages. Misconfiguration of cloud resources is still the number one cause for cloud attacks, but attacks aiming directly at the cloud services providers gaining popularity among hackers.



## DSP

Technical Guidelines for the implementation of minimum security measures for Digital Service Providers

enisa  
EUROPEAN  
CYBERSECURITY  
AGENCY

Technical guidelines for the implementation of minimum security measures for DSPs  
December 2020

### 2.12 SO 10 – Access control to network and information systems

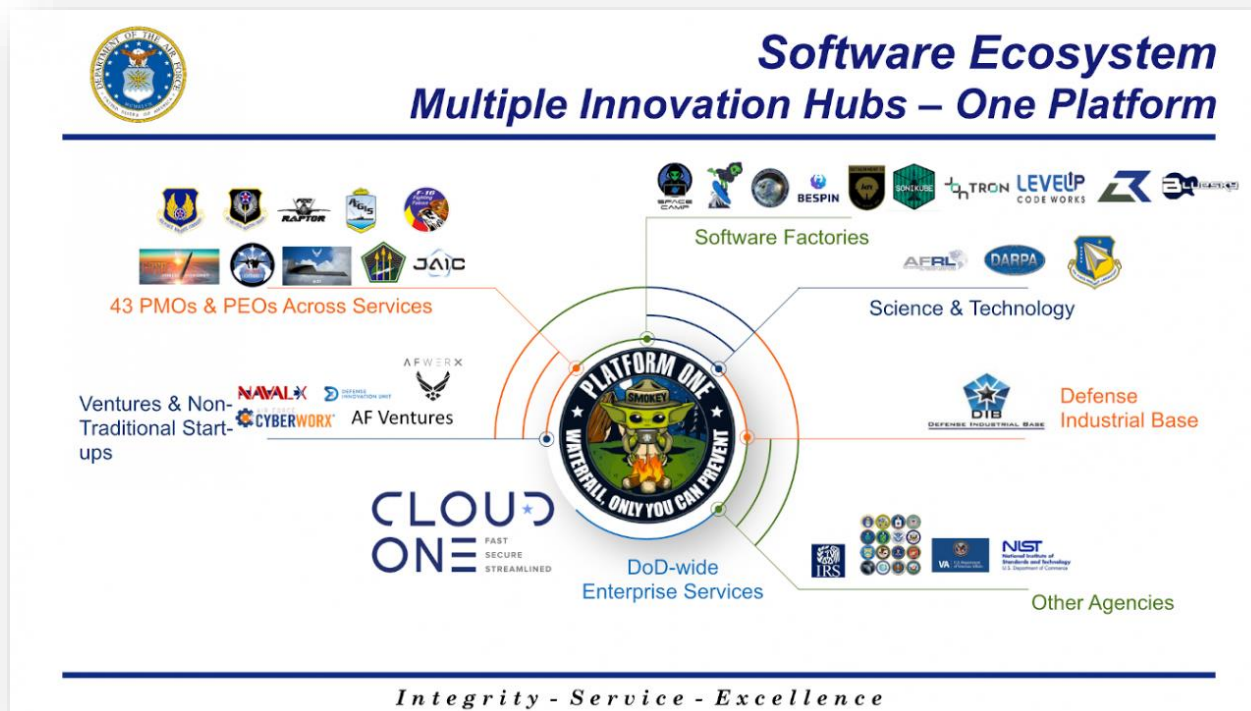
**Description**  
The DSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	<ul style="list-style-type: none"> <li>Users and systems have unique IDs and are authenticated before accessing services or systems.</li> <li>Implement (logical) access control mechanism for network and information systems to allow only authorized use.</li> </ul>	<ul style="list-style-type: none"> <li>Access logs show unique identifiers for users and systems when granted or denied access.</li> <li>Overview of authentication and access control methods for systems and users.</li> <li>Documented methods of access control containing at least:                             <ul style="list-style-type: none"> <li>Authentication type;</li> <li>Authorization schema.</li> </ul> </li> </ul>
2	<ul style="list-style-type: none"> <li>Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights.</li> <li>Based on the results of risk analysis, choose the relevant authentication mechanisms which are deemed relevant to different types of access.</li> <li>Monitor access to network and information systems, have a process for approving exceptions and registering access violations.</li> <li>Security functions are restricted to the least amount of users necessary to ensure the security of the information system.</li> <li>Track and monitor privileged accounts by validating their creation, use of specific authentication methods and regular reviews.</li> </ul>	<ul style="list-style-type: none"> <li>Access control policy including description of roles, groups, access rights, procedures for granting and revoking access.</li> <li>Different types of authentication mechanisms for different types of access, e.g. Single Sign-On, two-factor authentication, multi-factor authentication, etc. (including remote and WiFi mechanisms)</li> <li>Log of access control policy violations and exceptions, approved by the security officer.</li> <li>List of authorized users who can access to security functions.</li> <li>Logs from privileged accounts' usage.</li> <li>Network isolation and implementation of segmented network security zones that limit the impact of a malware incident</li> <li>Segregation of duties control matrix.</li> <li>Access control matrix.</li> </ul>

# PlatformOne: Standardized DevSecOps as a Service

<https://software.af.mil/team/platformone/>



# ReCap

- Cloud Native Architectures, DevSecOps, Zero Trust and Security AI have not been “silver bullets” in isolation ... and are unlikely to be in the future
- At the intersection between these innovations, truly interesting things begin to happen
- The hosting platform is in a position to connect these mutually beneficial technologies
- Some examples of evolution in this direction
  - Standards
  - Public Clouds



## Questions?

Dennis R Moreau, PhD  
Sr Engineering Architect  
Advanced Technology Group  
Office of the CTO  
VMware  
[dmoreau@vmware.com](mailto:dmoreau@vmware.com)

# Thank You



# INFORMATION SECURITY AWARENESS TRAINING STANDARD FORM INSTRUCTIONS

## INFORMATION SECURITY AWARENESS TRAINING STANDARD FORM INSTRUCTIONS

**Identify your training solution:** Mark your agency's proposed solution to meet the training requirements identified in A, B, C, D and E.

- ( A ) Core requirements;
- ( B ) Policy review and acceptance;
- ( C ) Role-based training;
- ( D ) Other regulatory requirements;
- ( E ) Phishing exercise;
- ( F ) Additional training where required

# SEC527 – INFORMATION SECURITY AWARENESS TRAINING STANDARD UPDATE

## SEC527 – INFORMATION SECURITY AWARENESS TRAINING STANDARD

### ORCA COMMENTS

CSRM would like to thank everyone who submitted comments or suggestions for the SEC527 Information Security Awareness Training Standard. The comments have been reviewed and will be incorporated accordingly.

### What's next?

SEC527 will be send to Nelson for review and approval. Any suggested changes by Nelson will be incorporated and a final copy of the standard will be posted on the VITA website under **ITRM Policies, Standards & Guidelines/Tools and Templates**.



## SEC527 – INFORMATION SECURITY AWARENESS TRAINING STANDARD CURRICULUM – ROLE-BASED TRAINING COURSES

The following role based training courses are now available in the COVLC/LMS

- 1231-Data owner
- 1232-Data custodian
- 1233-System administrator
- 1230-Agency head
- 1020-System owner overview
- 1021-System owner risk
- 1301-System owner 1

***If you have issues accessing the courses, contact your agency LMS Administrator***

## Agency information security awareness training solutions form

In accordance with the Code of Virginia, section 2.2-2009 sub-section I, all Commonwealth of Virginia agencies shall report the type of cybersecurity awareness training solution that they will administer to their employees. Training solutions (i.e. software, classroom or other) are required to meet the curriculum requirements identified in this document.

This information is to be submitted to VITA no later than Feb. 28, 2021 and every Jan. 31, thereafter.

Please complete the following:

**Agency name:** [click or tap here to enter text.](#)

**Information security officer:** [click or tap here to enter text.](#)

		InfoSec	KnowB4	SANS	Awareity	Security Mentor	*Other Software	DHRM LMS	Classroom or Other Method	VITA
<b>A</b>	Core Requirements (required):									
<b>B</b>	Policy Review & Acceptance (required):									
<b>C</b>	Role Based Training (required):									
	System Owner Training									
	Data Owner Training									
	System Admin Training									
	Data Custodian Training									
	Agency Head Training									
<b>D</b>	Regulatory Training (required as needed):									
	Federal Tax Information (FTI)									
	Health Insurance Portability & Accountability Act (HIPAA)									
	Criminal Justice Information Services (CJIS)									
	FERPA									

Identify training solution: please mark your agency's proposed solution to meet the training requirements identified in A, B, C and D.

	Social Security Training								
	Payment Card Information (PCI)								
	Personal Health Information (PHI)								
E	Phishing Exercise (required)								
F	Additional Training (optional)								

\*Other software: If you are planning to use a software solution other than: Infosec / KnowB4 / SANS / Awareity / Security Mentor, please indicate it here. The use of any other training solution must be approved in advance.



## A - CORE REQUIREMENT COURSES

**Separation of duties**  
**Security incidents**  
**Proper disposal of data storage media**  
**Proper use of encryption**  
**Access controls, secure passwords**  
**Working remotely**  
**Intellectual property rights**  
**Security of data**  
**Phishing and email**  
**Social engineering**  
**Mobile devices**  
**Ethics**

**Least privilege identifying and reporting**  
**Privileged access**  
**Insider threat**  
**Cloud services**  
**Browsing safely**  
**Physical security**  
**Hacking**  
**Personal identifiable information (PII)**  
**Privacy**  
**Social network**  
**Malware**

## B - POLICY REVIEW AND ACCEPTANCE COURSES

***Require documentation of IT system users' acceptance of the agency's security policies. Information Security Awareness training must include policy review and acceptance***

---

**Acceptable use - All users of IT systems must agree to the agency's acceptable use policy.**

**Remote access policy - All users of IT systems must agree to the agency's remote access usage and/or Telework Policy.**

**Other applicable policies - Users of IT systems must review and agree to comply with any applicable agency security policies.**

## D - OTHER REGULATORY REQUIREMENT COURSES

*Agencies must provide training for all regulatory or contractual requirements that affect IT users.  
Agencies need to decide the appropriate level of regulatory training that is required for its users*

---

**Federal Tax Information (FTI)**  
**Health Insurance Portability and Accountability Act (HIPAA)**  
**Criminal Justice Information Services (CJIS)**  
**Family Educational Rights and Privacy Act (FERPA)**  
**Social Security Administration Training (SSA)**  
**Payment Card Information (PCI)**  
**Federal PII**  
**Personal Health Information (PHI)**

## E - PHISHING EXERCISE

**Agencies are required to conduct a phishing exercise or phishing training with their employee / contractor users. A phishing campaign will help identify if users can successfully recognize, avoid and report phishing attempts that may occur.**

**VITA will provide assistance in developing a phishing campaign for your agency if needed.**



## F - ADDITIONAL TRAINING WHERE REQUIRED

**Agencies should offer training that goes beyond the required curriculum items when necessary in the agency's environment. The items below are a few suggested additional training that agencies should consider for their employees where appropriate:**

- *Senior leadership training*
- *New employee orientation training*
- *Creating a Cybersecure home*
- *Etc.*

## LOCATION OF FORM ON VITA'S WEBSITE

<https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>

### **Tools and Templates**

[Agency Security Awareness Training Solution Form](#)

**This form is also now available in Archer**

Virginia Information Technologies Agency | Archer App

ENTERPRISE GOVERNANCE RISK and COMPLIANCE

Risk Management | Enterprise Management | Task Management | Threat Management | CSRM Analyst Workspace | Reports

### Agency : Virginia Information Technologies Agency

EDIT VIEW

First Published: 8/6/2013 8:43 AM Last Updated: 2/1/2021 10:02 AM

Record 98 of 116

**ABOUT**

**NATIONWIDE CYBER SECURITY REVIEW 2020**

Questionnaire ID  
[583857](#)

**SECURITY AWARENESS TRAINING QUESTIONNAIRE** [Add New](#)

Questionnaire ID	Year
<a href="#">601854</a>	2021

**GENERAL INFORMATION**

Agency Name: Virginia Information Technologies Agency  
Agency Acronym: VITA  
Web Site: <http://www.vita.virginia.gov>  
Partnership Full Service Yes  
Customer:

The screenshot shows a web browser window with the following details:

- Browser Tabs:** Virginia Information Technolog..., Inbox (1,810) - tina.gaines@vita..., RSA - Commonwealth Security and Ris...
- Address Bar:** itgrcs.vita.virginia.gov/apps/ArcherApp/Home.aspx
- Page Header:** VIRGINIA IT AGENCY ENTERPRISE GOVERNANCE RISK and COMPLIANCE. Includes a search bar and user profile 'occ44262'.
- Navigation Menu:** Home, Risk Management, Enterprise Management, Task Management, Threat Management, CSRM Analyst Workspace, Reports.
- Section Title:** Security Awareness Training Questionnaire : 601859
- Buttons:** EDIT, VIEW, SAVE, SAVE AND CLOSE.
- Metadata:** Created Date: 2/2/2021 10:01 AM Last Updated: 2/2/2021 10:01 AM. 0 of 26 Completed.
- Form Fields:**
  - INSTRUCTIONS:** (Collapsed)
  - GENERAL INFORMATION:** Questionnaire ID: 601859, Submitted by: Tina Harris-Cunningham, Year: 2021, Agency: Virginia Information Technologies Agency.
  - Planned Training Solutions:** Verification and Compliance.
  - PLANNING STATUS:** Plan Submission Status, Plan Submission Date, Plan Review Status, Plan Review Date.
  - CURRICULUM REQUIREMENTS:** (Collapsed)
- Footer:** Version 6.8 P4, Windows taskbar with system clock 10:02 AM 2/2/2021.

## Security Awareness Training Questionnaire : 601859

EDIT VIEW SAVE SAVE AND CLOSE

Created Date: 2/2/2021 10:01 AM Last Updated: 2/2/2021 10:01 AM  
0 of 26 Completed

### ▼ CURRICULUM REQUIREMENTS

**Core Requirements:** Indicate which solution your agency will be using in order to fulfill the core requirements for training.

- InfoSec
- KnowB4
- Awareness
- SANS
- Security Mentor
- Other

### ▼ POLICY REVIEW AND ACCEPTANCE

**Acceptable Use Policy:** Indicate which solution your agency will be using in order to provide acceptable use policy training.

- Awareness

## QUESTIONS?

[Tina.gaines@vita.virginia.gov](mailto:Tina.gaines@vita.virginia.gov)

[Edward.miller@vita.virginia.gov](mailto:Edward.miller@vita.virginia.gov)



# UPCOMING EVENTS

## IS ORIENTATION

The next IS Orientation will be held on

March 31, 2021

Presenter: Marlon Cole (CSRM)

Registration link:

<https://vita2.virginia.gov/Events/chooseSession?MeetingID=10>



**VIRTUAL INFORMATION  
SECURITY CONFERENCE  
JUNE 24, 2021  
MORE DETAILS WILL BE  
FORTHCOMING**

## MARCH 2021 ISOAG

March ISOAG Meeting  
March 3 from 1- 4 p.m.  
Webex

- Manju Generiwala, Department of Treasury
- Michael French, FBI
- Jennifer Whitty, Google



**THANK YOU FOR  
ATTENDING**

