How to prioritize security controls for situational awareness in AWS
Today's speakers

Sounil Yu  
Creator of the Cyber Defense Matrix

Josh Thurston  
Sr. Category Lead, Security at AWS

Sagar Khasnis  
Partner Solutions Architect at AWS
Today’s Agenda

• What is situational awareness and why is it important
• How to attain higher levels of situational awareness
• Scenarios/examples of improved situational awareness
• Relevant AWS services and solutions in AWS Marketplace
• Customer success stories
Leveraging Four Types of Awareness to Secure Your AWS Environment

SOUNIL YU
Defenders need cyber situational awareness to mitigate the loss or compromise of assets

**Situational awareness** is defined as the “perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status”¹

But we face three key challenges in attaining cyber situational awareness

Faulty visibility

Faulty perception

Faulty comprehension

¹Wikipedia’s definition of situational awareness adapted from Mica R. Endsley’s, “Toward a Theory of Situation Awareness in Dynamic Systems”, 1995
Visibility vs Perception vs Comprehension vs Projection

Visibility

Perception

Faulty Visibility

Faulty Perception

Faulty Comprehension

Comprehension Verdict: Bad

Projection: Lateral Movement

Verdict: Bad

Faulty Comprehension
To discover blind spots and overcome challenges in attaining higher levels of situational awareness, frameworks are helpful.
The Cyber Defense Matrix is an adaptation of the CSF

https://cyberdefensematrix.com

<table>
<thead>
<tr>
<th>Degree of Dependency</th>
<th>Technology</th>
<th>Process</th>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Left & Right of Boom: Structural vs Situational Awareness

<table>
<thead>
<tr>
<th>Devices</th>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Structural Elements</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pre-Event Structural Awareness</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Situational Elements</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Post-Event Situational Awareness</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Critical Asset Inventory**
- **Identity attributes**
- **Known weaknesses from vuln scans**
- **Expected behaviors / interactions**
- **Threat landscape**

- **Evidence of vulnerability exploitation**
- **Unexpected state or behavioral changes**
- **Meaning of changes**
- **Impacted assets**

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

Sponsored by: 📚 [aws marketplace](https://aws.amazon.com/marketplace)

[@sounilyu](https://twitter.com/sounilyu)
## Asset Specific Structural and Situational Awareness

<table>
<thead>
<tr>
<th>Degree of Dependency</th>
<th>Technology</th>
<th>Process</th>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>Pre-Event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>Identify</td>
<td>Protect</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Identify**: Pre-Event Structural Awareness
- **Protect**: Post-Event Situational Awareness
- **Detect**: Post-Event Situational Awareness
- **Respond**: Post-Event Situational Awareness
- **Recover**: Post-Event Situational Awareness
<table>
<thead>
<tr>
<th>Devices</th>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Degree ofDependency</td>
<td>Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Environmental and Contextual Awareness

- Environmental Awareness
- Contextual Awareness

Identify, Protect, Detect, Respond, Recover

Sponsored by: SOUNIL YU

@sounilyu

Sponsored by: AWS Marketplace

@sounilyu
Bolstering Situational Awareness

<table>
<thead>
<tr>
<th>Devices</th>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Environmental Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td>Structural Awareness</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Degree of Dependency

- Technology
- Process

People

- Contextual Awareness
- Situational Awareness
- Environmental Awareness
- Structural Awareness
- Environmental Awareness
- Contextual Awareness
Bolstering Situational Awareness: Insider Threat

- Devices
  - Identify
  - Environmental Awareness
- Applications
  - Protect
  - Structural Awareness
- Networks
  - Detect
  - Contextual Awareness
- Data
  - Respond
  - Situational Awareness
- Users
  - Recover
  - Degree of Dependency
  - Technology
  - Process
  - People

Sponsored by: SOUNIL YU

@sounilyu
Four Types of Awareness

**Structural**
- For a specific asset, what are its inherent weaknesses
- What attributes provide verifiable authenticity of its identity
- What is the expected behavior of the asset?

**Environmental**
- For a given asset, what are the assets that surrounds it and for which there are upstream or downstream dependencies
- What are the inherent weaknesses of those surrounding assets that could harm or strengthen the posture of the asset of interest

**Contextual**
- What else is happening around the asset?
- How do changes in environmental factors positively or negatively influence the posture of the asset in question?

**Situational Awareness**
- Who/What/When/Where/How
- What behaviors has the asset exhibited historically and recently
- Where has it deviated from normal behavior
Example 1: Endpoint Vulnerability?

- **Structural:** Fully patched, locked down endpoint, 2FA enabled
- **Situational:** Machine compromised due to malware installed through client-side attack
- **Contextual:** User clicked on a spear phishing email
- **Environmental:** User of endpoint failed last phishing simulation test
- **Environmental:** Training and awareness not complete

```
<table>
<thead>
<tr>
<th>Devices</th>
<th>Applications</th>
<th>Networks</th>
<th>Data</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Protect</td>
<td>Detect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td>Process</td>
<td>Technology</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Sponsored by: AWS Marketplace

@sounilyu
Example 2: Insider?

Environmental: Content originated from server housing sensitive blueprints for new product

Environmental: New B2B connection made with a Chinese manufacturing plant

Structural: Data is encrypted

Environmental: Regular user of server aligned to new China project

Contextual: No unusual logins or interactions with server

Contextual: Machine sending 1GB of traffic to China on an hourly basis

Situational: Probably normal business activity

Did user get phished?

DLP alerts firing off

Devices

Applications

Networks

Data

Users

Degree of Dependency

Technology

Process

People

Identify

Protect

Detect

Respond

Recover

Sponsored by: AWS Marketplace

@sounilyu
How to navigate solutions in AWS Marketplace for situational awareness in AWS
Cybersecurity Threats
The CIS® and MS-ISAC® cybersecurity professionals analyze risks and alert members to current online security threats.

Frameworks

NIST
View the NIST CSF and explore AWS Marketplace solutions mapped to the CSF
NIST CSF

Cyber Defense Matrix
View the Cyber Defense Matrix and explore AWS Marketplace solutions mapped to the CDM
Cyber Defense Matrix

Featured AWS Marketplace Vendors

splunk
Explore Splunk Products

DEVO
Explore Devo Products

FORTINET
Explore Fortinet Products

paloalto
Explore Palo Alto Products

Explore Solutions by Topic Area and Use Case
Mapping Primitives

One: Is the control looking for people, process, or technology?

Two: Understand the primary function that a technology must have to meet the control requirement.

Three: Is the mapping believable. No silver bullets.

Example: Protect Data

Correct – Data Encryption category. Products in this category should protect data at rest as the primary function. (left of boom)

Incorrect – SIEM category. Products in this category collect and aggregate events related to data. (right of boom)
## Cyber Defense Matrix

### Device
- **Identify**
  - AWS Config
  - AWS Security Hub
  - AWS Web-Authenticated Tool
- **Protect**
  - AWS Control Tower
  - AWS IoT Device Defender
  - AWS Resource Access Manager
- **Detect**
  - Amazon Detective
  - AWS IoT Events
  - AWS Personal Health Dashboard
- **Respond**
  - AWS IoT Events
  - AWS Systems Manager
- **Recover**
  - AWS CloudFormation
  - AWS Capabilities
  - CloudEndure Disaster Recovery

### Application
- **Identify**
  - AWS Inspector
  - AWS Certificate Manager
  - AWS License Manager
- **Protect**
  - AWS Single Sign-On
  - AWS WAF
  - Elastic Load Balancing
- **Detect**
  - Amazon Cognito
- **Respond**
  - AWS Lambda
  - AWS Step Functions
- **Recover**
  - AWS Lambda
  - CloudEndure Disaster Recovery

### Network
- **Identify**
  - AWS Config
  - AWS Direct Connect
  - AWS Security Hub
  - AWS Transit Gateway
- **Protect**
  - Amazon GuardDuty
  - Amazon Route 53
  - Amazon Virtual Private Cloud
- **Detect**
  - AWS Policy Manager
  - AWS Private Link
  - Elastic Load Balancing
- **Respond**
  - AWS Personal Health Dashboard
  - AWS Security Hub
- **Recover**
  - AWS CloudFormation

### Data
- **Identify**
  - Amazon S3
  - AWS Config
  - AWS Trusted Advisor
- **Protect**
  - AWS CloudTrail
  - AWS Key Management Service (KMS)
  - AWS Resource Access Manager
- **Detect**
  - AWS Personal Health Dashboard
  - AWS Security Hub
- **Respond**
  - AWS S3 Glacial
  - AWS S3 Glacier
  - CloudEndure Disaster Recovery

### User
- **Identify**
  - AWS Identity and Access Management (IAM)
  - AWS Organizations
- **Protect**
  - AWS Directory Service
  - AWS Identity and Access Management (IAM)
  - AWS Organizations
- **Detect**
  - Amazon Detective
  - AWS Lambda
- **Respond**
  - AWS CloudTrail
  - AWS Security Hub
Sample Investigation

Addison submits a ticket to the security team claiming that her system is acting funny. Max, a security analyst, begins researching the event and contacts Addison for more information. During their brief discussion Max learns that Addison clicked on an email just a few minutes before she noticed her system performing abnormally slow.

- How would you perform this investigation?
- How do you know if you have the right tools?
- Where would you gather data for structural, environmental, contextual, and situational awareness?
1. What is the device name?
2. What is the device category? (laptop, workstation, physical server, cloud instance, IoT, smartphone, tablet)
3. What is the criticality or priority of the device?
4. Who is the asset assigned to?
5. What is the device operating system?
6. Is the device vulnerable?
7. Is the operating system fully patched?
8. What business unit does the device belong to?
9. Is there any endpoint protection software installed?
10. Is the endpoint protection software configured to protect known vulnerabilities?
11. What applications are installed on the device?
12. Are any applications vulnerable?
13. Are all applications fully patched?
14. Are any of the applications critical or priority?
15. Are the applications protected at the device level?
16. Are the applications protected at the network level?
17. Is there any critical or sensitive data on the device?
18. What user accounts have access to the device?
19. What privileges do the logged in accounts have? (user, admin, root, sa)?
20. Are any of the user accounts critical or priority?
21. What network zone was the device in at the time of the event?
22. Is the network zone vulnerable?
23. Is the network zone critical or priority?
24. What user account was logged in at the time of the event?
25. Who is the sender?
26. What is the domain associated to the sender?
27. What is the IP address associated to the domain?
28. What geo location is the IP or domain?
29. Who is the domain registered to?
30. How old is the domain?
31. Was there an attachment to the email?
32. Was there a link in the email?
33. Did the device communicate to any remote IP addresses, URLs, or domain names?
34. Is the malware associated to any CVE’s?
35. Are there any recent reports related to the malware?
36. Are there any known patches (OS, Application) that mitigate the malware?
37. Does the malware create a back door?
38. Does the malware pull down any additional payloads?
39. Does the malware update itself?
40. Does the malware change itself (name, hash, filepath etc.)?
41. Does the malware perform any network scanning or reconnaissance?
42. Does the malware attempt to move to other hosts?
43. Does the malware attempt to send email or other forms of communication?
44. Does the malware attempt to access user credentials?
45. Does the malware enumerate the file system?
46. Does the malware inject itself into any other processes?
Prioritizing Security Controls for Situational Awareness

### Structural Awareness

**Asset Specific:**
- For a specific asset, what are its weaknesses?
- What attributes provide verifiable authenticity of its identity?
- What is the expected behavior of the asset?

### Situational Awareness

**Asset Specific:**
- What behavior has the asset exhibited historically and recently?
- Where has it deviated from normal behavior?

### Environmental Awareness

**Asset Surroundings:**
- For a given asset, what are the assets that surround it, and which of them are upstream or downstream dependencies?
- What are the network weaknesses of these surrounding assets, and could they influence or degrade the security posture for the asset of interest?

### Contextual Awareness

**Asset Surroundings:**
- How do changes in the environment factors positively or negatively influence the security posture for the asset of interest?

---

### Cyber Defense Matrix

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td><strong>Application</strong></td>
<td><strong>Device</strong></td>
<td><strong>Application</strong></td>
<td><strong>Device</strong></td>
</tr>
<tr>
<td>AWS Config</td>
<td>AWS Inspector</td>
<td>AWS Config</td>
<td>AWS Inspector</td>
<td>AWS Config</td>
</tr>
<tr>
<td>AWS Security Hub</td>
<td>AWS Certificate Manager</td>
<td>AWS IoT Device Defender</td>
<td>AWS Certificate Manager</td>
<td>AWS IoT Device Defender</td>
</tr>
<tr>
<td>AWS Well-Architected Tool</td>
<td>AWS License Manager</td>
<td>AWS Resource Access Manager</td>
<td>AWS License Manager</td>
<td>AWS Resource Access Manager</td>
</tr>
<tr>
<td>Palo Alto</td>
<td>AWS Cloud</td>
<td>Palo Alto</td>
<td>AWS Cloud</td>
<td>Palo Alto</td>
</tr>
</tbody>
</table>

- **Identify:** AWS Control Tower, AWS Multi-Factor Authentication, AWS Resource Access Manager
- **Protect:** AWS IoT Device Defender, AWS Resource Access Manager, AWS Cloud
- **Detect:** AWS Detector, AWS IoT Events, AWS Personal Health Dashboard
- **Respond:** AWS Systems Manager, AWS CloudFormation, Cybersecurity Sce
- **Recover:** AWS Cloud, AWS CloudFormation, Cybersecurity Sce
What are the details about the device, applications, data, and user? Is there anything critical about the asset and should this be prioritized?
What activities were performed before, during, and after the email?
Is there abnormal behavior that for the device and user?
What tools are available to contain and eradicate?

What tools are available to strengthen the environment to block in the future?
Enabling situational awareness in AWS
AWS services that enhance situational awareness

- Identify
- Protect
- Detect
- Respond
- Recover

Identify
- AWS Security Hub
- AWS Organizations
- AWS Transit Gateway
- Amazon VPC
- AWS IoT Device Defender
- Amazon Cloud Directory
- Amazon GuardDuty
- Amazon Macie
- AWS CloudWatch
- AWS Step Functions
- AWS Systems Manager
- AWS Lambda

Protect
- AWS Config
- AWS Shield
- AWS Identity and Access Management
- AWS Direct Connect
- AWS Directory Service
- AWS Resource Access Manager
- AWS Secrets Manager
- AWS Key Management Service
- Amazon Cognito
- AWS Service Catalog
- AWS Well-Architected Tool

Detect
- Amazon Detective
- AWS CloudWatch
- AWS CloudFront
- Amazon Personal Health Dashboard
- Amazon Route 53

Respond
- Snapshot
- Archive

Recover
- AWS OpsWorks
- AWS CloudFormation

Investigate
- AWS CloudFormation

Automate
- AWS CloudFormation
- AWS CloudFormation
Increase visibility and strength of foundational controls

AWS forwarding findings into AWS Security Hub
- Firewalls
- Vulnerability
- Endpoint
- Compliance
- MSSP

“Taking Action”
- SIEM: splunk, sumo logic, DEVO
- SOAR: splunk, SWIMLANE, DEMISTO
- Other: slack, servicenow, ATLASIAN, TURBOT

AWS Security Services forwarding findings into AWS Security Hub
- Amazon Detective
- Amazon Macie
- Amazon Inspector
- Amazon GuardDuty
How are AWS customers leveraging Splunk?

- Security visibility and threat detection
- Real-time collection and indexing of log data
- Continuous security monitoring of infrastructure
Los Angeles enhances situational awareness

Benefits:

• Established always-available, real-time situational awareness

• Increased ability to view and compare log data from multiple sources

• Reduced time to detect and respond to incidents
Western Asset Management mitigates risk
With Prisma Public Cloud by Palo Alto Networks

Benefits:

• Full visibility across all accounts
• Incident and misconfiguration response times reduced from days to minutes
• Eliminated manually sifting through audit files
CaixaBank improves security analytics
Leveraging Devo for greater speed and scale of investigations

Benefits:

• Achieve data ingest rates of 11 to 20TB per day

• Query times reduced by 98%

• Time-to-alert reduced to milliseconds
Why AWS Marketplace?

Flexible consumption and contract models

Quick and easy deployment

Helpful humans to support you
How can you get started?

**Find**

A breadth of security solutions:

- splunk
- paloalto
- SOPHOS
- DEVO
- ALERT LOGIC
- TREND MICRO
- FORTINET
- sumo logic
- CloudGuard
- CrowdStrike

**Buy**

Through flexible pricing options:

- Free trial
- Pay-as-you-go
- Hourly | Monthly | Annual | Multi-Year
- Bring Your Own License (BYOL)
- Seller Private Offers
- Channel Partner Private Offers

**Deploy**

With multiple deployment options:

- Software as a Service (SaaS)
- Amazon Machine Image (AMI)
- AWS CloudFormation (Infrastructure as Code)
- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)
Webinar summary

- Consider solutions that enhance situational awareness in AWS.
- Leverage solutions that integrate with AWS Services.
- Current tools? Bring your own license to leverage benefits of AWS Marketplace.
- New tools? Select solutions in AWS Marketplace for a curated list proven on AWS.
Thank you!