



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

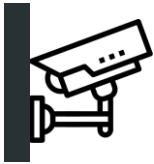


Defenders need cyber situational awareness to mitigate the loss or compromise of assets

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

```
Fri 20 Nov 2015 14:37:07 PST: 134.173.42.70 http://sync.mathtag.c
om/sync/img?mt_exid=10025&redir=http%3A%2F%2Fsu.addthis.com%2Fred
%2Fusync%3Fpid&mm_bnc&mm_bct&UID=223d-33d212 442 Sun 22 Nov 201
5 22:51:24 PST: 134.173.197.65 http://download.mozilla.com/?produ
ct=firefox-42.0-complete&os=osx&lang=en-US 401 Sun 22 Nov 2015 2
2:51:25 PST: 134.13.197.6 http://download.cdn.mozilla.com/pub/fin
efox/releases/42.0/update/mac/en-US/firefox-42.0.complete.exe 300
480 Sun 22 Nov 2015 22:57:59 PST: 134.173.197.65 http://www.find
evil.com/ 1888 Sun 22 Nov 2015 23:05:58 PST: 134.173.197.65 http
://cs.hmc.edu/ 179 Tue 24 Nov 2015 10:07:05 PST: 134.173.42.70 h
ttp://self-repair.mozilla.org/en-US/repair 572 Tue 24 Nov 2015 1
0:07:25 PST: 134.173.42.70 http://www.pomona.edu/sites/default/fin
les/css/css_QSWyDNAFYyPolo_fQ5W5McyjIhuOqPPgAPPkIi9BpgrI.css 13296
Tue 24 Nov 2015 10:12:11 PST: 134.173.42.70 http://www.googletagm
anager.com/gtm.js?id=GTM-FVBCBG 17495 Tue 24 Nov 2015 10:12:11 P
ST: 134.173.42.70 http://www.pomona.edu/sites/default/files/style
s/homepage_spotlight/public/spotlight.jpg?itok=-VKvyhfY 28159 Tu
e 24 Nov 2015 10:12:11 PST: 134.173.42.70 http://evil.com/ 654 T
ue 24 Nov 2015 10:12:11 PST: 134.173.42.70 http://www.google-ana
lytics.com/analytics.js 228 Tue 24 Nov 2015 10:12:11 PST: 134.173
```

Visibility →

Perception →

Faulty
Visibility →

Faulty
Perception

Faulty
Comprehension

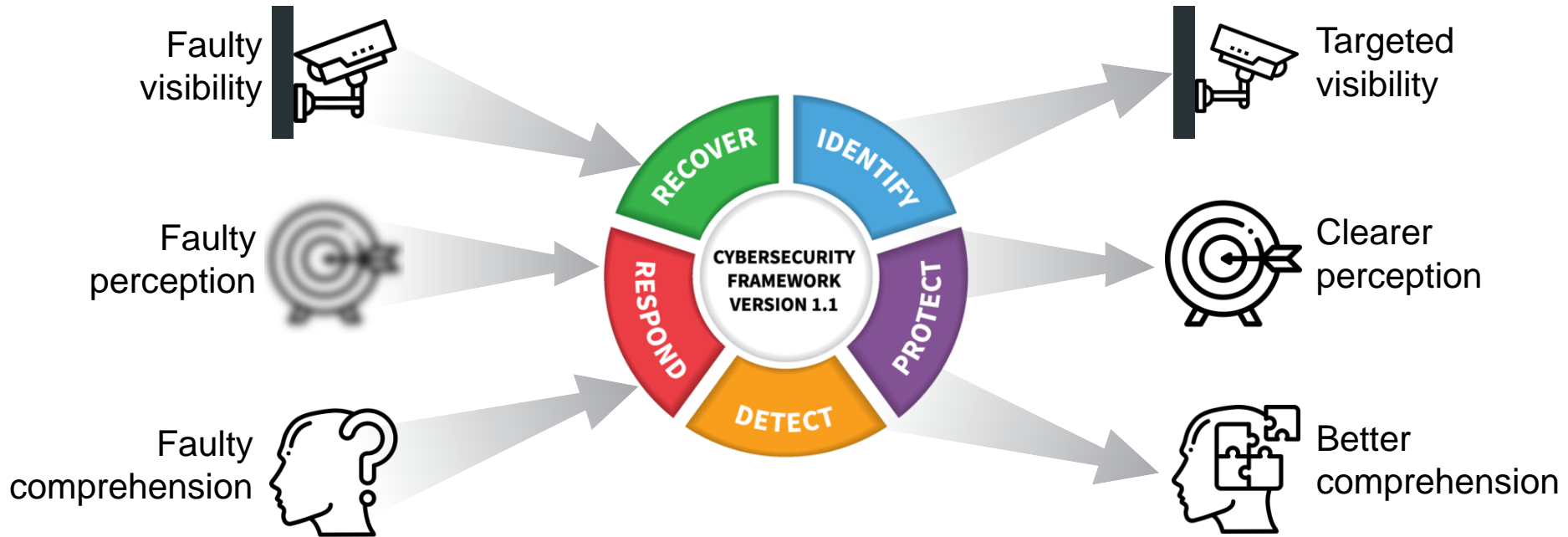
Verdict: Bad

Comprehension
Verdict: Bad

Projection:
Lateral Movement



To discover blind spots and overcome challenges in attaining higher levels of situational awareness, frameworks are helpful



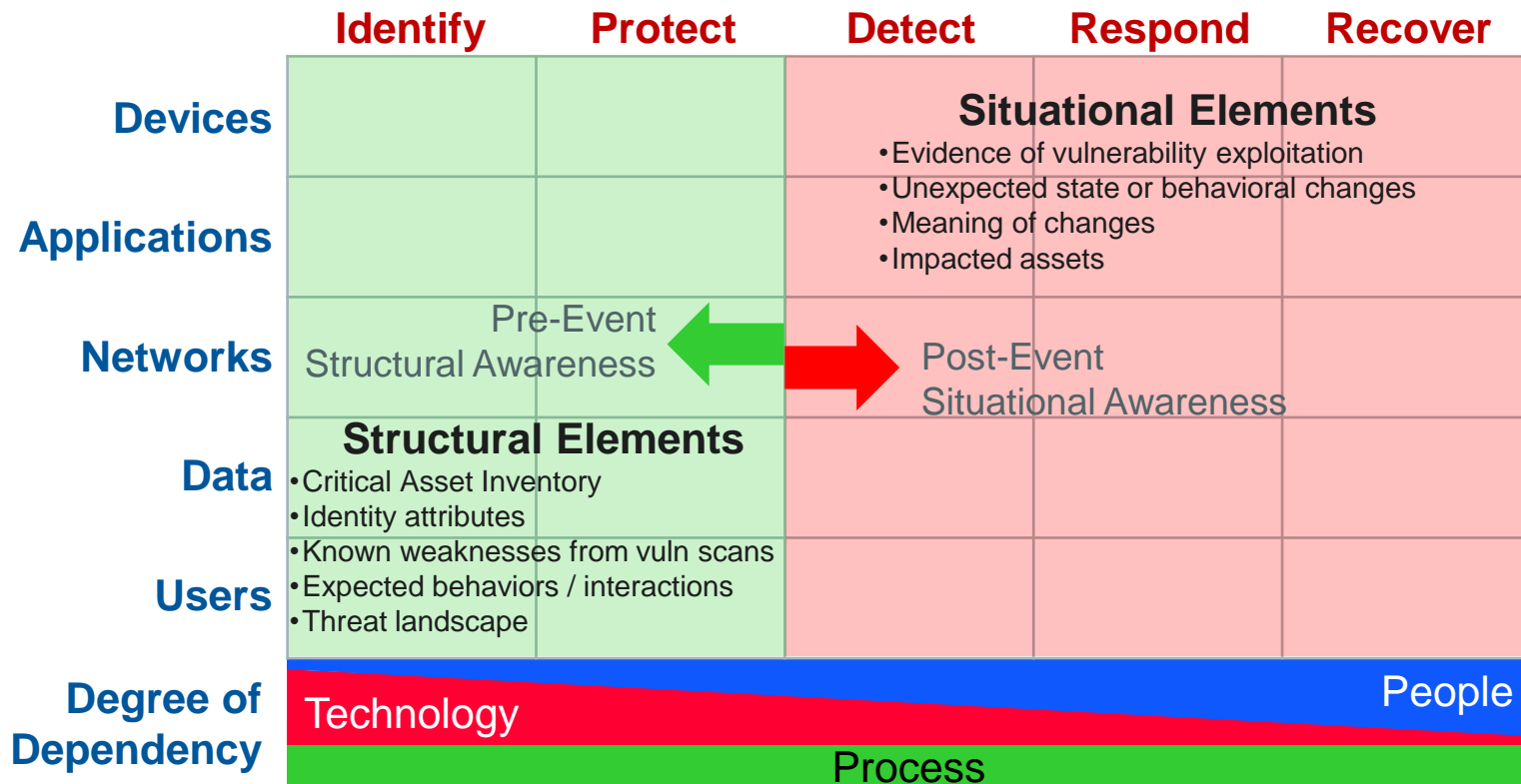
The Cyber Defense Matrix is an adaptation of the CSF

<https://cyberdefensematrix.com>

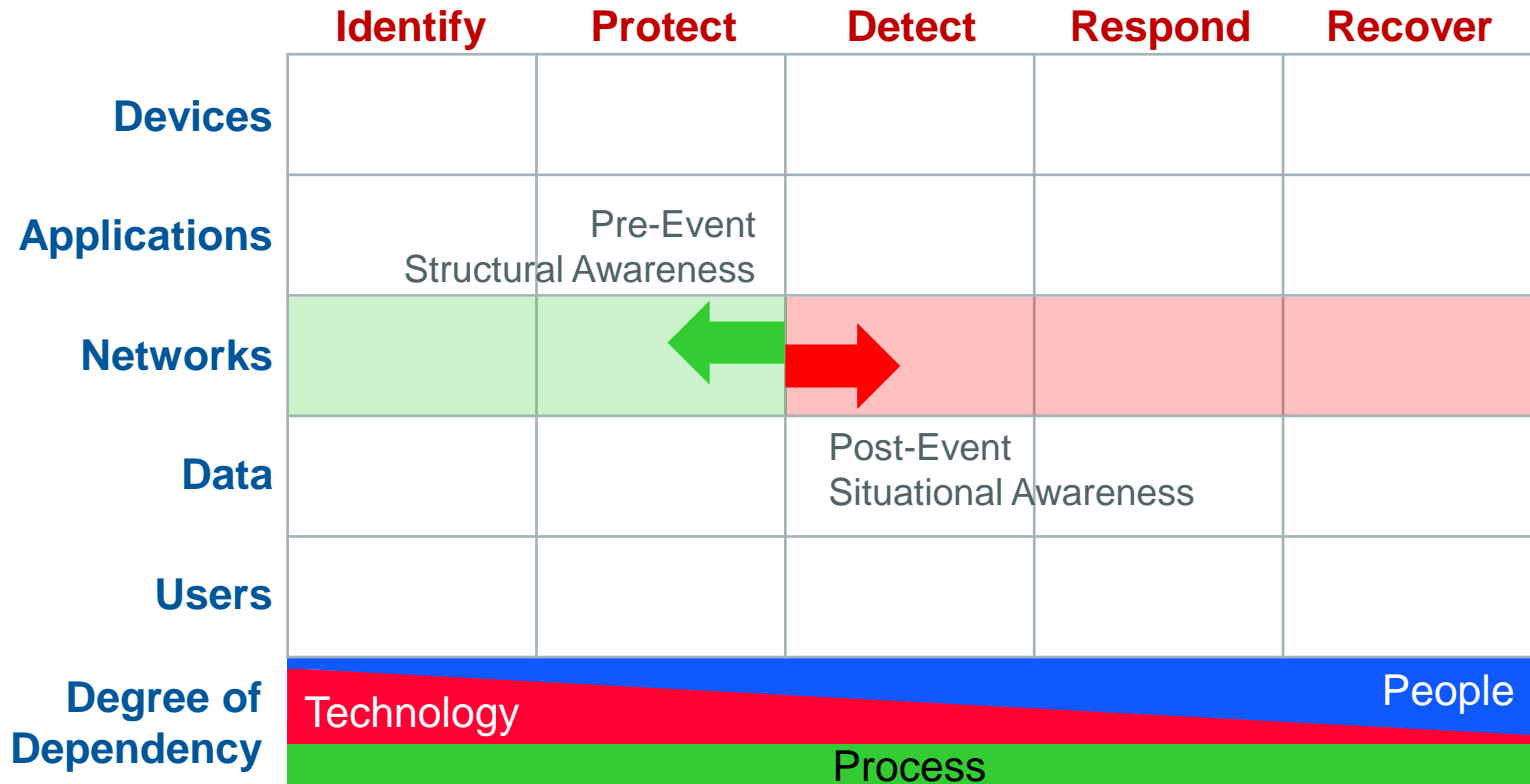
	Identify	Protect	Detect	Respond	Recover	
Devices						
Applications						
Networks						
Data						
Users						
Degree of Dependency	Technology		Process			People



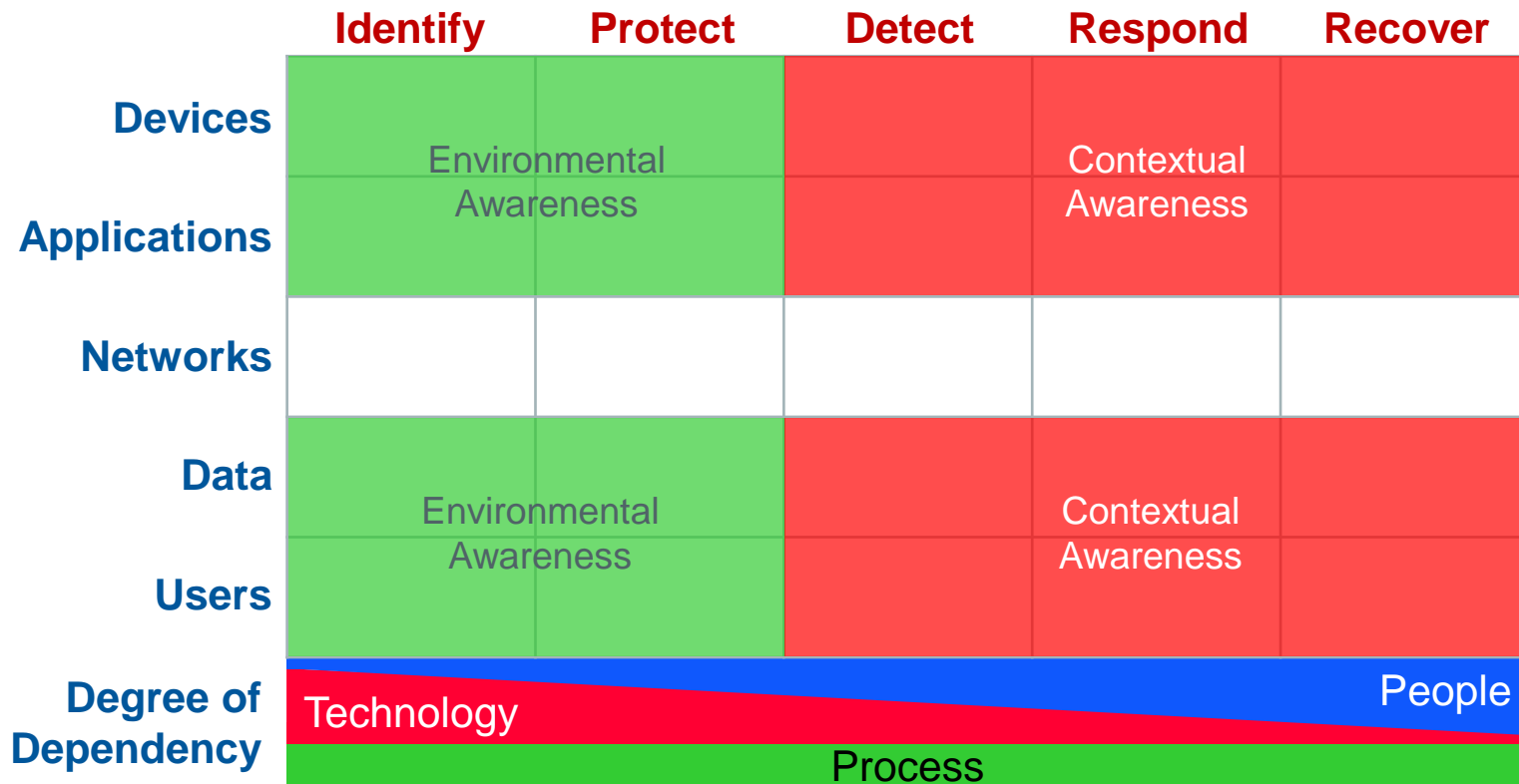
Left & Right of Boom: Structural vs Situational Awareness



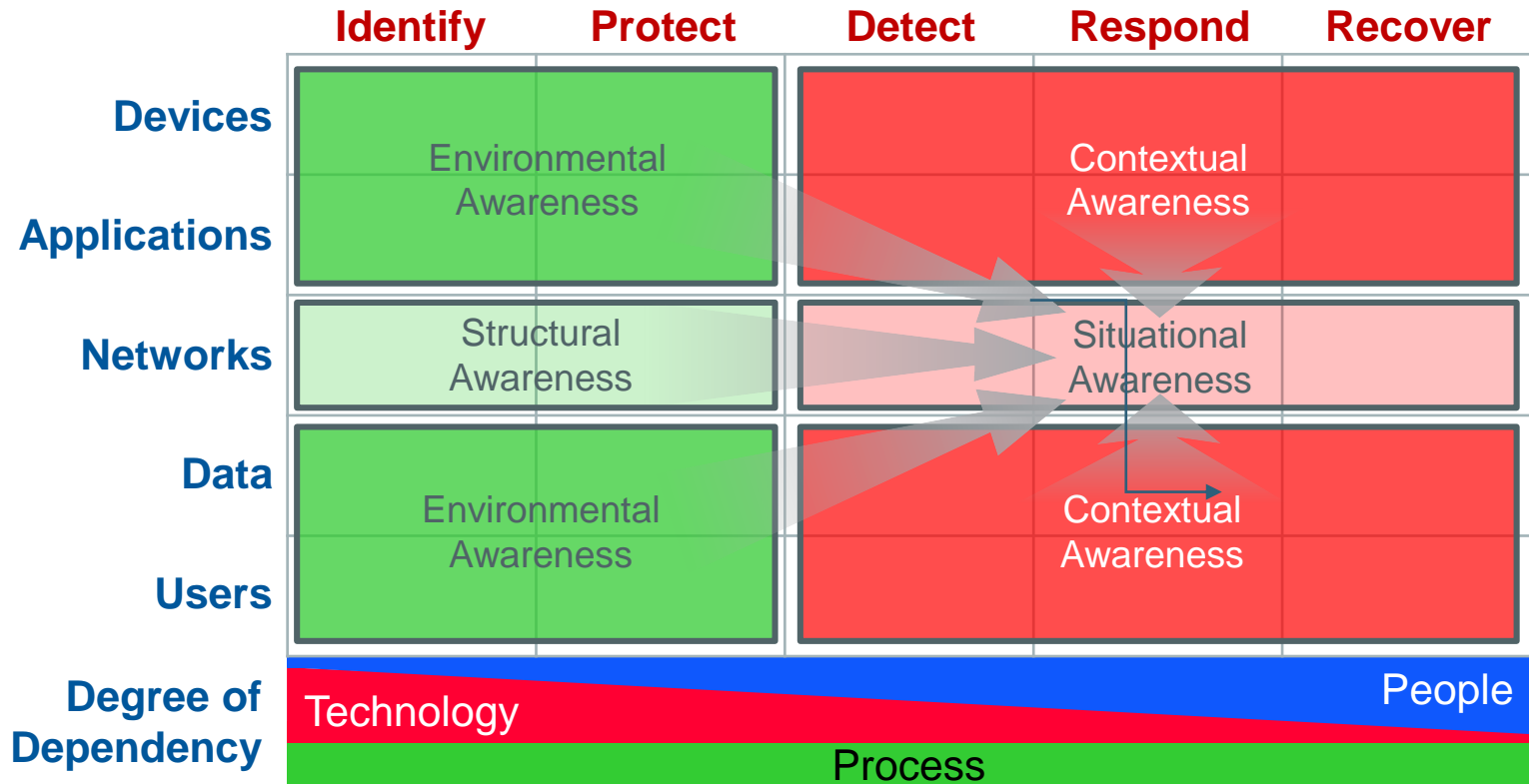
Asset Specific Structural and Situational Awareness



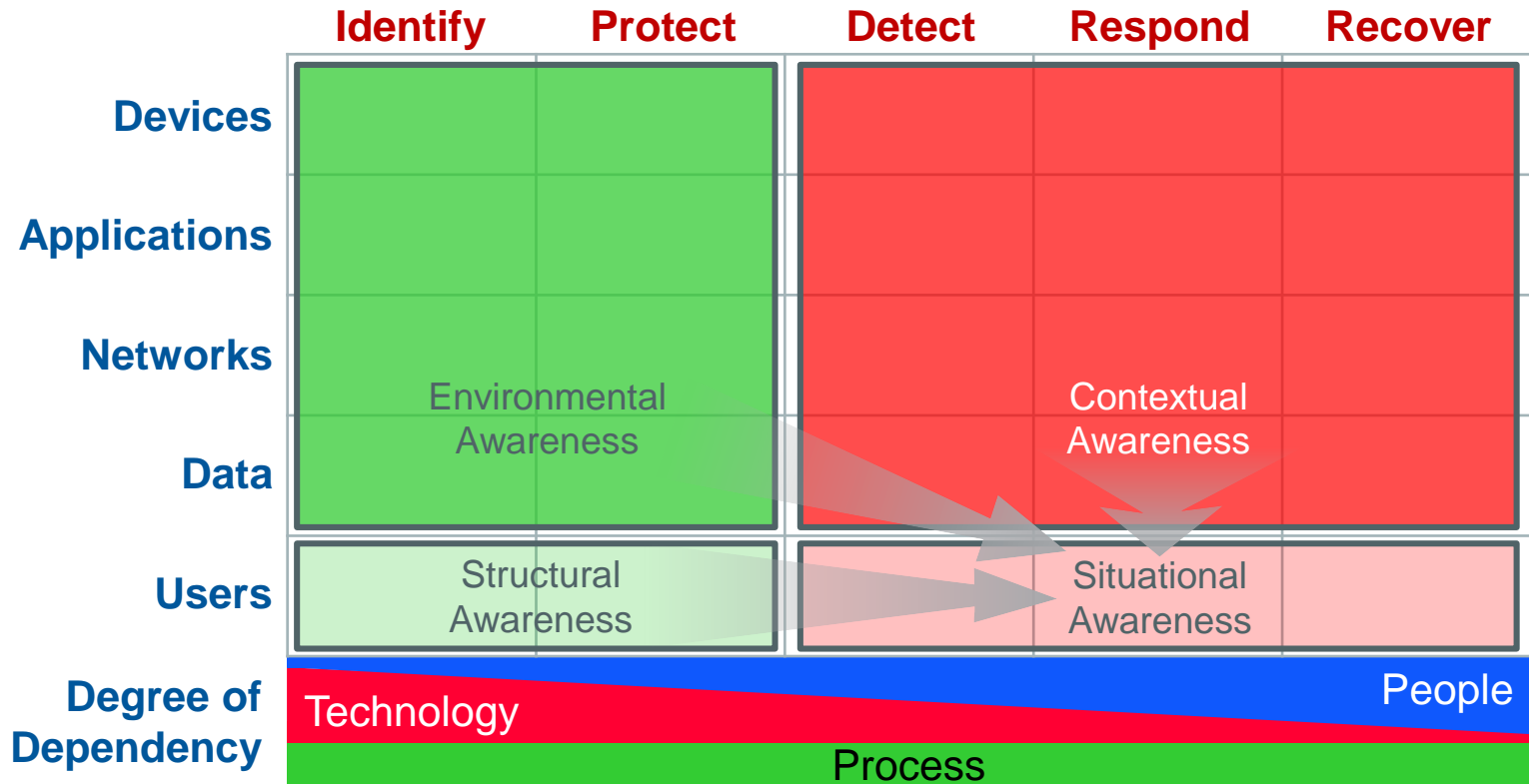
Environmental and Contextual Awareness



Bolstering Situational Awareness



Bolstering Situational Awareness: Insider Threat



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

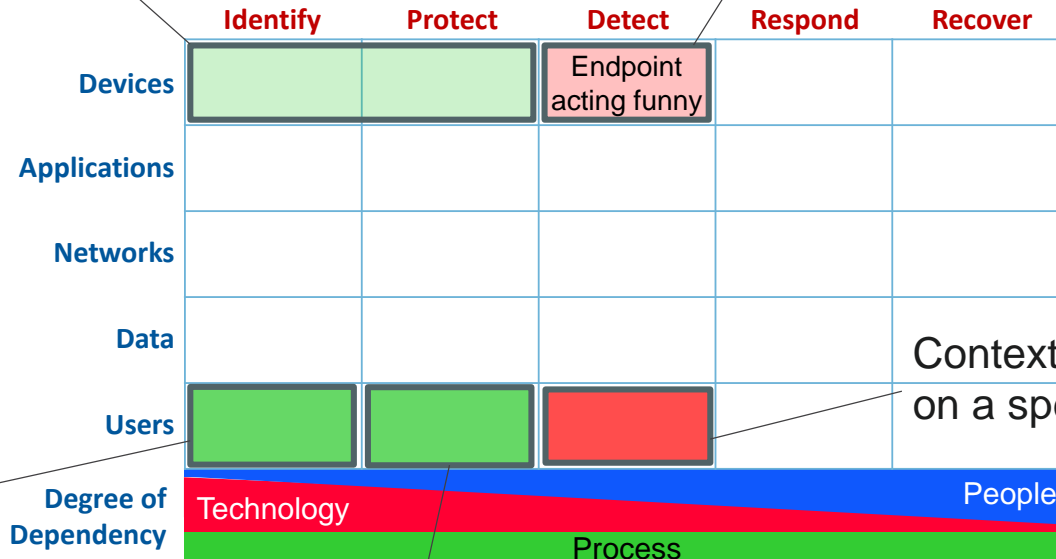
- Who/What/When/Where/How
- What behaviors has the asset exhibited historically and recently
- Where has it deviated from normal behavior



Example 1: Endpoint Vulnerability?

Structural: Fully patched, locked down endpoint, 2FA enabled

Situational: Machine compromised due to malware installed through client-side attack



Environmental: User of endpoint failed last phishing simulation test

Environmental: Training and awareness not complete

Sponsored by: aws marketplace

SOUNIL YU

@sounilyu



Example 2: Insider?

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

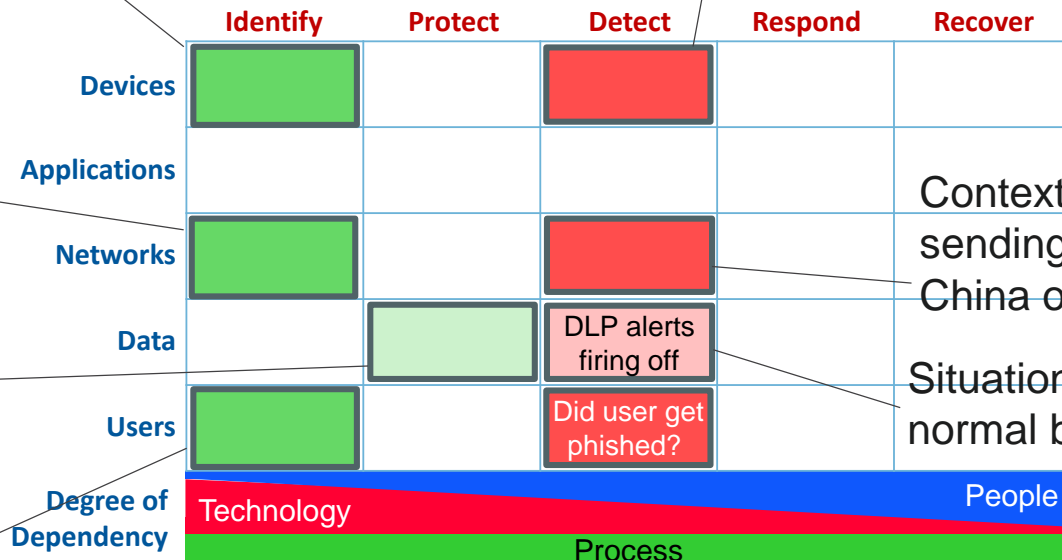
Contextual: No unusual logins or interactions with server

Environmental:
New B2B connection made with a Chinese manufacturing plant

Structural:
Data is encrypted

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

Situational: Probably normal business activity



Environmental: Regular user of server aligned to new China project





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](#)



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

[Cyber Defense Matrix](#)


Featured AWS Marketplace Vendors



[Explore Splunk Products](#)



[Explore Devo Products](#)



[Explore Fortinet Products](#)



[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

	Identify	Protect	Detect	Respond	Recover
Device	<ul style="list-style-type: none"> AWS Config AWS Security Hub AWS Well-Architected Tool 	<ul style="list-style-type: none"> AWS Control Tower AWS IoT Device Defender AWS Resource Access Manager 	<ul style="list-style-type: none"> Amazon Detective AWS IoT Events AWS Personal Health Dashboard AWS Security Hub 	<ul style="list-style-type: none"> AWS IoT Events AWS Systems Manager 	<ul style="list-style-type: none"> AWS CloudFormation AWS OpsWorks CloudEndure Disaster Recovery
Application	<ul style="list-style-type: none"> Amazon Inspector AWS Certificate Manager AWS License Manager AWS Secrets Manager AWS Service Catalog 	<ul style="list-style-type: none"> Amazon Cognito AWS Single Sign-On AWS WAF Elastic Load Balancing 	<ul style="list-style-type: none"> AWS Security Hub 	<ul style="list-style-type: none"> AWS Lambda AWS Step Functions 	<ul style="list-style-type: none"> AWS Logo CloudEndure Disaster Recovery
Network	<ul style="list-style-type: none"> AWS Config AWS Direct Connect AWS Security Hub AWS Transit Gateway 	<ul style="list-style-type: none"> Amazon GuardDuty Amazon Route 53 Amazon Virtual Private Cloud AWS Firewall Manager AWS PrivateLink AWS Shield Elastic Load Balancing 	<ul style="list-style-type: none"> AWS Personal Health Dashboard AWS Security Hub 	<ul style="list-style-type: none"> AWS Lambda AWS Step Functions 	<ul style="list-style-type: none"> AWS CloudFormation
Data	<ul style="list-style-type: none"> Amazon Macie AWS Config AWS Trusted Advisor 	<ul style="list-style-type: none"> AWS CloudHSM AWS Key Management Service (KMS) AWS Resource Access Manager 	<ul style="list-style-type: none"> AWS Personal Health Dashboard AWS Security Hub 		<ul style="list-style-type: none"> Amazon EBS Snapshots AWS S3 Glacier CloudEndure Disaster Recovery
User	<ul style="list-style-type: none"> Amazon Cloud Directory AWS Directory Service AWS Identity and Access Management (IAM) AWS Organizations AWS Security Hub 		<ul style="list-style-type: none"> Amazon Detective Amazon Macie AWS CloudTrail AWS Security Hub 		

Sample Investigation

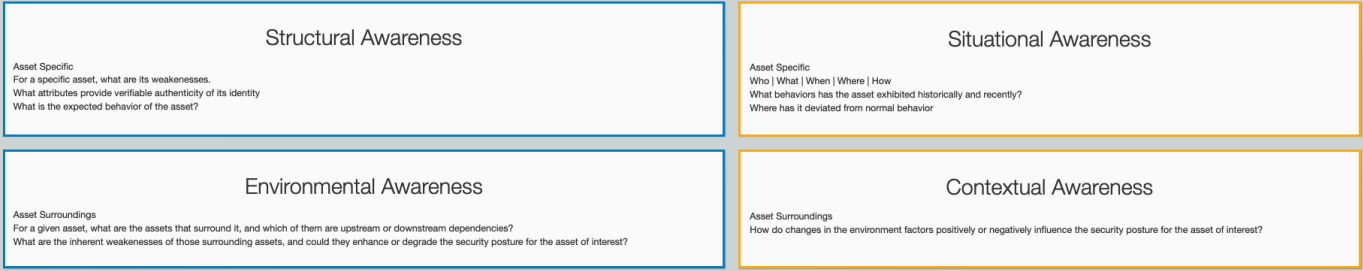
Addison submits a ticket to the security team claiming that her system is acting funny. Max, a security analyst, begins researching the event and contacts Addison for more information. During their brief discussion Max learns that Addison clicked on an email just a few minutes before she noticed her 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 domains?
34. What IP addresses, URLs, or domains did the device communicate to?
35. What protocols did the device communicate to?
36. What ports did the device communicate to?
37. What protocols did the device receive from?
38. What ports did the device receive from?
39. What protocols did the device receive from?
40. What ports did the device receive from?
41. What protocols did the device receive from?
42. What ports did the device receive from?
43. What protocols did the device receive from?
44. What ports did the device receive from?
45. What protocols did the device receive from?
46. What ports did the device receive from?
47. What protocols did the device receive from?
48. What ports did the device receive from?
49. What protocols did the device receive from?
50. What ports did the device receive from?
51. What protocols did the device receive from?
52. What ports did the device receive from?
53. What protocols did the device receive from?
54. What ports did the device receive from?
55. What protocols did the device receive from?
56. Is the malware associated to any CVE's?
57. Are there any recent reports related to the malware?
58. Are there any recent reports related to the malware?
59. Are there any known patches (OS, Application) that mitigate the malware?
60. Does the malware create a back door?
61. Does the malware pull down any additional payloads?
62. Does the malware update itself?
63. Does the malware change itself (name, hash, filepath etc.)?
64. Does the malware perform any network scanning or reconnaissance?
65. Does the malware attempt to move to other hosts?
66. Does the malware attempt to send email or other forms of communication?
67. Does the malware attempt to access user credentials?
68. Does the malware enumerate the file system?
69. Does the malware inject itself into any other processes?

Vendor Awareness Scenarios

Prioritizing Security Controls for Situational Awareness

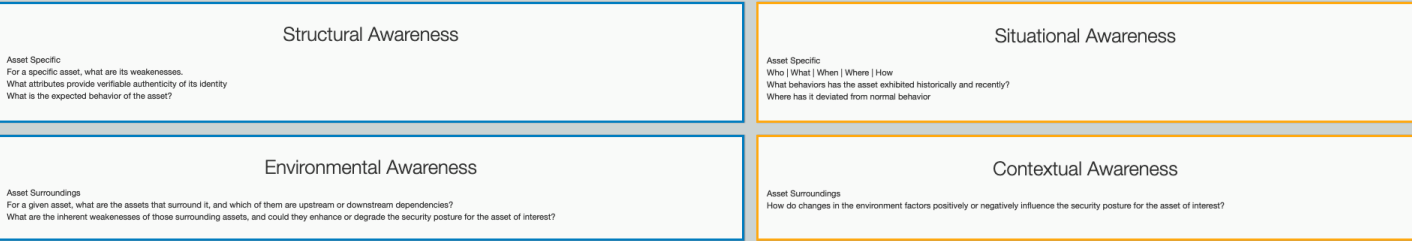


Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device	<ul style="list-style-type: none"> aws AWS Config aws AWS Security Hub aws AWS Well-Architected Tool paloalto Prisma Cloud 	<ul style="list-style-type: none"> aws AWS Control Tower aws AWS IoT Device Defender aws AWS Resource Access Manager paloalto Aporeto Distributed Firewall 	<ul style="list-style-type: none"> aws Amazon Detective aws AWS IoT Events aws AWS Personal Health Dashboard aws AWS Security Hub DEVO Devo Data Analytics Platform DEVO Devo Security Operations splunk Splunk Cloud splunk Splunk Enterprise 	<ul style="list-style-type: none"> aws AWS IoT Events aws AWS Systems Manager fortinet CyberSponse CyOps paloalto Demisto splunk Phantom 	<ul style="list-style-type: none"> aws AWS CloudFormation aws AWS OpsWorks aws CloudEndure Disaster Recovery
Application	<ul style="list-style-type: none"> aws Amazon Inspector aws AWS Certificate Manager aws AWS License Manager 	<ul style="list-style-type: none"> aws Amazon Cognito aws AWS Single Sign-On aws AWS WAF 	<ul style="list-style-type: none"> aws AWS Security Hub 	<ul style="list-style-type: none"> aws AWS Lambda aws AWS Step Functions 	<ul style="list-style-type: none"> aws CloudEndure Disaster Recovery

Vendor Awareness Scenarios

Prioritizing Security Controls for Situational Awareness



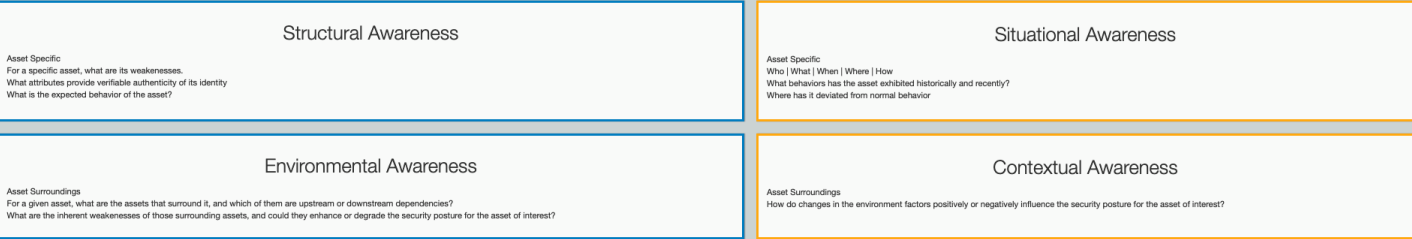
Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device			splunk - Splunk Cloud splunk - Splunk Enterprise	splunk - Phantom	
Application					
Network			splunk - Splunk Cloud splunk - Splunk Enterprise	splunk - Phantom	
Data					
User			splunk - Splunk Cloud splunk - Splunk Enterprise		

What are the details about the device, applications, data, and user?
Is there anything critical about the asset and should this be prioritized?

Vendor Awareness Scenarios

Prioritizing Security Controls for Situational Awareness



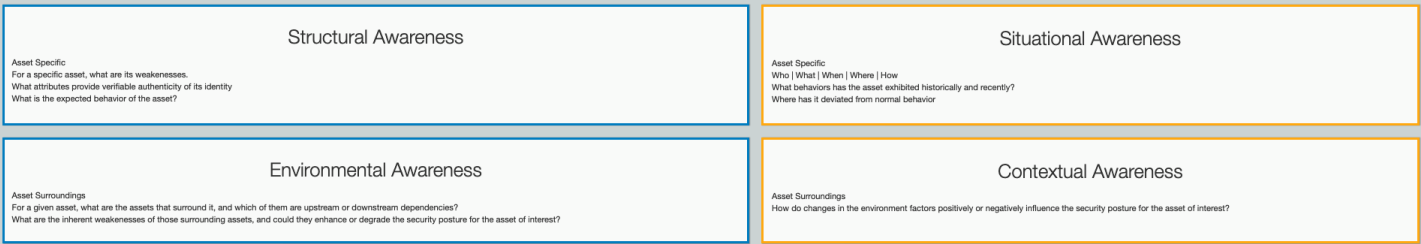
Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device			splunk - Splunk Cloud splunk - Splunk Enterprise	splunk - Phantom	
Application					
Network			splunk - Splunk Cloud splunk - Splunk Enterprise	splunk - Phantom	
Data					
User			splunk - Splunk Cloud splunk - Splunk Enterprise		

What activities were performed before, during, and after the email?
Is there abnormal behavior that for the device and user?

Vendor ▾ Awareness ▾ Scenarios ▾

Prioritizing Security Controls for Situational Awareness



Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device			splunk - Splunk Cloud splunk - Splunk Enterprise	splunk - Phantom	
Application					
Network			splunk - Splunk Cloud splunk - Splunk Enterprise	splunk - Phantom	
Data					
User			splunk - Splunk Cloud splunk - Splunk Enterprise		

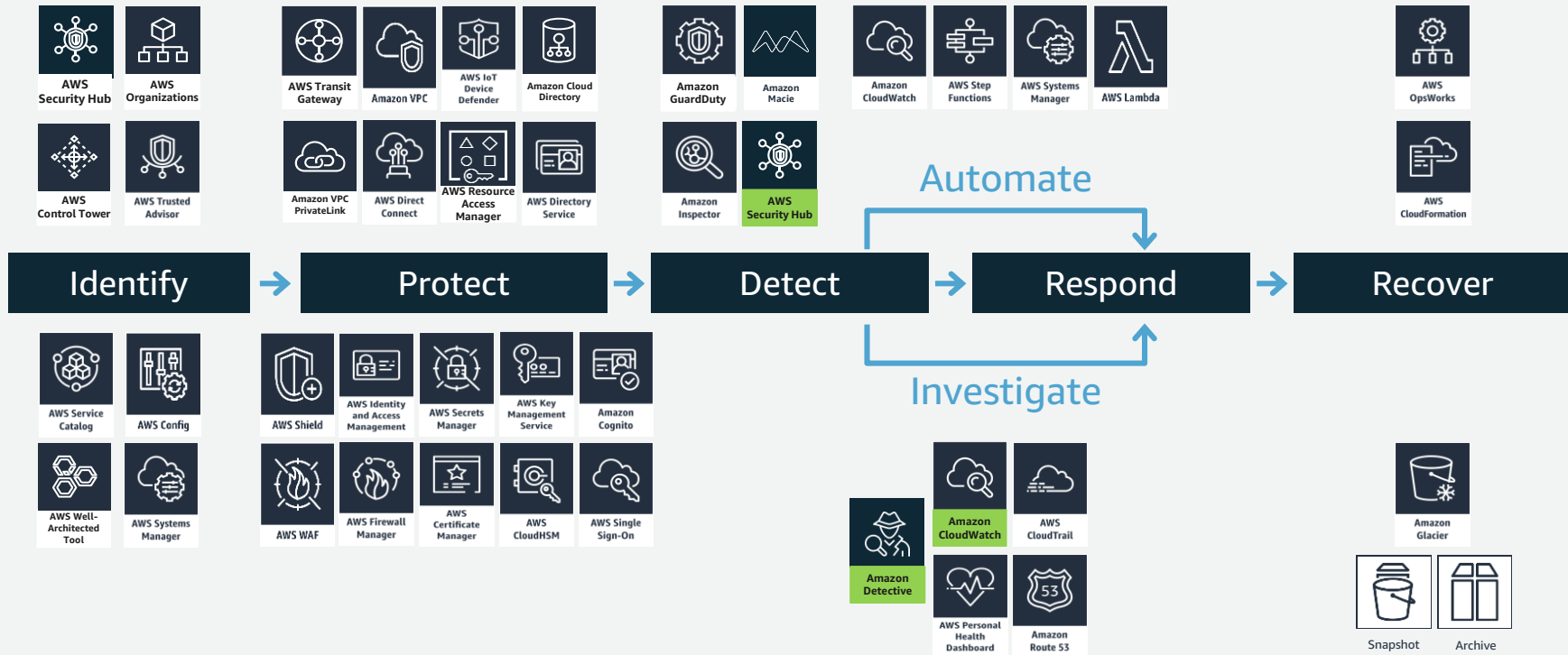
What tools are available to contain and eradicate?
 What tools are available to strengthen the environment to block in the future?



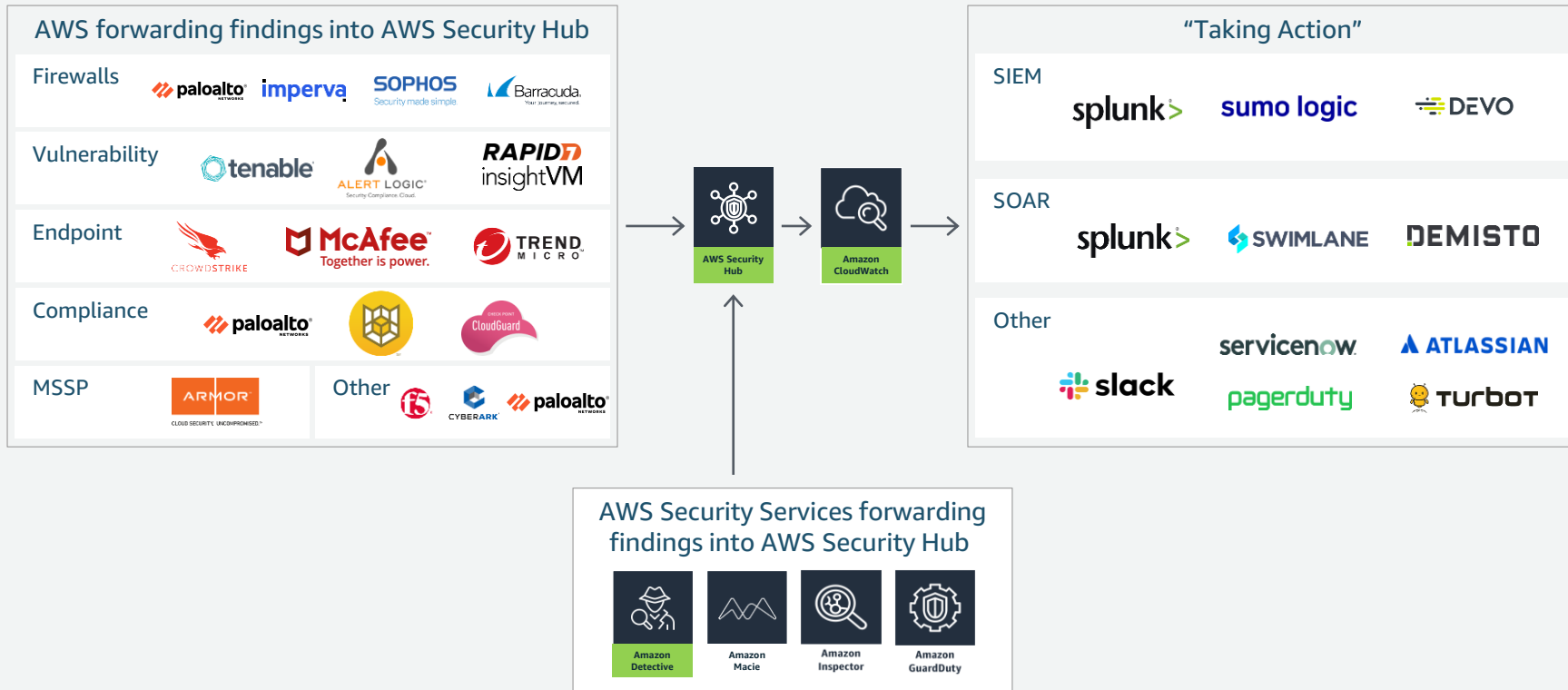
Enabling situational awareness in AWS



AWS services that enhance situational awareness



Increase visibility and strength of foundational controls



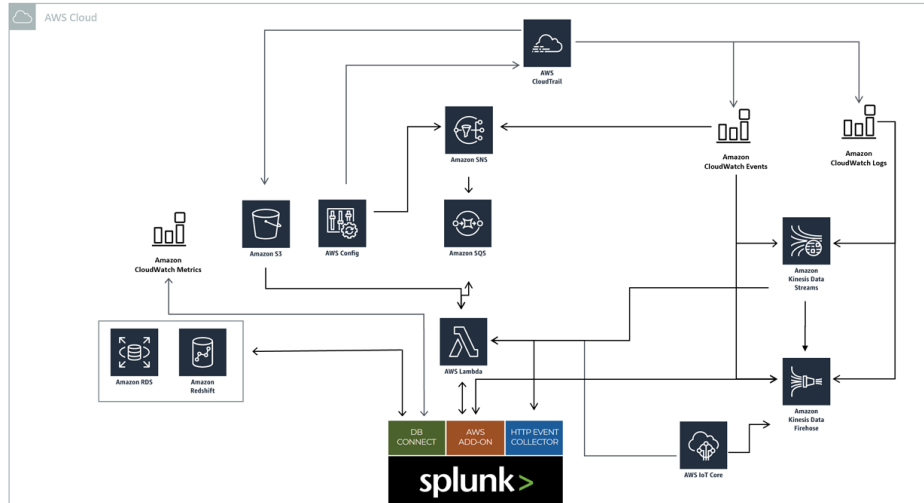
How are AWS customers leveraging Splunk?



Security visibility and threat detection

Real-time collection and indexing of log data

Continuous security monitoring of infrastructure



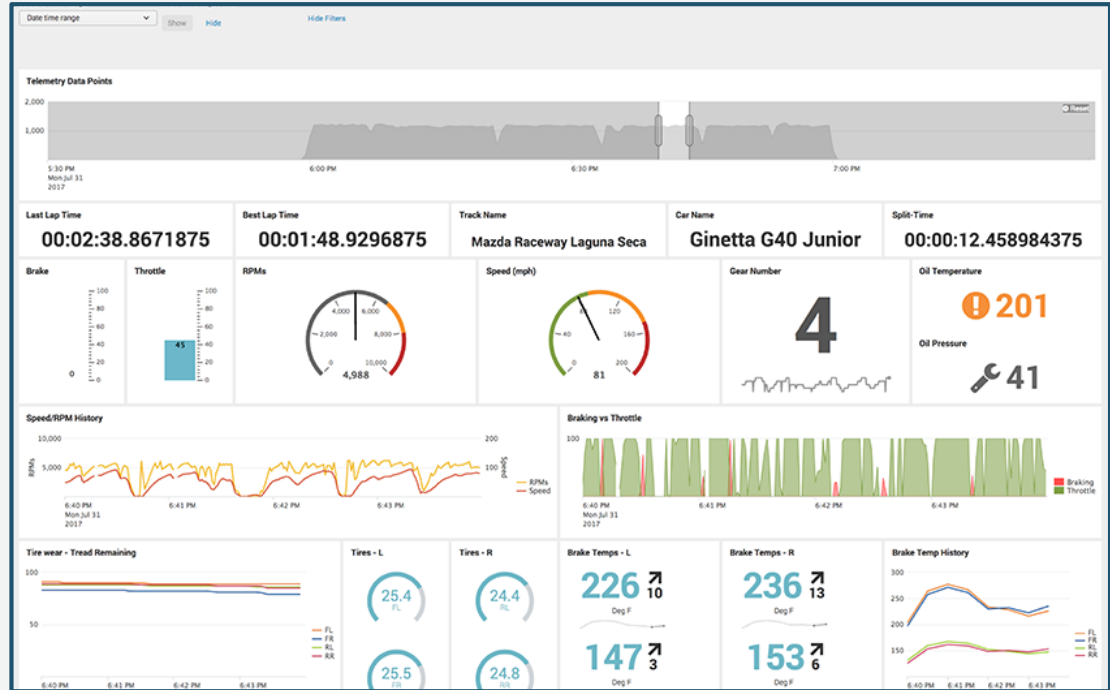
Los Angeles enhances situational awareness

Leveraging Splunk solutions for real-time threat intelligence



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



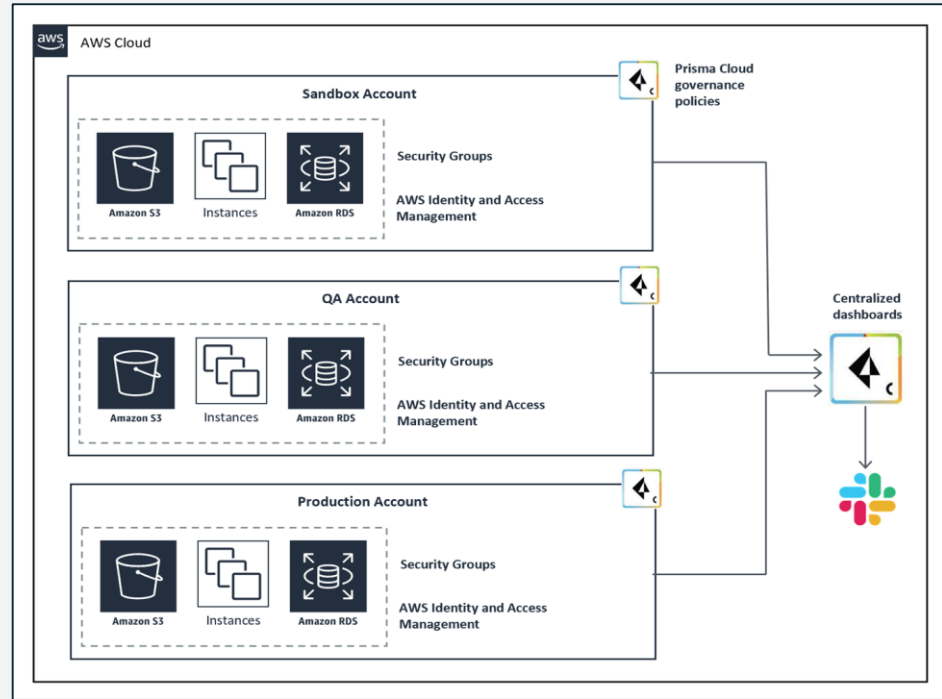
Western Asset Management mitigates risk

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

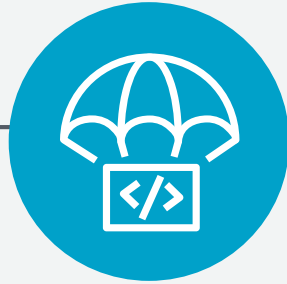
The screenshot displays the Devo Security Operations interface, which is divided into several key sections:

- Alerts:** Shows a status of '6/24 Critical' and '64/179 High' alerts, indicating a high volume of detected threats.
- Analytics:** Features a world map with green data points and connecting lines, representing global network activity and threat patterns.
- Investigations:** A table listing various investigations with columns for 'Created', 'Modified', 'Investigation name', 'Importance', 'Mitigation', 'Assignee', and 'Status'. It includes entries such as 'Directory traversal', 'User behavior', and 'OSINT'. A word cloud below this section highlights terms like 'powershell', 'powercat', 'netcat', 'msfrpc', and 'behavior'.
- Alert types dictated by ATT&CK-MTTC techniques:** A stacked bar chart showing the distribution of alerts across different MITRE ATT&CK techniques like Model, Analytics, Observation, and Detection.
- Top alerts by MITRE ATT&CK:** A list showing the frequency of specific techniques, with 'Credential Access' having the highest count at 243.
- Top entities by impact:** A table listing IP addresses, hostnames, countries, and cities, along with their impact metrics.
- Investigation labels word cloud:** A visual representation of keywords associated with investigations, including 'powershell', 'powercat', 'netcat', 'msfrpc', and 'behavior'.

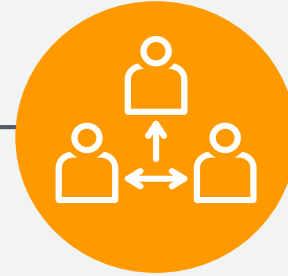
Why AWS Marketplace?



**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
NETWORKS

SOPHOS

DEVO



TREND
MICRO

FORTINET

sumo logic



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.

Q & A

Thank
you!