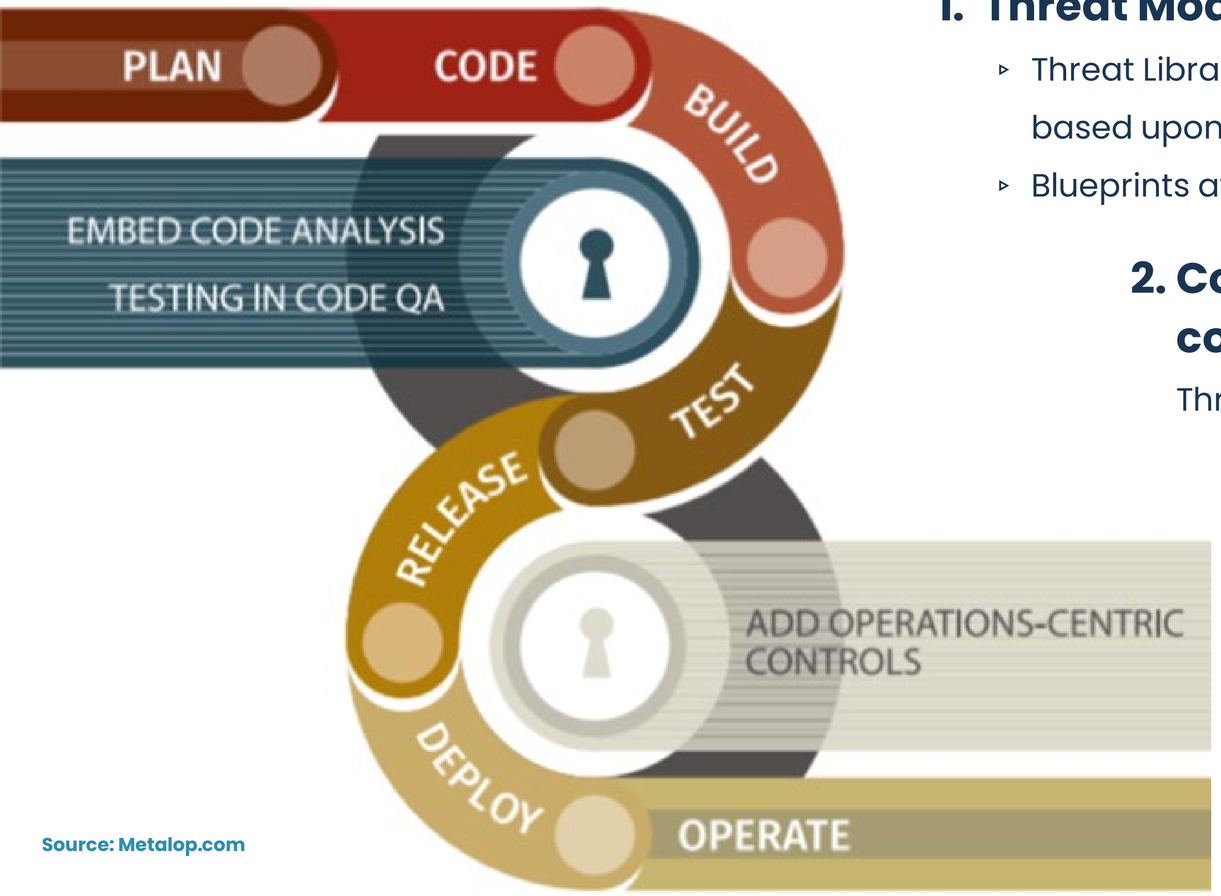
VERSPRITE

ISSA METRO ATLANTA

Building Valid Threat Libraries for Cloud Based Applications

Substantiating Threat Models with Threat Data

Leverage a Threat Model to Guide DevSecOps



Source: Metalop.com

1. **Threat Modeling activities lend well to DevSecOps stages**
   - Threat Library builds context of applicable menaces to Cloud application based upon industry, data model, and technology footprint
   - Blueprints attack patterns to test, vulns to check, controls to configure

2. **Correlating Threat Libraries to build as many security controls in DevOps is possible**

   Threats → Attacks → Vulns → Affected Components → Controls for Automation

2. **Fosters security automation in** Build, Test, Release, Deploy, **&** Operate **phases**
   - Threat Modeling (PASTA S1-S4) → Plan stage
   - Risk based Countermeasure Development (PASTA S7) → Code, Build, Deploy
   - Vulnerability Analysis (PASTA S5 → Deploy (Configuration), Operate
   - Threat Analysis (PASTA S4 → Operate (Monitoring), Plan)

Tony UcedaVélez

CEO/ Founder, VerSprite

VerSprite.com - Global Security Firm

- OWASP Atlanta Chapter Leader (past 10 years)
- Author, “Risk Centric Threat Modeling – Process for Attack Simulation & Threat Analysis”, Wiley June 2015
- Passionate global, threat modeling evangelist
- Dreams of bankrupting #infosec with intelligent, threat inspired DevSecOps automation

LinkedIn.com/tonyuv **@ t0nyuv**

Threat Considerations & Misinterpretations

Basic Tenants of Threat Libraries in Cloud Threat Models

"Cloud security automation can leverage threat models as blueprints; threat libraries that leverage both threat intel & data help kickoff evidence based DevSecOps security workflows"

Problem & Resolutions on Today's Threat Models

Cloud, Threat Confusion, Misuse Impairs Ability to Model Threats

Problem Statement:

Threat Models Are Not Addressing Cloud Related Threats

- Many threat modeling activities are foregoing the inclusion of threat considerations.
- Vulnerabilities ≠ Threats; DFDs ≠ Threat Models
- Since vulnerabilities do map to exploits, many equate exploits or attack patterns to threats
- Practitioners compelled to only look outwardly to threat intel vs. leveraging threat data
- AWS & Azure both provide centralized 'dashboard' of security threats, however, still overwhelming to look at
- Azure Security Center (now Hybrid) facilitates alerts per tenant
- Means Energy, Transportation sectors dependent on SaaS vendors for efforts between threat identification to mitigation

Proposed Resolution:

Help Substantiate Your Threat Model with Threat Data and Customer Threat Intelligence

- Important to substantiate your threats for your Cloud threat models
- Threat intelligence provides outside, industry threat perspectives
- However - threat data provides security events incidents that may support threat claims in a threat model
- Threat data can substantiate underlying attack patterns in a threat model
- SME/Security Champion conducting threat modeling can leverage threat intel and data

Clarifying Threat Terms Use & Abuses

Threats Against Cloud Castles – Key Threat Modeling

- **Threat modeling** should represent “Model of Threats”
  - Threat model can serve as blueprint for DevSecOps efforts across the **FULL** Cloud stack
- Remember Cloud can be SaaS, PaaS, IaaS, CaaS; Cloud is not just serverless apps, containers, or VMs
- Today, threats are often inferred from **Attack Surfaces** or **Vulnerabilities**
- Threats should point to viable attack patterns that can automated via automated testing
  - Example: Crypto mining threat (aka cryptojacking) via priv escalation attack to instantiate new EC2 instance
- “Threat Hunting” has completely perversed the use of **Threat Intelligence**
  - Reboot & refactor needed to iteratively feed threat models
- **Threat Data** may represent lessons learned from prior battles/ attacks logged in Cloud management logs, VMs, serverless apps

PASTA Methodology Applied to Cloud

- PASTA applies to the full stack, not just the App tier
- Stage I sets tone of importance around Cloud use cases, particularly in Energy sector where **use cases** can be baselined in Cloud Apps/Management APIs
- Stage II defines **technical scope** of app components; essentially can provide **attack surface** across full stack in CSP
- Stage III maps use cases to actors/worker processes and data sources in Cloud. Helps in **IAM** Cloud **policy configuration** via Cloud Mgt APIs.

- Stage IV correlates relevant threat patterns. Threat intelligence and threat data fed. **(Key focus of talk)**
- Stage V & VI – "**proof**" stages; prove viability; allow for integrated security testing in threat-led DevSecOps efforts
- Stage VII – Rationale for **countermeasure** development based upon **residual risk** can be incorporated into Design & Build phases of DevSecOps lifecycle
- Model is fed by Operate & Monitor phases in DevSecOps

Tiered Approach to PASTA DevSecOps Adoption

Scoping Cloud API PUTS & GETS Supports Evidence Driven Model

Blind Threat Model

- Industry 'Best Practice' Applied to app components
- Maps key goals of app or service and correlates to clear technical standards for architecture, hardening of server/ service, app framework, containers
- Applies Stage 1 & Stage 2 of PASTA

Evidence Driven Threat Model

- Integrate threat log data analysis
- Focus on logs that support attack vector w/ greatest motives (e.g. – TLS MITM vs. Injection based events)
- Correlate threat evidence for substantiating threat trends of attacks for target apps.

Full Risk Based Threat Model

- Ability to run statistical analysis/ probabilistic analysis on threat data & attack effectiveness
- Consider non-traditional attack vectors, still supporting threat motives.
- Conduct probabilistic analysis on threat data and attack sequences from pen testing efforts.

Collaboration in DevSecOps

Carnegie Mellon TMM November 2016 Study†

	BU/Product Groups						Corporate Functions							3rd Party	
APPLICATION THREAT MODELING ACTIVITIES per STAGE	**MGT**	**PMO**	**BA**	**ARC**	**SWE**	**QA**	**SYS**	**SOC**	**RL**	**PC**	**SA**	**EA**	**CTO**	**VA**	**PT**
STAGE 1 - DEFINE BUSINESS OBJECTIVES - Est. New TM = 2-4 hours | Est. Repeat TM = < 1 hour	A	R	R	A	I	I	I	–	I	R	I	I	R	–	–
Obtain business objectives for product or application	A	I	R	A	I	I	I	–	I	–	–	I	I	–	–
Identify regulatory compliance obligations	A	I	I	A	I	I	I	–	I	R	–	I	I	–	–
Define a risk profile or business criticality level for the application	A	I	I	A	I	I	I	–	I	C	I	I	R	–	–
Identify the key business use cases for the application/product	A	R	R	A	I	I	I	–	I	–	–	I	I	–	–
STAGE 2 - TECHNICAL SCOPE - Est. New TM = 3-4 hours | Est. Repeat TM = 1-3 hours	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
Enumerate software applications/database in support of product/application	I	I	C	A	R/A	C	I	–	–	–	–	C	I	–	–
Identify any client-side technologies (Flash, DHTML5, etc.)	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate system platforms that support product/application	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Identify all application/product actors	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate services needed for application/product use & management	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate 3rd party COTS needed for solution	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Identify 3rd party infrastructures, cloud solutions, hosted networks, mobile devices	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
STAGE 3 - APPLICATION DECOMPOSITION - Est. New TM = 8 hours | Est. Repeat TM = 4 hours	I	I	I	A	R	C	C	–	I	–	–	C	–	–	–
Perform data flow diagram of application environment	I	I	I	A	R	I	C	–	–	–	–	C	–	–	–
Define application trust boundaries/trust models	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Enumerate application actors	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Identify any stored procedures/batch processing	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Enumerate all application use cases (ex: login, account update, delete users, etc.)	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
STAGE 4 - THREAT ANALYSIS - Est. New TM = 6 hours | Est. Repeat TM = 2 hours	I	I	R/A	A	R/A	R/A	C	C	–	–	–	I	–	–	–
Gather/correlate relevant threat intel from internal/external threat groups	I	I	R/A	A	C	I	C	C	–	–	–	I	–	–	–
Review recent log data around application environment for heightened security alerts	–	–	I	A	R	R/A	I	C	–	–	–	I	–	–	–
Gather audit reports around access control violations	–	I	I	A	R	C	I	C	–	–	–	I	–	–	–
Identify probable threat motives, attack vectors & misuse cases	I	I	I	A	R/A	C	I	C	–	–	–	I	–	–	–
STAGE 5 - VULNERABILITY ASSESSMENT - Est. New TM = 12 hours | Est. Repeat TM = 6 hours	I	I	I	A	R	C	I	C	I	–	–	C	–	R/A	R
Conduct targeted vulnerability scans based upon threat analysis	–	–	–	A	R	C	I	C	I	–	–	I	–	R	R
Identify weak design patterns in architecture	–	–	–	A	R	C	I	–	–	–	–	C	–	R	C
Review/correlate existing vulnerability data	I	I	I	A	R	I	I	C	–	–	–	I	–	R/A	I
Map vulnerabilities to attack tree	–	I	I	A	R	I	I	–	–	–	–	C	–	C	I
STAGE 6 - ATTACK ENUMERATION - Est. New TM = 10 hours | Est. Repeat TM = 5 hours	I	I	I	A	R	R	–	–	I	–	–	C	I	I	R/A
Enumerate all inherent and targeted attacks for product/application	I	I	I	A	R	C	–	–	I	–	–	C	I	I	R/A
Map attack patterns to attack tree vulnerability branches (attack tree finalization)	–	–	–	A	R	C	–	–	I	–	–	C	–	I	A
Conduct targeted attacks to determine probability level of attack patterns	–	–	–	A	C	R	–	–	I	–	–	C	–	I	R/A
Reform threat analysis based upon exploitation results	I	I	I	A	R	C	–	–	I	–	–	C	I	I	C
STAGE 7 - RESIDUAL RISK ANALYSIS - Est. New & Repeat TM = 5 days (inc. countermeasure dev.)	C	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Review application/product risk analysis based upon completed threat analysis	I	I	I	A	R	C	I	C	I	I	C	C	I	I	R
List recommended countermeasures for residual risk reduction	I	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Re-evaluate overall application risk profile and report.	C	I	I	A	R	C	I	I	I	C	C	C	I	I	I

Roles Legend

MGT	Product Mgmt
PMO	Project Mgmt
BA	Business Analyst
ARC	Architect
SWE	Software Engineer
QA	Quality Assurance
SYS	SysAdmin
SOC	Security Operations
RL	IT Risk Leader
PC	Product Compliance
SA	Software Assurance
EA	Enterprise Architect
CTO	Administration
VA	Vuln Assessor
PT	Pen Tester

Corporate Functions

- Office of the CTO
- Compliance
- Security (ISRM)

RACI Legend

R	Responsible
A	Accountable
C	Consulted (2way)
I	Informed (1way)

- PnG (Persona non Grata) reflected least false positives
- PnG reflected consistent threats across multiple teams conducting threat analysis
- PASTA focuses on:
  - Substantiating models with real threats
  - Supporting threats via real attack patterns that can be tested (DevSecOps test cases)
  - Supporting vulns that map to attack patterns (e.g. – CWE/ CVE: CAPEC mapping)
  - Collaborative amongst various constituents

† https://insights.sei.cmu.edu/sei_blog/2016/11/cyber-threat-modeling-an-evaluation-of-three-methods.html

Objectives in Building a Threat Library

VERSPRITE

Learn to Substantiate Your Model

- FUD perceptions do not constitute valid threat patterns
- Threats help contextualize probability of threat occurrence for assets at risk
- Provides realistic considerations to real threats affecting critical infrastructure (i.e. – Transportation/ Energy)
- Threat patterns provide a top level hierarchy context to organize underlying attacks, vulnerabilities around crucial infrastructure being threat modeled

Role of the Threat Library

- Provides 'living' body of content around viable threats
- Should be revisited monthly to see if an evolving threat landscape warrants changes to the threat library
- Provides a list of threats that shape the pinnacle node of attack trees
- An exhaustive list is not the objective; a quality list is

Research

- Threat Data
- Threat Intelligence
- Industry Reports & Trends

Analyze

- Select most relevant threats
- Consider timing of threat info
- Attack patterns ≠ threats

Incorporate

- Prioritized top threats based upon assumed impact
- Threats serve as top nodes in attack tree

Break Bad Threat Consumption Habits

Importance of Consistency in Good Threat Information

Security Media Can Have Worst Threat Info

Vulnerability reports masquerading as threat information

Industry Incidents to Threat Considerations

Reported incidents against CI best form of auto-checking or adding to threat libraries

Function + Dysfunction Threat Mashup

- Collaboration between those that understand functional use + creative, threat driven approaches can easily kickstart a great threat library
- For Critical Instructure government resources provide good insight to the function of key industries and associated systems
- [ENERGY] European Commission (EC), Energy Expert Cyber Security Platform (EECSP) Expert Group
- [TRANSPORTATION] PT-ISAC (U.S) Public Transportation Info Sharing & Analysis Center
- Transit And Rail Intelligence Awareness Daily (TRIAD) replaced daily PT-ISAC report

VERSPRITE

Threat Modeling + DevOps in Energy Sector

Opportunities for Security Automation via Evidence Supported Threat Modeling

A brief case study on Cloud adoption in Oil & Gas and how an evidence supported library can be the cornerstone to a good threat model and foster security automation.

Building a Threat Library for Oil & Gas

DevSecOps Threat Tuning Begins with a Solid Threat Library

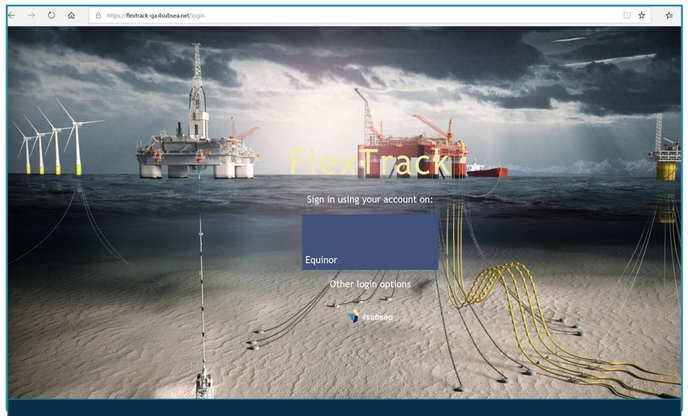
- Traditional threats to Oil & Gas are physical in nature
  - piracy
  - terrorism
  - insurgency
  - organized crime
  - civil protest
  - inter-state hostilities
  - vandalism
  - internal sabotage
- Highly competitive, capital intensive industry, depending on accuracy field data shapes future use of Cloud adoption
- Cyber related threats aim to incapacitate interconnected systems
  - **Taint Data** [Integrity, Availability] Research Exploration, Operations Data
  - **Extortion** via suppressing [Availability] of Cloud management panels or Cloud Energy SaaS Apps
  - **Mine Cryptocurrency** on PaaS infrastructure [Integrity]
  - **Steal Secrets** (e.g. - Exploration/ R&D) [Confidentiality]

Role Playing the Threat Actor

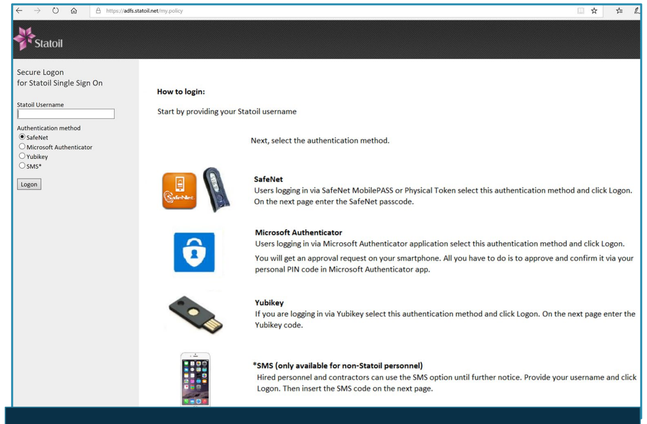
Cloud WellSpot Application under PASTA's Threat Analysis IV

Selecting a Cloud Target in Wellhead Operations

Targeted OSINT



FlexTrack Multi-Tenant Energy App



Authentication Components

Threat Library
- Sabotage
- Steal
- Extortion

Attack Surface
- Azure AD
- Web API
- Auth Panel

Attack Patterns
- Auth Bypass
- Social Eng
- Injection

Vulnerable Assets
- Web Server
- Web App
- Human

Sample Threat Model w/ Custom Oil & Gas Threat Library

Equinor's WellSpot Threat Model Summary Card

Threat Library

- Establish Persistence
- Steal Secrets
- Taint Data
- Sabotage
- Extortion
- Cryptojacking
- Tenant Hopping
- Cloud Admin Access

Threat Motives

Long term, multi-faceted compromise
Steal R&D Data, Wellhead locations, Well Performance Metrics
Affect accuracy in reporting for more macro economic or competitive reasons
Vengeance driven, corporate sabotage to largely disrupt availability of information, services
Hold hostage parts or complete IT infrastructure for the purposes of using as financial leverage.
Leverage compromised IT infrastructure in order to mine crypto currencies
Discover other Energy providers leveraging WellSpot multi-tenant cloud application
Obtain administrative access to control panel for aforementioned motives; sell access on black market.

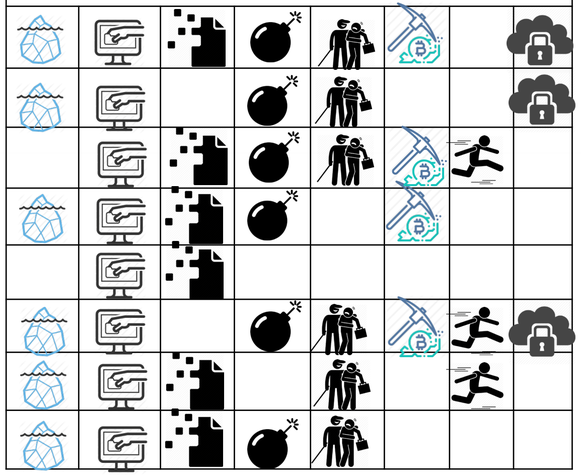
Attack Surface

- Employees/ Contractors
- Endpoints
- Web Apps/ APIs
- Internal Applications
- Domain Controllers
- Cloud Admin Panel/ API
- O365
- Network

Attack Patterns

Vishing, Smishing, Rogue SW
Drive-by-download, malware via docs, email
Injection based attacks, authentication bypass
Insider threats, rogue software
Pass the hash cracking attempts
Social Eng, Illicit Cloud Access via Auth Attacks
Targeted phishing over email vector
Network MITM

Associated Threats



Attack Tree Rooted by Sabotage Threat

Cloud WellSpot Application under PASTA's Threat Analysis IV

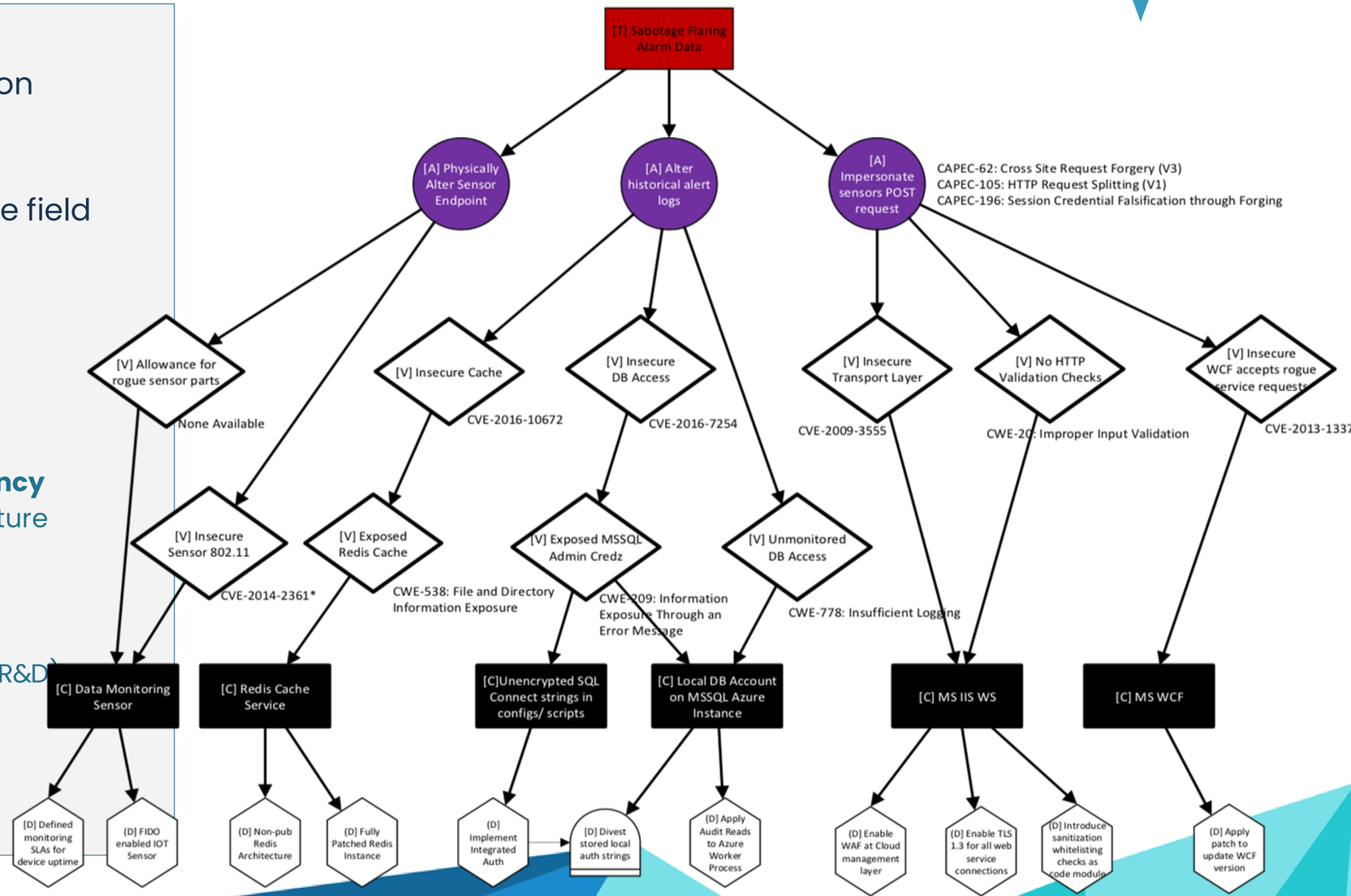
- Attack trees provide DevSecOps automation blueprint
- Oil & Gas depends on depends on accurate field data quickly; Cloud provides automation opportunity
- Cyber related threats aim to incapacitate interconnected systems

Taint Data [Integrity, Availability] Research Exploration, Operations Data

Mine Cryptocurrency on PaaS infrastructure [Integrity]

Extortion via suppressing [Availability] of Cloud management panels or Cloud Energy SaaS Apps

Steal Secrets (e.g. - Exploration/ R&D) [Confidentiality]



VERSPRITE

Mapping a Detective Control to a Threat Target

Script Mapping Countermeasures to Threat Targets

Detective Control Checks to Automate for Exposed Redis

Detective control can be implemented during the DevSecOps environment Build process or Deploy, Operate, & Maintain cycles

Check validates FW rules in front of Redis Cache service for Cloud Energy application

Again, target asset or component is supported by threat model, thereby rationalizing its prioritization as a control check

Script Mapping Countermeasures to Threat Targets

Detective Control Checks to Automate for Exposed Redis

Result Tracking on API Responses

- Detective checks help to establish a baseline of security configuration under Monitor & Operate DevSecOps phases
- Detective Open Source tools like:
  - **Scout2**
    https://github.com/nccgroup/Scout2
  - **Cloud Security Suite**
    https://github.com/SecurityFTW/cs-suite
  - **Prowler**
    https://github.com/toniblyx/prowler

RedisCacheFirewallRulesList

Sample Response

Status code: 200

JSON Copy


```
{
  "value": [
    {
      "id": "/subscriptions/subid/resourceGroups/rg1/providers/Microsoft.Cache/Redis/cache1/firewallRules/rule1",
      "name": "rule1",
      "type": "Microsoft.Cache/Redis/firewallRules",
      "properties": {
        "startIP": "192.168.1.1",
        "endIP": "192.168.1.4"
      }
    },
    {
      "id": "/subscriptions/subid/resourceGroups/rg1/providers/Microsoft.Cache/Redis/cache1/firewallRules/rule2",
      "name": "rule2",
      "type": "Microsoft.Cache/Redis/firewallRules",
      "properties": {
        "startIP": "192.169.1.0",
        "endIP": "192.169.1.255"
      }
    }
  ]
}
```

Script Mapping Countermeasures to Threat Targets

Detective Control Checks to Automate for Exposed Redis

RedisCacheFirewallRuleCreate

Sample Request

HTTP Copy

```
PUT
https://management.azure.com/subscriptions/subid/resourceGroups/rg1/providers/Microsoft.Cache/Redis/cache1/firewa
api-version=2016-04-01
```

Request Body

JSON Copy

```
{
  "properties": {
    "startIP": "192.168.1.1",
    "endIP": "192.168.1.4"
  }
}
```

Sample Response

Status code: 200

JSON Copy

```
{
  "id": "/subscriptions/subid/resourceGroups/rg1/providers/Microsoft.Cache/Redis/cache1/firewallRules/rule1",
  "name": "cache1/rule1",
  "type": "Microsoft.Cache/Redis/firewallRules",
  "properties": {
    "startIP": "192.168.1.1",
    "endIP": "192.168.1.4"
  }
}
```

Result Tracking on API Responses

- Detective checks help to establish a baseline of security configuration under Monitor & Operate DevSecOps phases
- Altering or creating a new rule is also easy by simply changing http method
- PUT https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Cache/Redis/{cacheName}/firewallRules/{ruleName}?api-version=2016-04-01
- Creating new rule can be done as part of Build or Deploy phases.

Script Mapping Countermeasures to Threat Targets

Detective Control Checks to Automate for Exposed Redis

RedisCacheFirewallRuleCreate

Sample Request

HTTP Copy

```
PUT
https://management.azure.com/subscriptions/subid/resourceGroups/rg1/providers/Microsoft.Cache/Redis/cache1/firewa
api-version=2016-04-01
```

Request Body

JSON Copy

```
{
  "properties": {
    "startIP": "192.168.1.1",
    "endIP": "192.168.1.4"
  }
}
```

Sample Response

Status code: 200

JSON Copy

```
{
  "id": "/subscriptions/subid/resourceGroups/rg1/providers/Microsoft.Cache/Redis/cache1/firewallRules/rule1",
  "name": "cache1/rule1",
  "type": "Microsoft.Cache/Redis/firewallRules",
  "properties": {
    "startIP": "192.168.1.1",
    "endIP": "192.168.1.4"
  }
}
```

Result Tracking on API Responses

- Detective checks help to establish a baseline of security configuration under Monitor & Operate DevSecOps phases
- Altering or creating a new rule is also easy by simply changing http method
- PUT https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Cache/Redis/{cacheName}/firewallRules/{ruleName}?api-version=2016-04-01
- Creating new rule can be done as part of Build or Deploy phases.

AWS Automation Opportunities

JSON Supported Web Interfaces Facilitates Security Checks


```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "[redacted]",
        "arn": "arn:aws:sts::019439391423:assumed-
role/vs_audit_instance_profile_role/i-0be51d801db986e86",
        "accountId": "[redacted]",
        "accessKeyId": "[redacted]",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-06-26T19:38:22Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAJIR4T73QJ2MJBBAZQ",
            "arn":
"arn:aws:iam::[redacted]:role/vs_audit_instance_profile_role",
            "accountId": "[redacted]",
            "userName": "vs_audit_instance_profile_role"
          }
        }
      },
      "eventTime": "2018-06-26T20:05:23Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "DescribeSubnets",
      "awsRegion": "us-west-1",
      "sourceIPAddress": "54.71.128.16",
      "userAgent": "Boto3/1.4.6 Python/2.7.14 Linux/4.14.33-51.37.amzn1.x86_64
Botocore/1.10.45",
      "requestParameters": {
        "subnetSet": {},
        "filterSet": {}
      },
      "responseElements": null,
      "requestID": "36718327-680e-49e8-858b-10c23e966b9b",
      "eventID": "6b1ee381-de43-4d3a-8a25-881eba65b693",
      "eventType": "AwsApiCall",
      "recipientAccountId": "019439391423"
    },
```


Security, Identity & Compliance

- AWS Identity and Access Management (IAM)
- Amazon Cloud Directory
- Amazon Cognito
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- AWS Certificate Manager
- AWS CloudHSM
- AWS Directory Service
- AWS Firewall Manager
- AWS Key Management Service
- AWS Organizations
- AWS Secrets Manager
- AWS Single Sign-On
- AWS Shield
- AWS WAF
- AWS Artifact

- Detective controls against CloudTrail web API allows for detective audit checks.
- Image on far left identifies if subnetting is present within a VPC for an AWS account. Useful for determining if subnetting perhaps needs to be present with logical ACLs applied.

Azure Security Manager (Hybrid)

Comparing & Integrating CloudSec Ops to TM Led DevSecOps

Problem Statement: Threat Models Are Not Addressing Cloud Related Threats

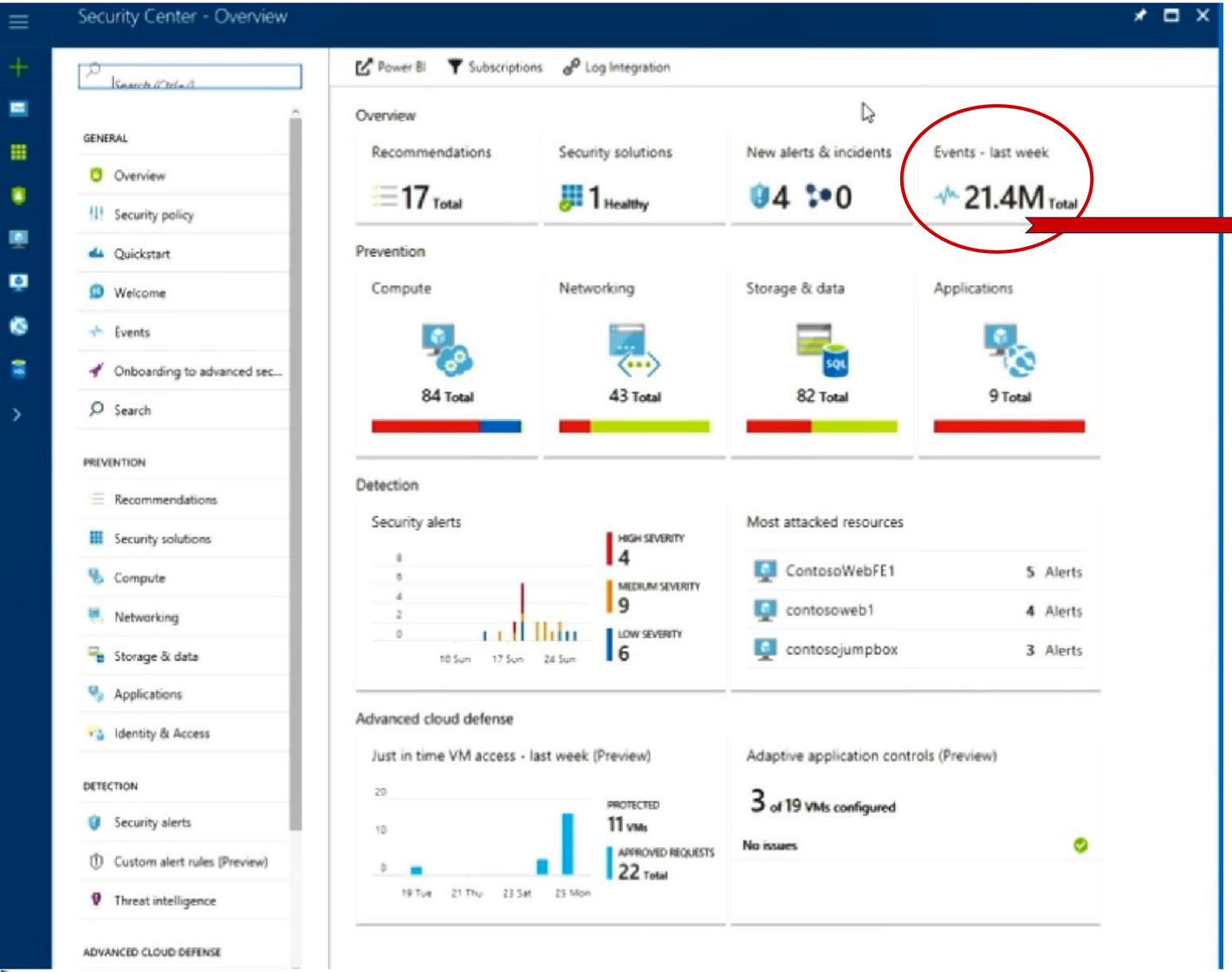
- Many threat modeling activities are foregoing the inclusion of threat considerations.
- Vulnerabilities ≠ Threats; DFDs ≠ Threat Models
- Since vulnerabilities do map to exploits, many equate exploits or attack patterns to threats
- Practitioners compelled to only look outwardly to threat intel vs. leveraging threat data
- AWS & Azure both provide centralized ‘dashboard’ of security threats, however, still overwhelming to look at.
- Azure Security Center (now Hybrid) facilitates alerts per tenant.
- Means Energy, Transportation sectors dependent on SaaS vendors for efforts between threat identification to mitigation.

Proposed Resolution: Help Substantiate Your Threat Model with Threat Data and Customer Threat Intelligence

- Important to substantiate your threats for your Cloud threat models
- Threat intelligence provides outside, industry threat perspectives
- However - threat data provides security events incidents that may support threat claims in a threat model
- Threat data can substantiate underlying attack patterns in a threat model
- SME/Security Champion conducting threat modeling can leverage threat intel and data

Azure Security Manager (Hybrid)

Comparing & Integrating CloudSec Ops to TM Led DevSecOps



Focused vs. Traditional

1. Azure provides centralized security information via Hybrid compared to 7 different AWS security product subscriptions

2. 4SubSea management of WellSpot in Azure, following a traditional approach will be largely vuln, event driven
   - Blind to a threat library or model
   - Not fueling threat data back into a threat model
   - Traditional approach would still be overwhelming to automate – ***where do you start?***

3. Cloud security dashboards today are simply carrying traditional SOC data
   - Although Azure does great job of aggregating:
     - WAF Alerts
     - Policy violations
     - VM vulnerabilities via partner scans or Azure agents - (configuration checks)
   - Threat context is still missing

4. For Energy sector, is your SaaS provider doing either – traditional security driven or evidence, threat model supported SaaS management?

4. Threat inspired management of Cloud events is more **focused & iterative**.
   *Azure Hybrid is per tenant

VERSPRITE

The Future of Your Threat Lib & Security Automation

Industry Perspective + Adversarial Tendencies

"Understanding a range of threat scenarios provides the basis for security readiness and opportunity for security automation."

Mindset to Build Future Threat Libs

Business + Hacker + Technologist = Good Threat Lib

Global Economic / Business

Business perspective keeps understanding in terms of what are ultimately business threats, not necessarily security threats.

Hacker

Hacker or criminal mindset is helpful in emulating the psych needed to circumvent barriers for the purposes of achieving threat objectives to a criminal or criminal group.

Sound Technologists

Attack patterns, vulns, and countermeasures will largely be technical. Knowing how they work and how to automate places an important role.

Resources & References | Grading Online Threat Information Sources

Threat Libraries Are Simple, Useful, Informative

VERSPRITE

PT-ISAC :: Transportation (U.S)

C-

TRIAD is the Transit & Rail Intelligence Awareness Daily replaces daily PT-ISAC reports. Email based.

ISACs in general reflect prior incident information with limited IOC data. (except: FS-ISAC)

European Commission on Energy Sector

A+

CybSec in Energy Sector
https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

DOE (U.S) Assessment of Electricity Disruption Incident Response Capabilities

B+

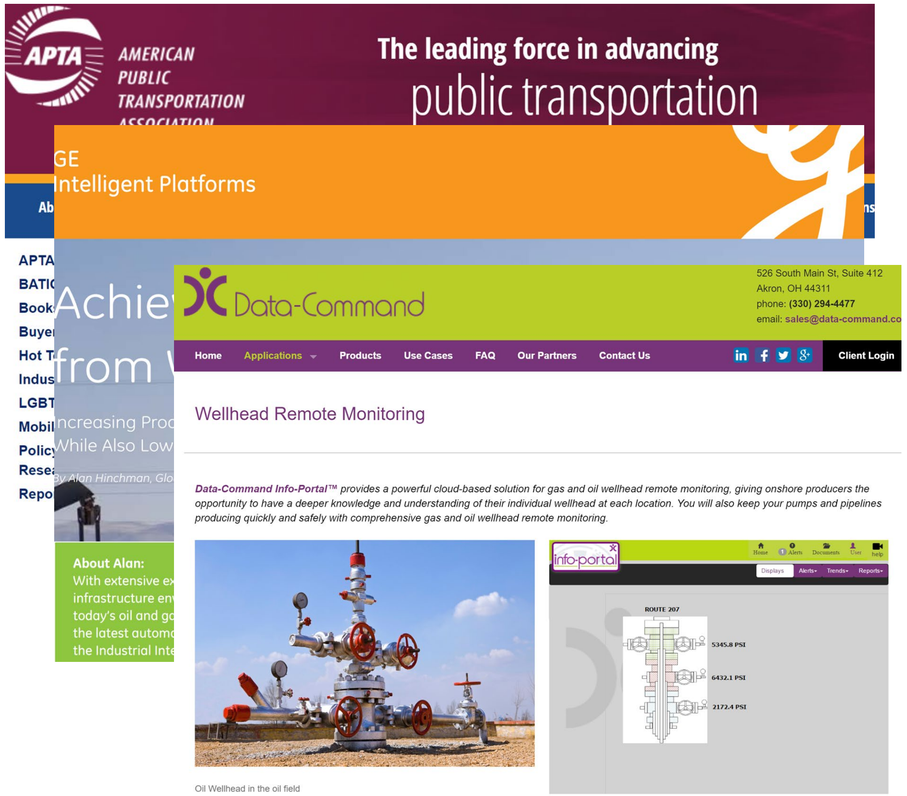
https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf

Twitter, Google News Alerts

A-

Industry Leaders (GE), Data Command, & OEM leaders and their sector reports on data reliance for operations

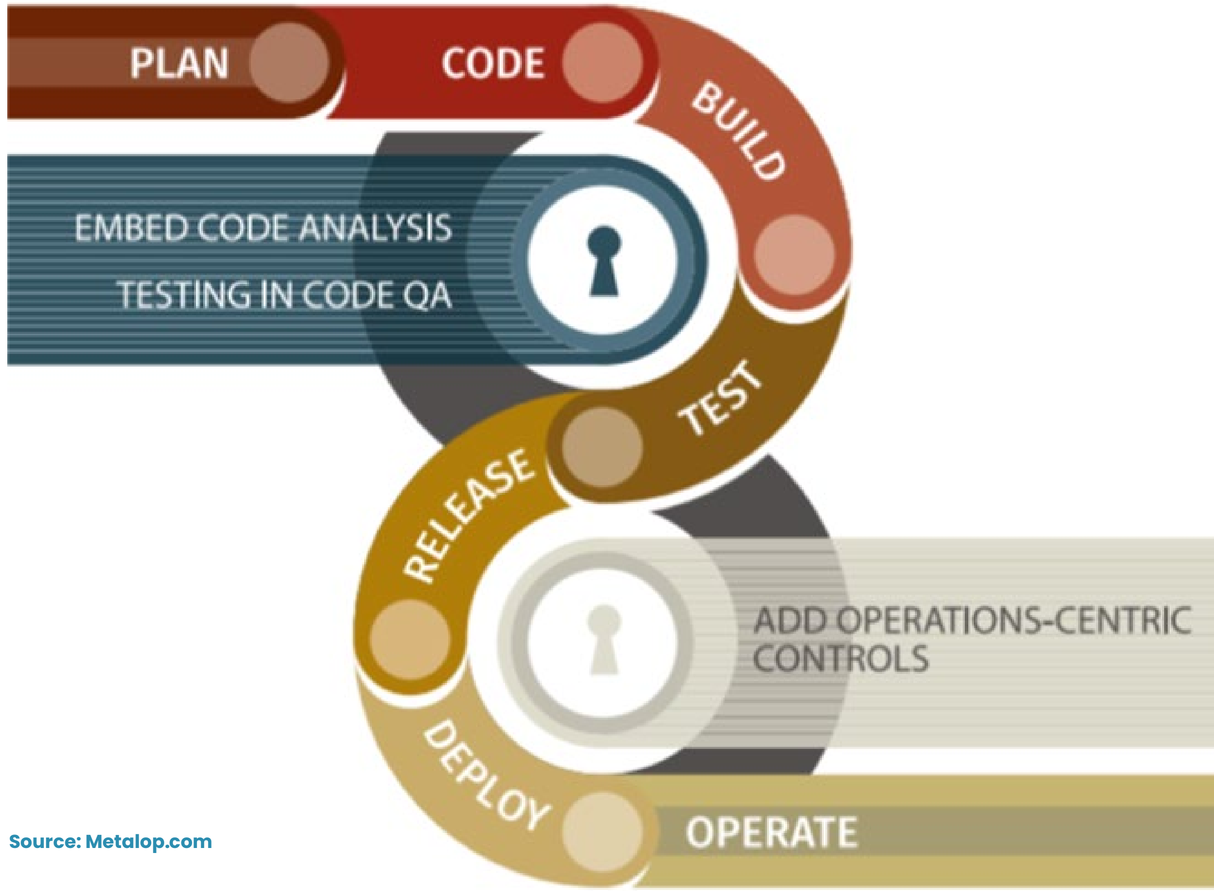
A+



Oil Wellhead in the oil field

Standardization, Correlation Key to Automation in Cloud

1. “Cloud” encompass management PaaS/ IaaS layer that has exposed APIs and web UI interface
2. “Cloud” also encompasses the full tech stack within your SaaS. Agent or traditional agentless scans from within the Cloud remain.
3. Left Sided Security opportunities begin w/ a Threat inspired Threat Model helps define security objectives in PLAN, CODE, & BUILD efforts
4. External threat intelligence feeds are noisy. TAXII services still need to evolve and follow a schema that can easily map CAPEC, CVEs, CWEs
5. Threat to Countermeasure to Threat Re-Learning automation will come from the private sector.
6. Lessons from SCAP shortcomings in mass adoption
7. STIX, TAXII MITRE divestiture; OASIS schema changes
8. Web supported interfaces facilitate greater automation via workflows

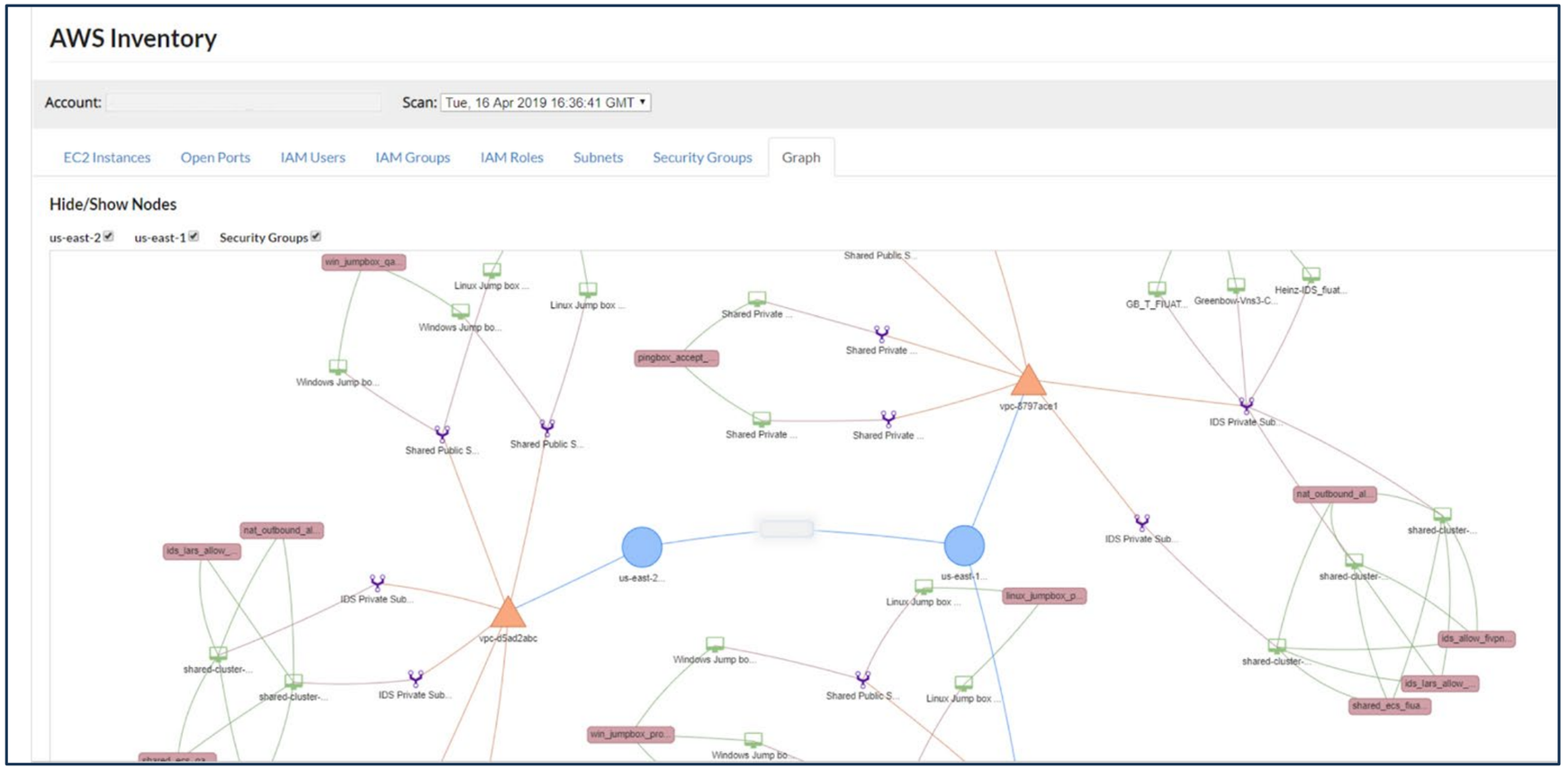


Source: Metalop.com

Questions?

- @t0nyuv
- www.linkedin.com/tonyuv
- tonyuv@versprite.com
- VerSprite.com/security-resources/

LinkedIn.com/tonyuv @t0nyuv


AWS Inventory
Account:
Scan: Tue, 16 Apr 2019 16:36:41 GMT
EC2 Instances
Open Ports
IAM Users
IAM Groups
IAM Roles
Subnets
Security Groups
Graph
Hide/Show Nodes
us-east-2
us-east-1
Security Groups
win_jumpbox_qa...
Linux Jump box ...
Linux Jump box ...
Windows Jump bo...
Windows Jump bo...
Shared Public S...
Shared Public S...
Shared Private ...
Shared Private ...
pingbox_accept_...
Shared Private ...
Shared Private ...
Shared Public S...
vpc-6797ace1
GB_T_FIUAT...
Greenbow-Vns3-C...
Heinz-IDS_fiuat...
IDS Private Sub...
nat_outbound_al...
shared-cluster-...
nat_outbound_al...
ids_lars_allow_...
IDS Private Sub...
vpc-d5ad2abc
us-east-2...
us-east-1...
Linux Jump box ...
linux_jumpbox_p...
IDS Private Sub...
shared-cluster-...
shared-cluster-...
IDS Private Sub...
Windows Jump bo...
Shared Public S...
Linux Jump box ...
win_jumpbox_pro...
Windows Jump bo...
shared-cluster-...
shared-cluster-...
ids_allow_fivpn...
ids_lars_allow_...
shared_ecs_fiua...