Building Valid Threat Libraries for Cloud Based Applications

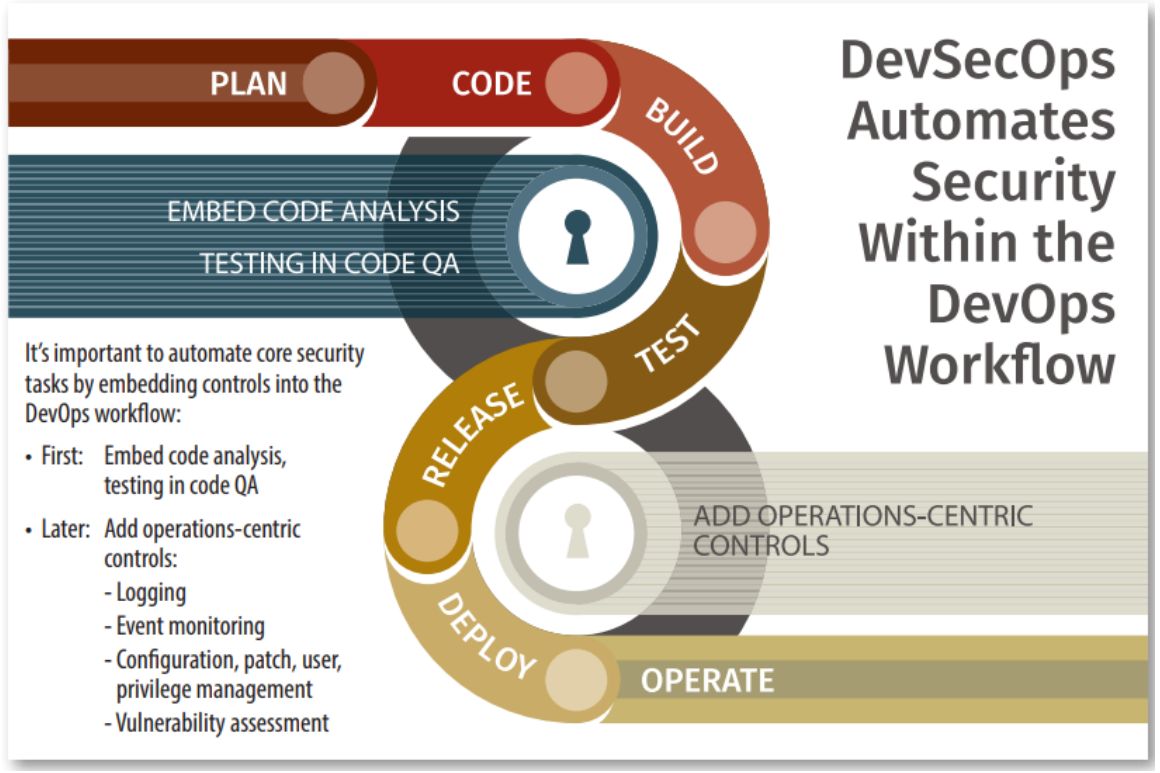
Substantiating Threat Models w/ Threat Data

Tony UcedaVelez // @t0nyuv

Talk Objectives

Tony UcedaVelez // @t0nyuv

Leverage a Threat Model to guide



***Source**: metalop.com*

1. **Threat Modeling activities lend well to DevSecOps stages**
   i. 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 security controls in DevOps is possible.**
   i. Threats → Attacks → Vulns → Affected Components → Controls for Automation
3. **Fosters security automation in Building, Test, Release, Deploy, & Operate phases.**
   i. Threat Modeling (PASTA S1-S4) → Plan stage
   ii. Risk based Countermeasure Development (PASTA S7) → Code, Build, Deploy

Speaker Background

Tony UcedaVelez // @t0nyuv

Bio & Background

- **CEO/ Founder**, VerSprite (www.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
- ~25 years of diverse IT/ Security experience in software development, architecture, pen testing, threat modeling, sys admin, security operations
- Dreams of bankrupting #infosec with intelligent, threat inspired DevSecOps automation

@t0nyuv
www.linkedin.com/tonyuv
tonyuv@versprite.com
https://versprite.com/security-resources/blog/

Threat Considerations & Misinterpretations

Basic Tenants of Threat Libraries in Cloud Threat Models

Problem & Resolutions on Today's Threat Models

Cloud Threat Confusion, Misuse Impairs Ability to Model Threats

Tony UceedaVelez // @t0nyuv

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 w/ Threat Data & 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 Points to Consider

Tony UcedaVelez //
@t0nyuv

- ***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

Tony UcedaVelez // @t0nyuv

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

Tony UcedaVelez // @t0nyuv

APPLICATION THREAT MODELING ACTIVITIES per STAGE	BU/Product Groups						Corporate Functions							3rd Party	
	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	–	I	–	–	C	I	–	–
Identify any client-side technologies (Flash, DHTML5, etc.)	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
Enumerate system platforms that support product/application	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
Identify all application/product actors	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
Enumerate services needed for application/product use & management	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
Enumerate 3rd party COTS needed for solution	I	I	C	A	R/A	C	I	–	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
Perform threat analysis based upon exploitation results	I	I	I	A	R	C	I	C	I	I	C	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

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 (2 way)
I	Informed (1way)

- PnG 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

Objectives in Building a Threat

Tony UcedaVelez // @t0nyuv

Research

- Threat Data
- Threat Intelligence
- Industry Reports/ Trends

Analyze

- Select most relevant threats
- Consider timing of threat info
- Remember that attack patterns ≠ threats

Incorporate

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

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.

Break Bad Threat Consumption Habits

Importance of Consistency in Good Threat Information

Tony UcedaVelez // @t0nyuv

CSO FROM IDG

Register

1. Data breaches

A data breach might be the primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices, CSA says. It might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual property. An organization's cloud-based data may have value to different parties for different reasons. The risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.

[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!]

2. Insufficient identity, credential, and access management

Bad actors masquerading as legitimate users, operators, or developers can read, modify, and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source, CSA says. As a result, insufficient identity, credential, or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users.

SponsoredPost Sponsored by G-Research
The AI Poker revolution
Alessandro, a Quantitative Researcher at G-Research, discusses the impact Artificial Intelligence attempts to have on imperfect information games such a Poker

3. Insecure interfaces and application programming interfaces (APIs)

Cloud providers expose a set of software user interfaces (UIs) or APIs that customers use to manage and interact with cloud services. Provisioning, management, and monitoring are all performed with these interfaces, and the security and availability of general cloud services depends on the security of APIs, CSA says. They need to be designed to protect against accidental and malicious attempts to circumvent policy.

4. System vulnerabilities

Security Media Can Have Worst Threat Info

- Vulnerability reports masquerading as threat information

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

Industry Incidents to Threat Considerations

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

Threat Modeling + DevOps in Energy Sector

Opportunities for Security Automation via Evidence Supported Threat Modeling

Building a Threat Library for Oil & Gas

DevSecOps Threat Tuning Begins w/ a Solid Threat Library

Building a Threat Library for Gas & Oil Players

- 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 intense 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

Equinor (formerly Statoil) Example for Wellhead Operations Application

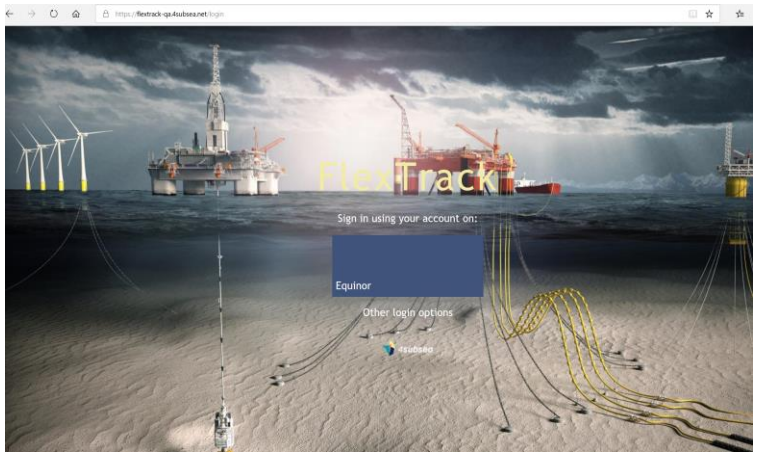
Selecting a Cloud Target in Wellhead Operations

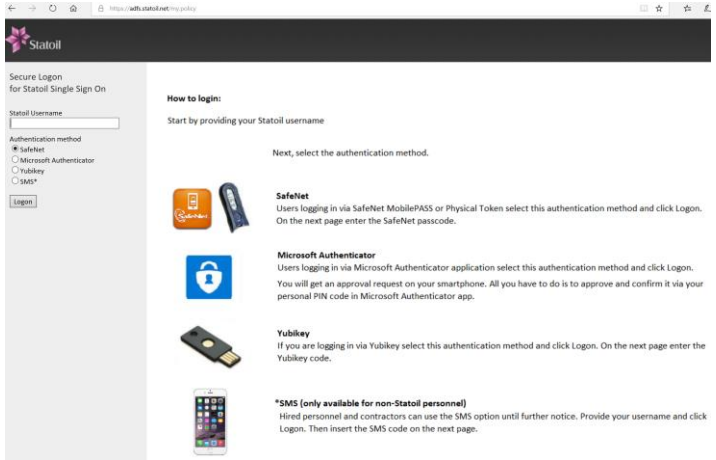
SOLUTIONS RESOURCES NEWS CAREER ABOUT CONTACT

4subsea

Statoil's Trouble-free Move to the Cloud

Statoil selected the platform Microsoft Azure for the software WellSpot™, a solution that supports workflows and processes for efficient, digitised operation of wellheads.

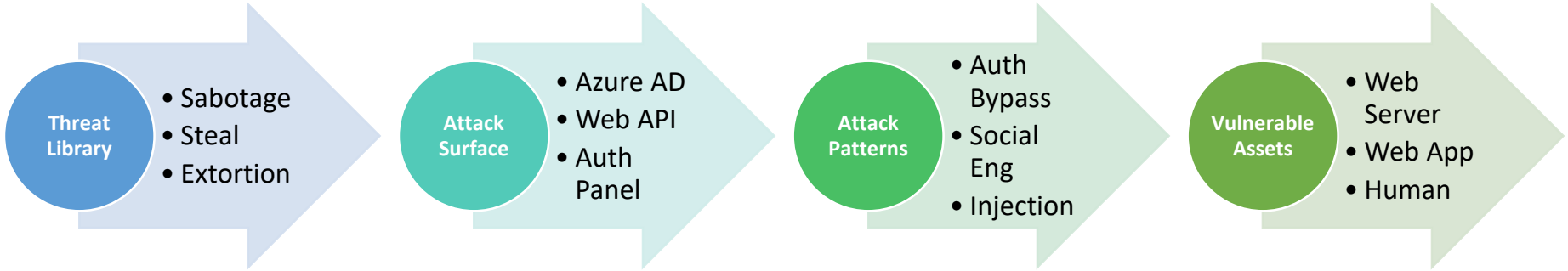




Targeted OSINT

lexTrack Multi-Tenant Energy App

Authentication



Sample Threat Model w/ Custom Oil & Gas Threat Library

Equinor's WellSpot Threat Model Summary Card

Tony UcedaVelez // @t0nyuv

OWASP AppSec Europe
London 2nd-6th June 2018

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.

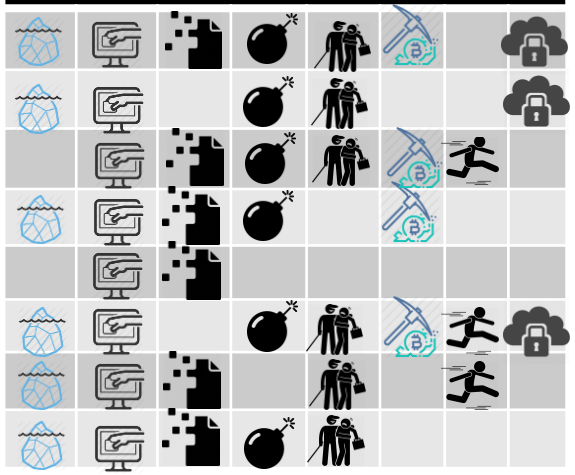
Attack Surface

- *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 by-pass
Insider threats, rogue software
Pass the hash cracking attempts
Social Eng, Illicit Cloud Access via Auth Attacks
Targeted phishing over email vector
Network MITM

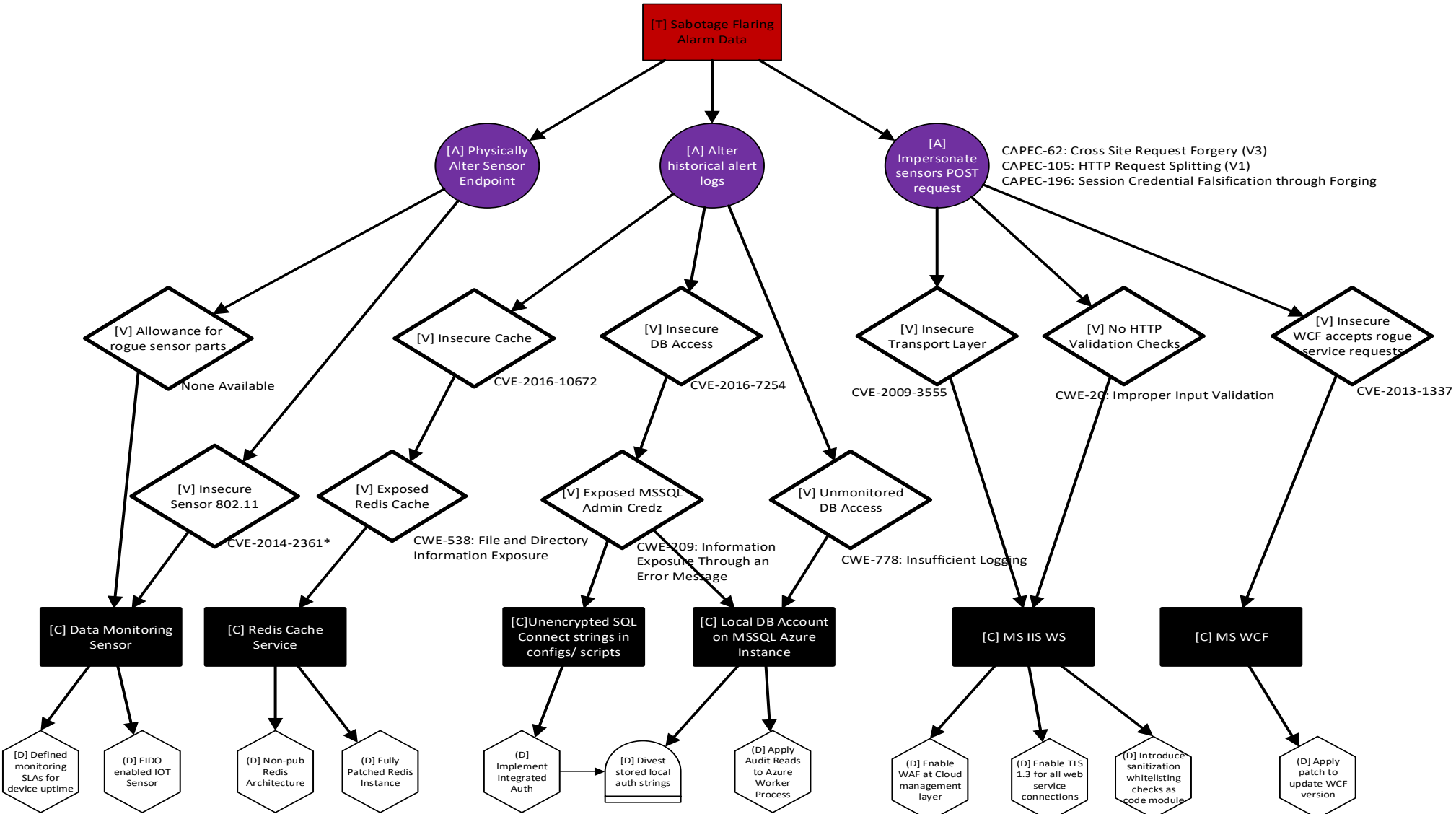
Associated Threats



Attack Tree Rooted by Sabotage Threat

Cloud WellSpot Application under PASTA's Threat Analysis IV

Tony Ueda Velez // @t0nyuv



- 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
  - **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]

Script Mapping Countermeasures to Threat Targets

Detective Control Checks to Automate for Exposed Redis

Tony UcedaVelez // @t0nyuv

RedisCacheFirewallRulesList

Sample Request

HTTP | Copy

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

Mapping a Detective Control to a Threat Target

- 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 (continued)

Tony UcedaVelez // @t0nyuv

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"
      }
    }
  ]
}
```


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),
  - Prowler https://github.com/toniblyx/prowler)
  - Cloud Security Suite https://github.com/SecurityFTW/cs-suite

Script Mapping Countermeasures to Threat Targets

Preventative Control Checks to Automate for Exposed Redis

Tony UcedaVelez // @t0nyuv

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

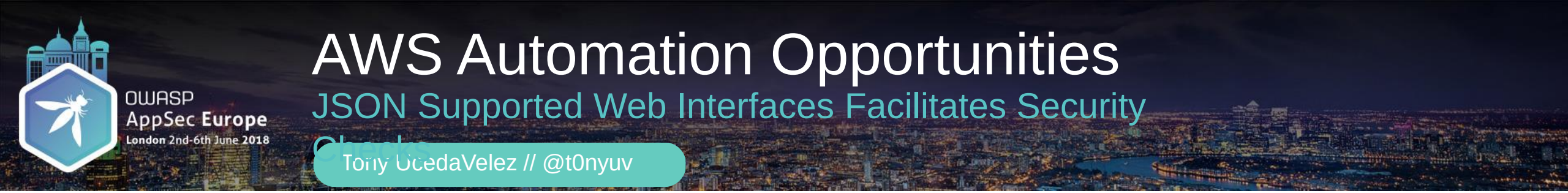
Status code: 200

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

Tony UcedaVelez // @t0nyuv


```
{
      "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

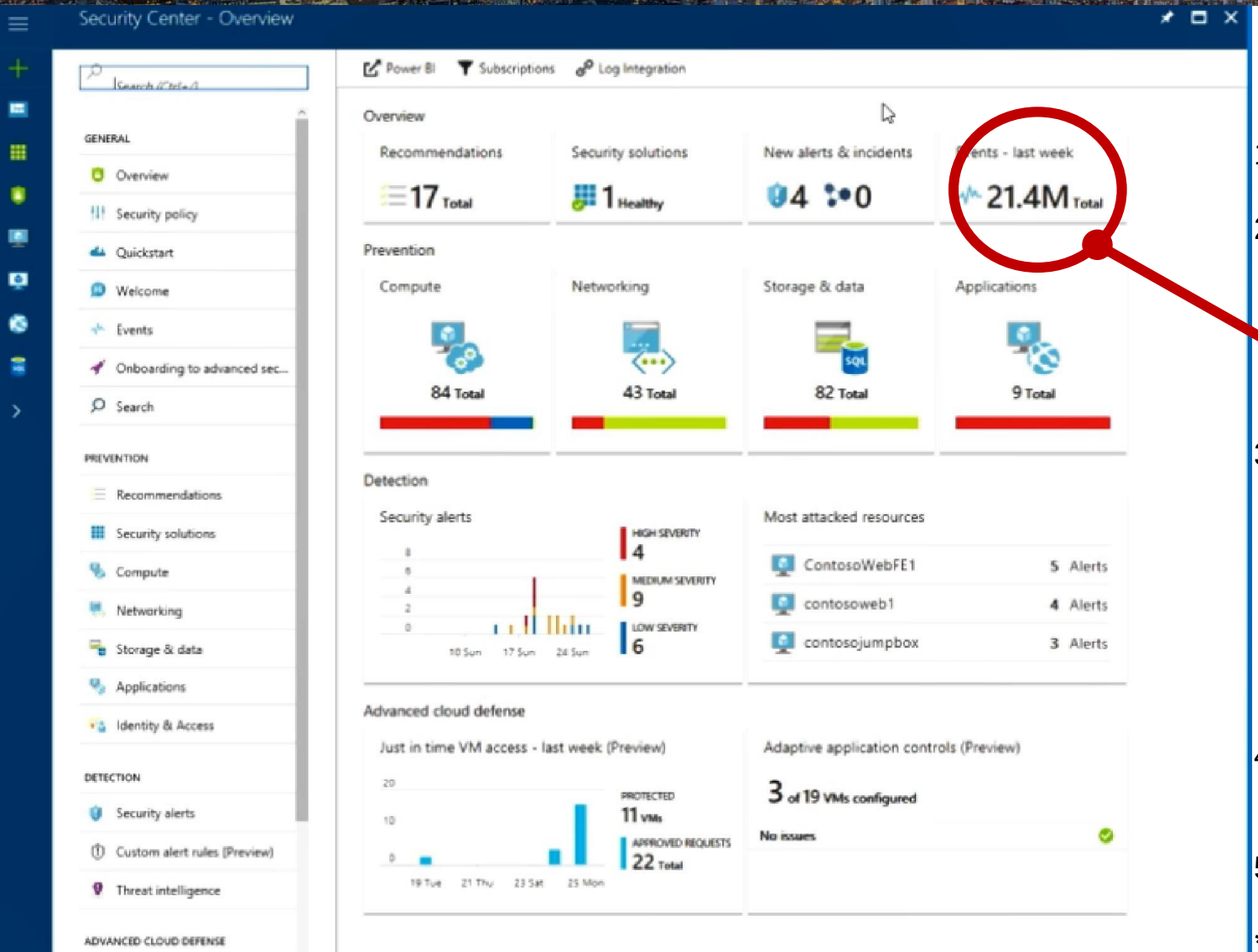
- Detective controls against CloudTrail web API allows for detective audit checks.
- Image on far left identifies if subnetting is present within a VPC for an AWS account. Useful for determining if subnetting perhaps needs to be present with logical ACLs applied.

OWASP AppSec Europe
London 2nd-6th June 2018

Azure Security Manager (Hybrid)

Comparing & Integrating CloudSec Ops to TM Led DevSecOps

Tony UcedaVélez // @t0nyuv



Focused vs. Traditiona

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
    1. Blind to a threat library or model
    2. Not fueling threat data back into a threat model
    3. Traditional approach would still be overwhelming to automate – where do you start?
3. Cloud security dashboards today are simply carrying traditional SOC data
    1. Although Azure does great job of aggregating:
        1. WAF Alerts
        2. Policy violations
        3. VM vulnerabilities via partner scans or Azure agents (configuration checks)
    2. 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?
5. Threat inspired management of Cloud events is more ***focused & iterative.***

Azure Hybrid is per tenant

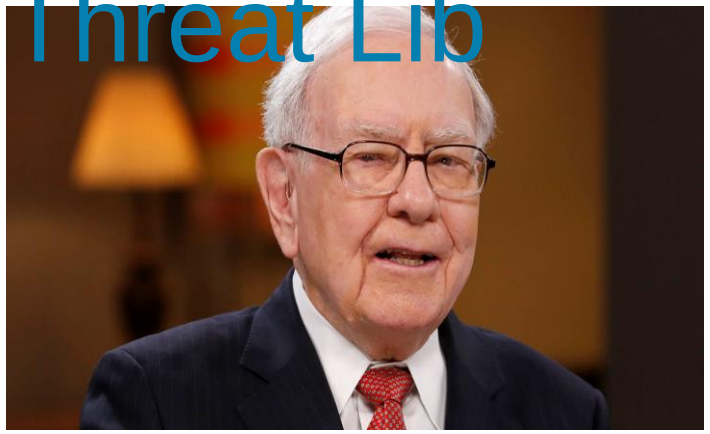
The Future of Your Threat Lib & Security Automation

Industry Perspective + Adversarial Tendencies

Mindset to Build Future Threat

Tony UcedaVelez // @t0nyuv

Business + Hacker + Technologist = Good Threat Lib



Global Economic / Business

Hacker

Sound Technologists

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

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.

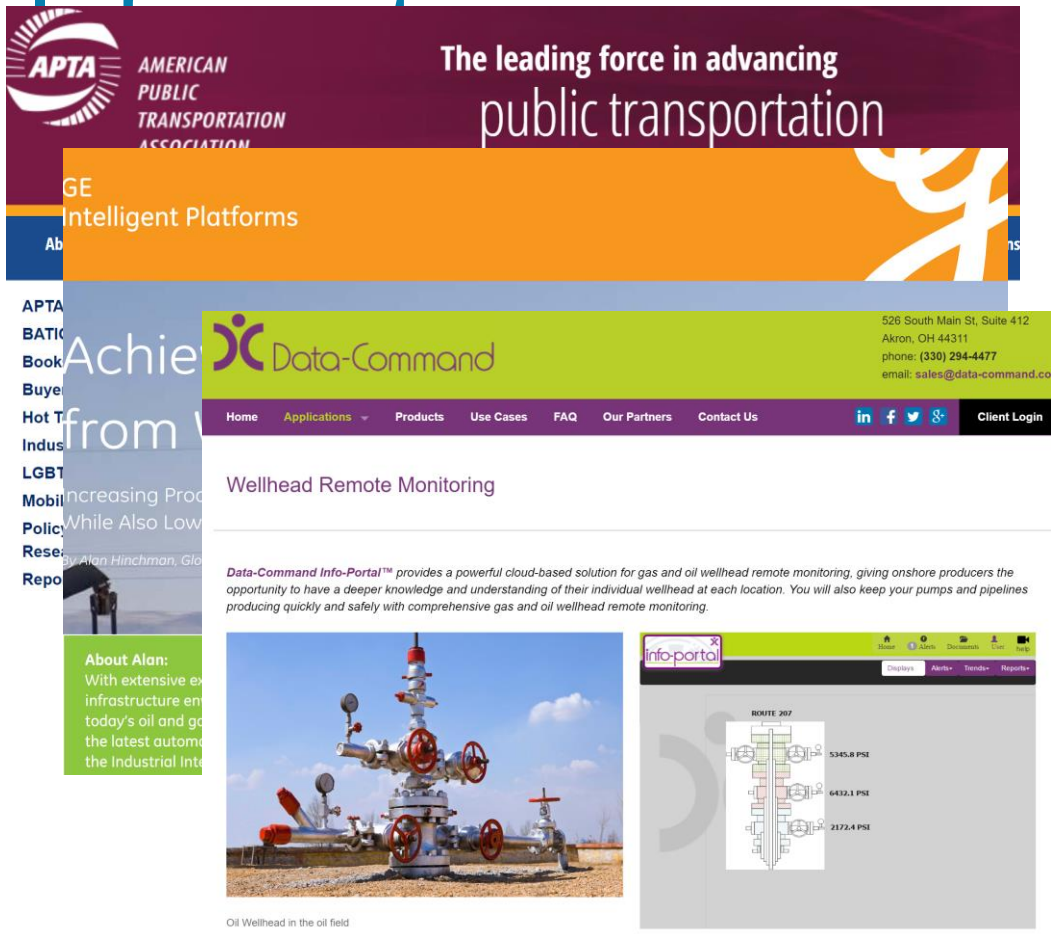
Attack patterns, vulns, and countermeasures will largely be technical. Knowing how they work and how to automate places an

Resources & References

Grading Online Threat Information Sources

Tony UcedaVelez // @t0nyuv

Threat Libraries Are Simple, Useful,



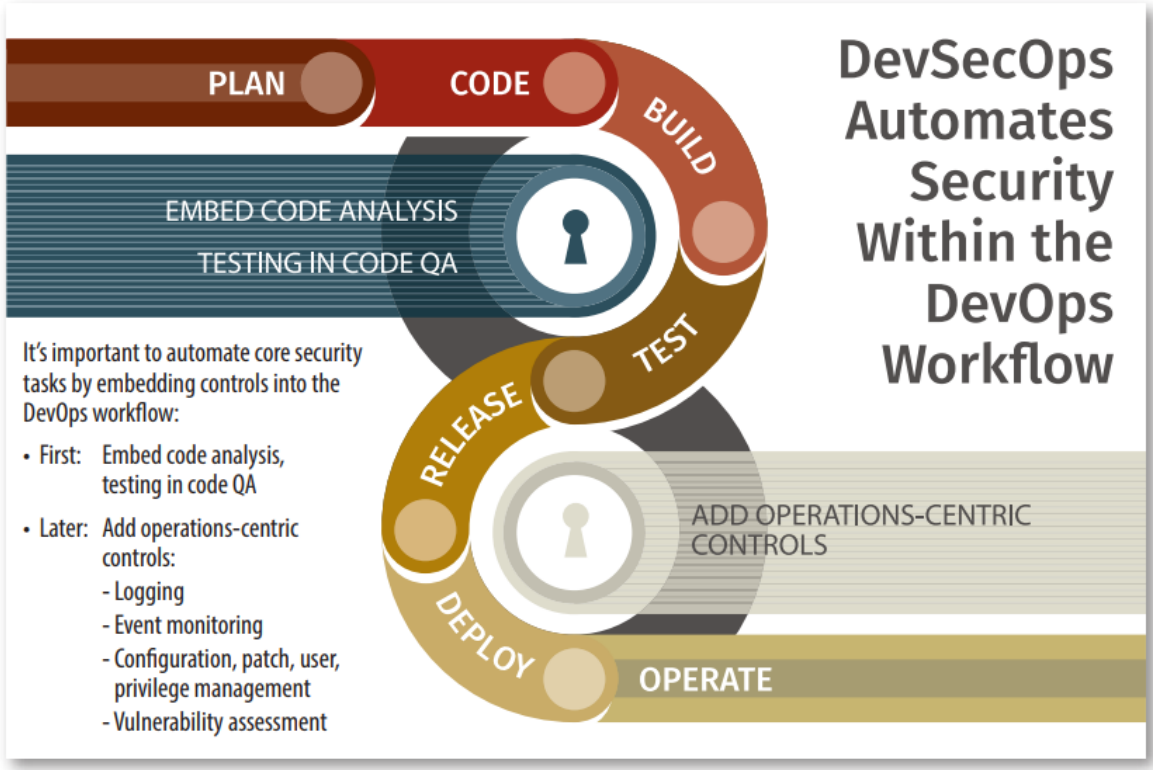
1. **PT-ISAC :: Transportation (U.S)** **C-**
   - TRIAD is the Transit & Rail Intelligence Awareness Daily replaces daily PT-ISAC reports. Email based.
   - ISACs in general reflect prior incident information with limited IOC data. (except: FS-ISAC)
2. **European Commission on Energy Sector** **A+**
   1. CybSec in Energy Sector https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
   2. DOE (U.S) Assessment of Electricity Disruption Incident Response Capabilities https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf **B+**
3. **Twitter, Google News Alerts** **A-**

Closing Remarks & Future Outlook

Threat Libs Contextualizing Security Info & Automation

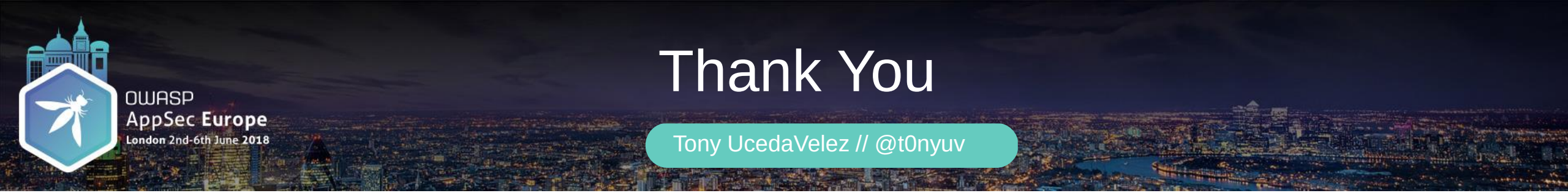
Tony UcedaVelez // @t0nyuv

Standardization, Correlation key to Automation in Cloud



***Source**: metalop.com*

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.
    1. Lessons from SCAP shortcomings in mass adoption
    2. STIX, TAXII MITRE divestiture; OASIS schema changes
6. Web supported interfaces facilitate greater automation via workflows



Thank You

Tony UcedaVelez // @t0nyuv

Questions?

@t0nyuv
www.linkedin.com/tonyuv
tonyuv@versprite.com
https://versprite.com/security-resources/blog/