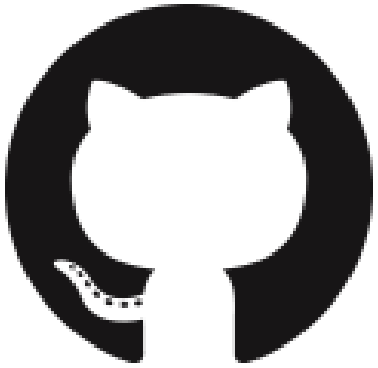
Welcome to OWASP
the free and open software security community

- International organization with chapters all over the world
- Provides guidance and tools to develop secure Web Applications
- Organizes conferences, forums, and training events to educate communities
- A valuable pool of resources at no cost

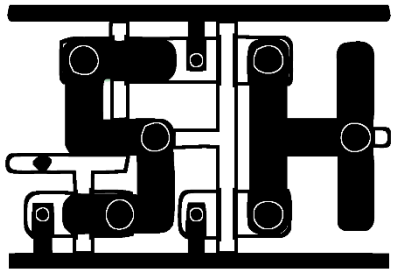
Visit www.owasp.org for more information

Consider joining OWASP, $50 year to support the work towards better software security and so much more…

OWASP Portland Chapter
Training Day 2017
A Big “Thank You” to Our Sponsors



online business systems



BLINDSPOT

SUMMIT
SECURITY GROUP, LLC

Securing your AWS Infrastructure

Derek Hill – MBA, CISSP
CSO Security Manager – HP Inc.
derek@dh-solutions.com
@secureITtoday

Adam Simpson
Blue Team Security Engineer – HP Inc.
k_rad@hotmail.com

Presentation can be downloaded from here:
https://github.com/derekhillhp/AWS-Security-Class

Objectives

- A big picture view of security in AWS (30,000 ft vs. 3 ft)
  - Don’t worry, some links are included to dive deeper into subject areas
- Give you a better understanding on the various AWS technologies
- How to secure the various technologies?
  - Going to address the big ones
  - Just scratching the surface here
  - Give you real world examples and hopefully some ideas on how you can implement them in your organization
  - Not all issues are technical
- Have a discussion
  - Not meant as a lecture, but rather collaborative

Agenda

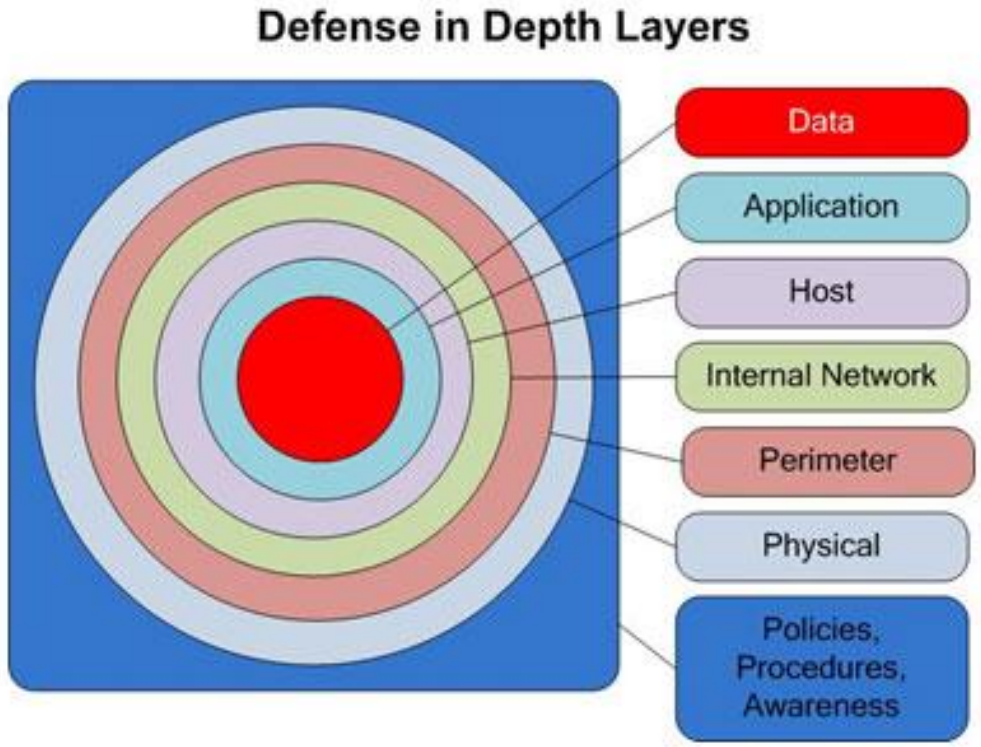
- Concepts
- Instances
- Account Management
- Logging
- Tools
- Vulnerability scanning / pen testing
- Software
- Data Security
- Demos

Concepts

Laying a basic foundation

Defense in Depth

- Layers of security
- Have defenses in more than one layer
- Don’t put all your eggs in one basket – what happens when that defense fails?
- Applies to the cloud, however, the terminology is different
- Can’t implement all layers as you don’t have access to all of them – think physical layer in AWS or shared responsibilities
- Limit the blast radius, keep your applications / networks compartmentalized, the smaller the better and require authentication to move between compartments



Roles and Responsibilities

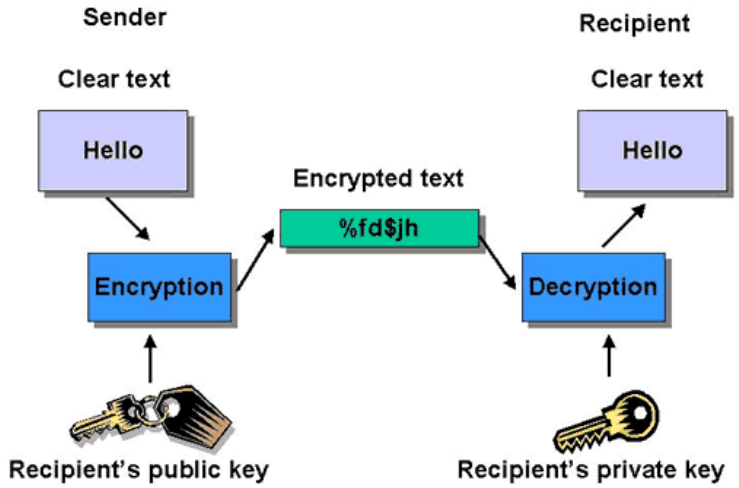
- Have personnel defined for certain tasks, hold them accountable and give them authority
  - A person responsible for the security architecture
  - A person responsible for vulnerability management
  - etc……
- Implement peer review for changes
  - Changes are easy and often the left hand doesn't know what the right hand is doing, especially the case with distributed teams (more on next slide)
- Have incident handling plan (out of scope for today)
  - IR/IH is an entire topic by itself, too much to cover here
- Generally try to understand and follow practices around team organization for your particular industry/project type
- Adopt a RACI model – clarify who is responsible for what
  - https://en.wikipedia.org/wiki/Responsibility_assignment_matrix

Change Management and the challenges

- Even more important in the cloud as it is extremely easy to make changes
- Changes are almost too easy, how do you keep things under control
- How do you handle distributed teams? Establish and maintain good relationships with remote/distributed teams.
- If you have to follow compliance rules, how do you know what you have? Who made what change? How long has it been this way? ... [This might become a much larger issue in the not so distant future]
- Even if you maintain your environments with automation, who is making changes to those scripts/tools? Are those changes tested?

Encryption

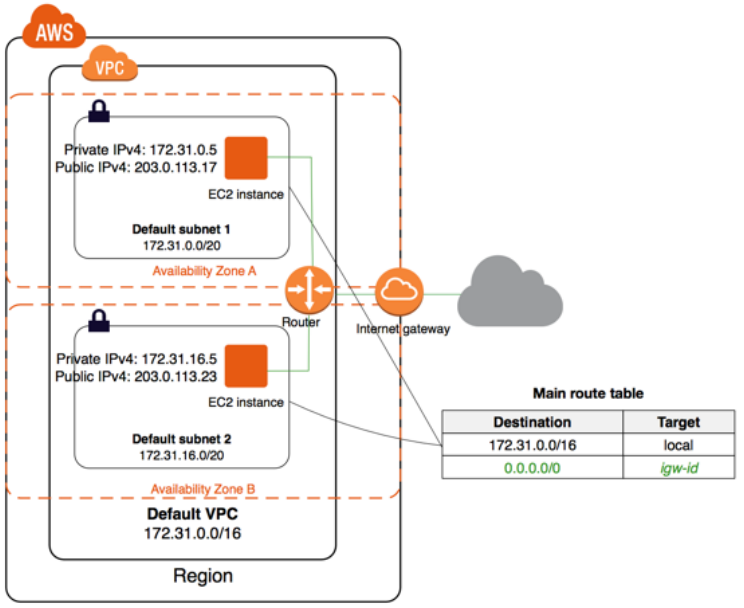
- Always use “open” encryption such as AES-256, SHA-2, RSA 4096 bits or what you are required by your company, gov’t agency, compliance, etc.
  - Never roll your own encryption, you want something that has been publicly vetted for a decade or more
- Encryption is only as good as the key
- It always comes down to key management, where is it stored, who has access to the key(s)
- Encryption at rest – disk encryption
- Encryption in motion – transport encryption (SSL/TLS) – SSL is broken, use TLS 1.1 or later
- When in doubt, encrypt – err on the side of security vs. performance, nobody has been sued for negligence for encrypting data vs. unencrypted data – make sure you use strong encryption and good key management

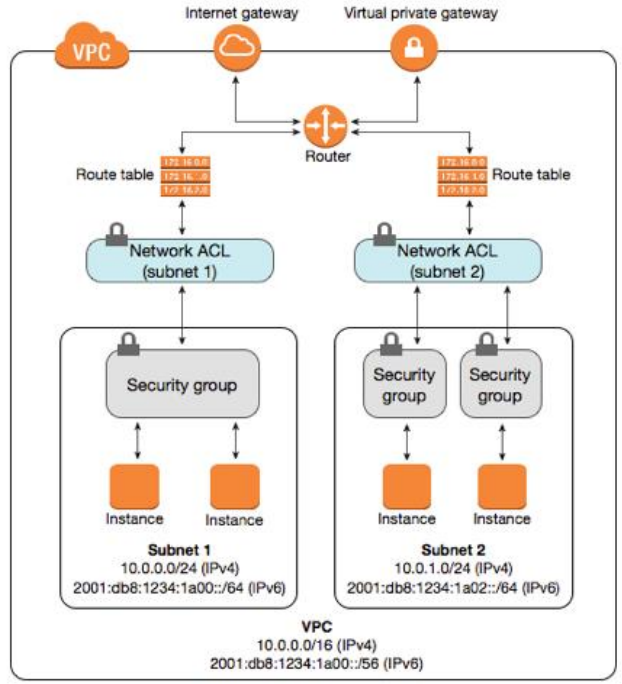


Virtual Private Cloud (VPC)

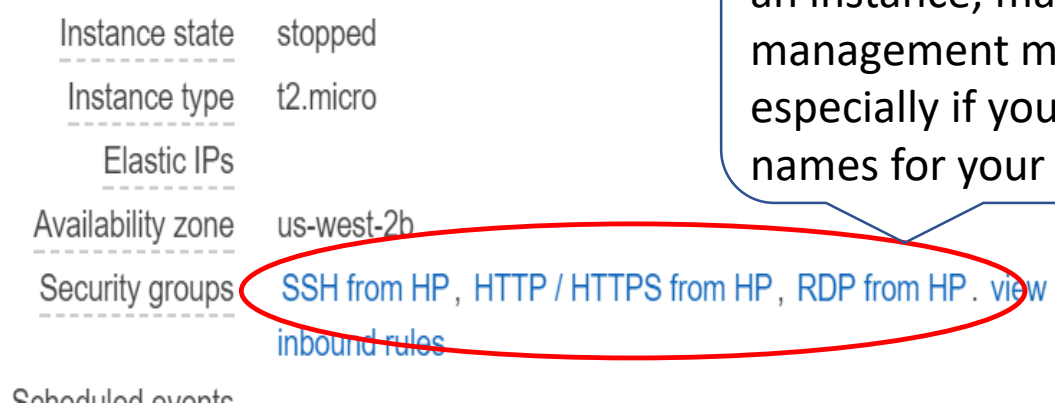
- What is a VPC?
  - Think of it as a VLAN if you need a traditional network reference
  - You can create multiple isolated subnets inside a VPC
  - A VPC can span multiple Availability Zones (AZ), this can provide you with local redundancy
  - A VPC cannot span multiple regions, i.e. US-West-2 and US-East-1 cannot share a VPC
    - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

- How to secure VPC's?
  - Use security groups (stateful) to control INSTANCE ingress and egress of your VPC, you can also use ACL's (stateless) if you want to control access at the SUBNET level
  - Use VPC flow logs to collect traffic coming and leaving your VPC (similar to spanning in a traditional network) – you can send those to an IDS
    - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html
  - Enable CloudTrail to monitor changes to VPC
  - Better to have more and smaller VPC's, rather to have all your resources in a large VPC (blast radius)





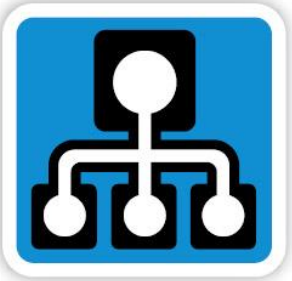
Security Groups (SG)



You can add multiple SG's to an instance, makes management much easier, especially if you descriptive names for your SG's.

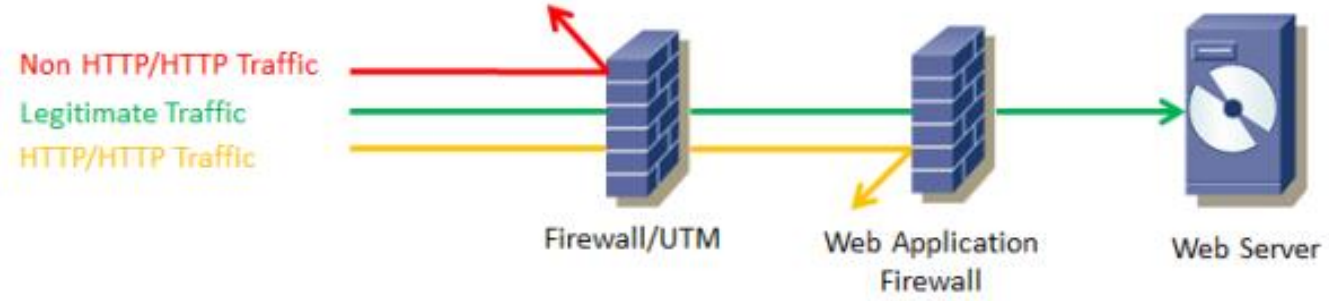
- Basically a Stateful firewall
- Ingress (inbound) and egress (outbound) filtering at the instance level
- Easily configured – almost too easy
- Need to be continually reviewed for effectiveness (remember submitting request for firewall changes)
- Create security groups for individual protocols/services, layer multiple groups onto an instance – it will help you see what is applied to each instance, without having to dig into each group
- Remove the launch-wizard groups, not descriptive at all and often wide open
- Label all your groups as to what type of traffic is allowed and where it is coming from

Load Balancers (LB)



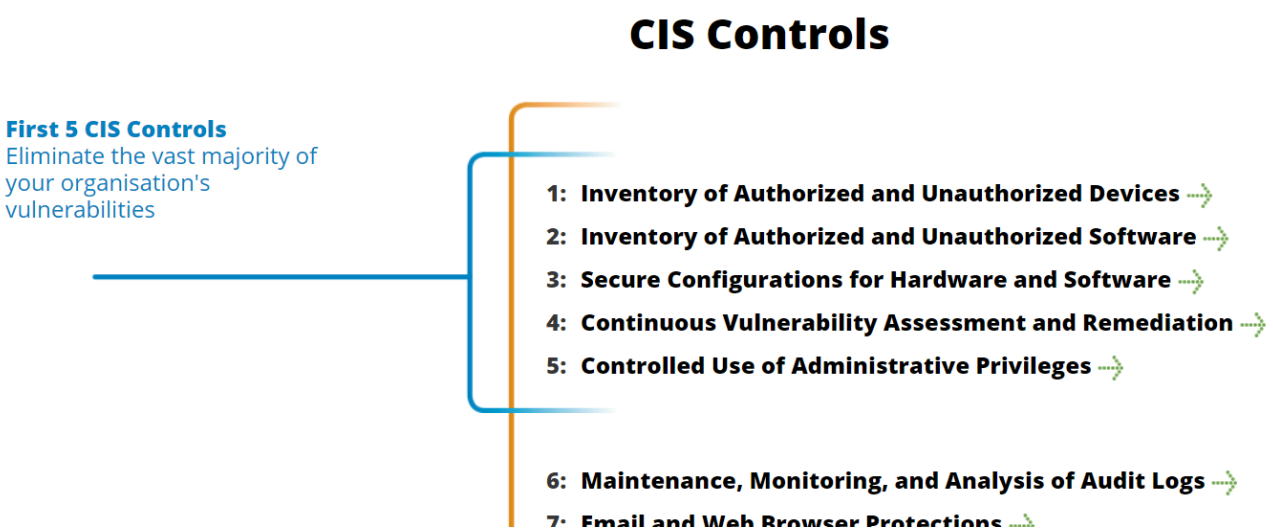
- Elastic Load Balancer (ELB) [now renamed to Classic] Layer 4 & 7 (X-headers) – Terminate or Pass-through
- Application Load Balancer (ALB) Layers 7 – ELB with a WAF integrated and more – Terminate Only, option to re-encrypt for last leg
- Network Load Balancer [just released (Sep 7) – not covered here]
- DNS Load Balancing (DNS failover)
  - https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
  - https://aws.amazon.com/elasticloadbalancing/details/#compare
  - https://aws.amazon.com/blogs/aws/new-network-load-balancer-effortless-scaling-to-millions-of-requests-per-second/

Web Application Firewall (WAF)



- Firewall for HTTP applications that operates at the Application layer of the OSI model (Layer 7)
  - It is designed to block and filter out undesirable traffic between the HTTP client and server – based on rules you apply
- Often considered a reverse proxy that protects servers, not clients
- AWS has WAF offerings, however, you have to create your own rules – often a trial and error
  - Sample rules: https://github.com/awslabs/aws-waf-sample
  - AWS WAF with OWASP Top 10 rules: https://aws.amazon.com/about-aws/whats-new/2017/07/use-aws-waf-to-mitigate-owasps-top-10-web-application-vulnerabilities/
- OWASP provides a basic set of rules free of charge:
  - https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project
- When initially implementing a WAF, do not put it into blocking mode, otherwise some part of the site may be broken.

Critical Security Controls



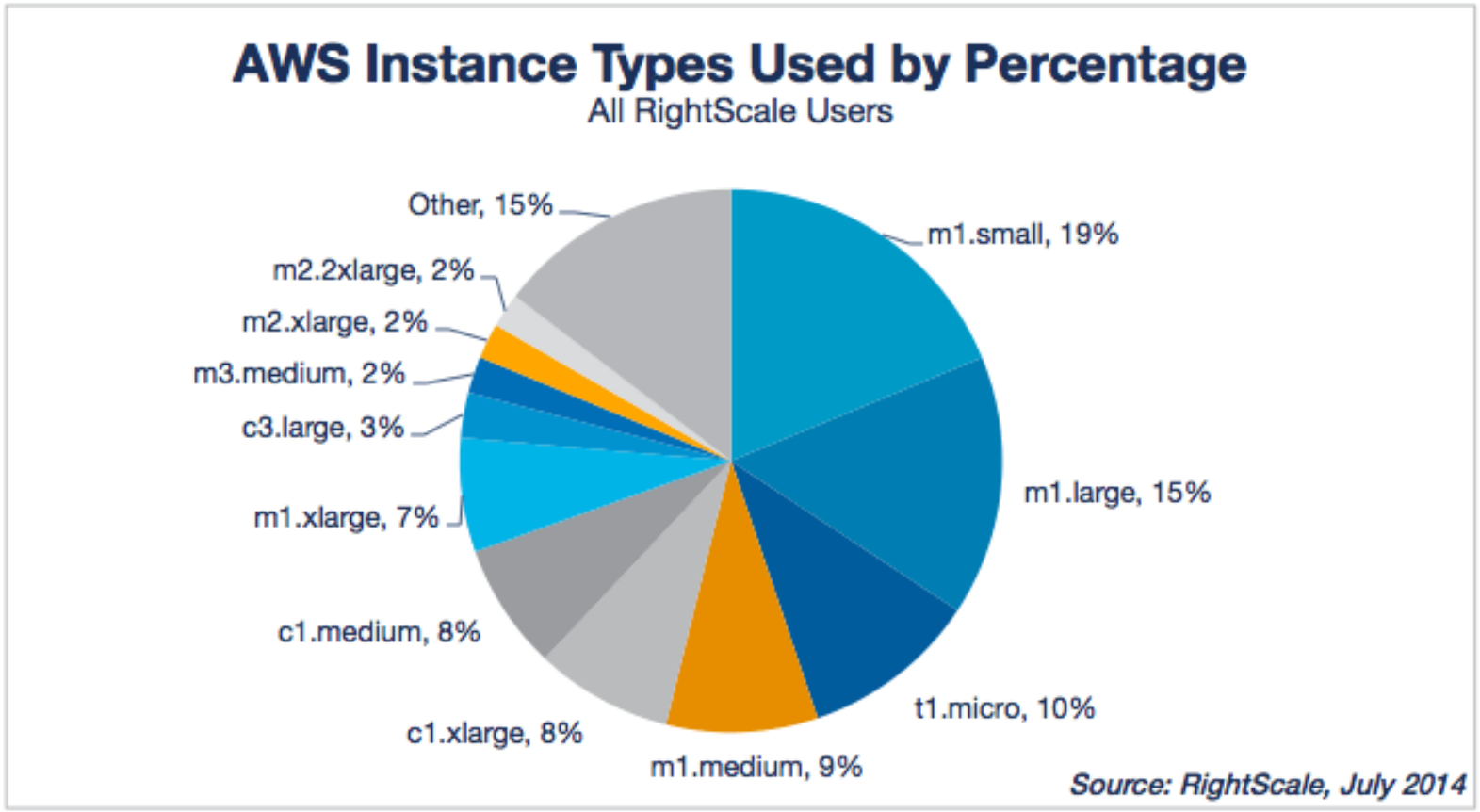
- Total of 20 controls
- Usually updated every 12-18 months
- Most of the controls can be automated
- Implementing the top 5 will get you into pretty good shape – not perfect, but you will protect against the most common types of attacks (85-95% depending on who you ask)
- https://www.cisecurity.org/controls/
- https://www.sans.org/critical-security-controls/guidelines
- https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

CSC – Controls 6-20

6: **Maintenance, Monitoring, and Analysis of Audit Logs**
7: **Email and Web Browser Protections**
8: **Malware Defenses**
9: **Limitation and Control of Network Ports**
10: **Data Recovery Capability**
11: **Secure Configurations for Network Devices**
12: **Boundary Defense**
13: **Data Protection**
14: **Controlled Access Based on the Need to Know**
15: **Wireless Access Control**
16: **Account Monitoring and Control**
17: **Security Skills Assessment and Appropriate Training to Fill Gaps**
18: **Application Software Security**
19: **Incident Response and Management**
20: **Penetration Tests and Red Team Exercises**

Instances

VM’s in AWS



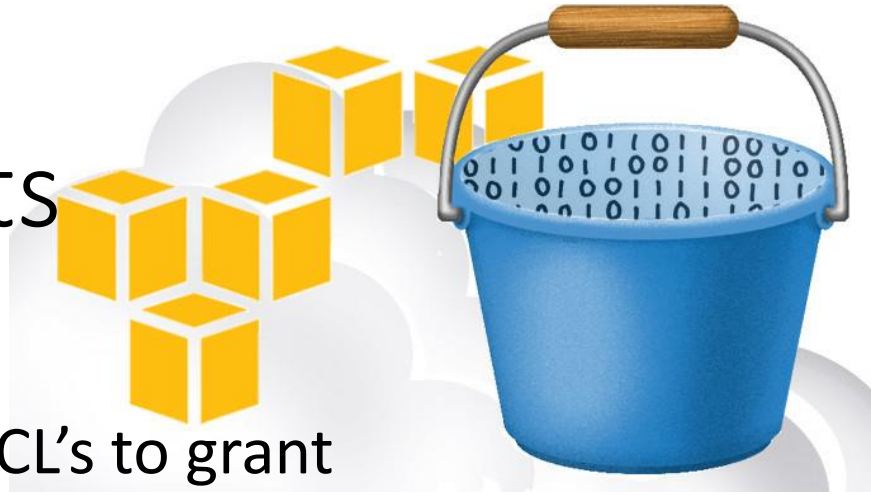
Admin Access

- Some instances are under your full control, you have full admin rights (root) – these should be the easiest to secure …. or are they?
- Some instances are under somebody else's control inside your AWS account – your key is not installed, however, somebody in your org does have root – How do you know what is installed, what that instance is doing, etc?
- Are you using 3rd party instances? For example, Virtual Appliance, Vendor provided AMI.
- Many AWS services don't give you root access, think RDS, RedShift, etc.
- Remove / disable user keys from instances once they leave the company

Encrypted Volumes

- As of recently you can now encrypt your root volumes in Elastic Block Storage (EBS) (didn't use to be the case) – might have to go rebuild older instances that were built previously
- You can have Amazon manage the key or you can manage it, you decide
  - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
- Who has control over the key vs. the increased complexity

Simple Storage Service (S3) Buckets



- Enhance default security by using bucket policies and ACL's to grant permission
  - https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html
  - These can be scripted using JSON and applied to multiple buckets quickly to deploy an organizational policy
- Encrypt your S3 buckets using either Amazon's encryption options or manage it yourself (server side vs. client side)
  - Pick the one that fits your risk profile and your organization guidelines
  - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html
- Consider using VPC Endpoints to access your S3 buckets. This will restrict access to only certain systems can access your S3 buckets.
  - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html

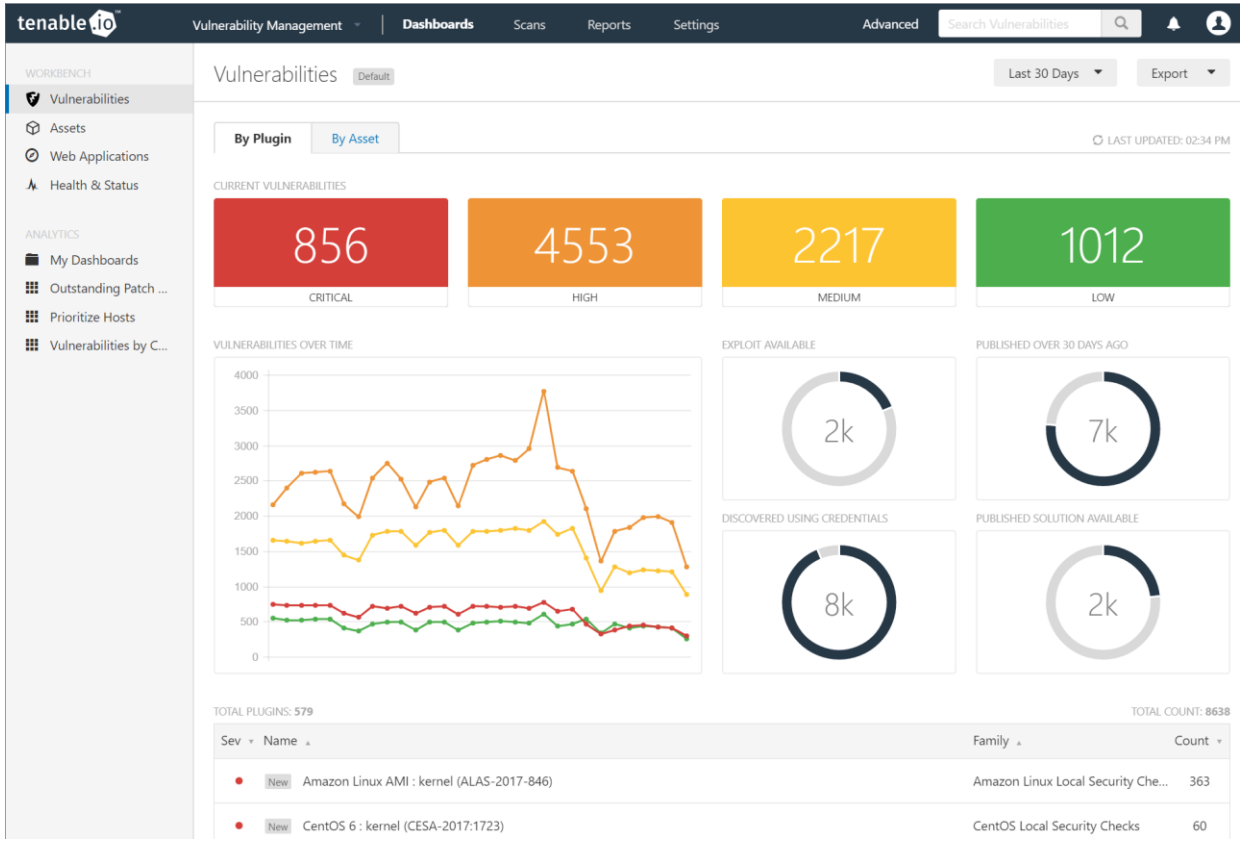
Amazon Machine Instance (AMI)

An image in the cloud

- Who created the AMI?
- Do you trust the creator of the AMI?
- What software is installed on the AMI?
- How is the AMI configured?
- How recently was the AMI patched?
  - Were the patches validated as resolving the vulnerabilities
- Are there any backdoors or access keys installed?
- Roll your own?

Vulnerability management on your instance(s)

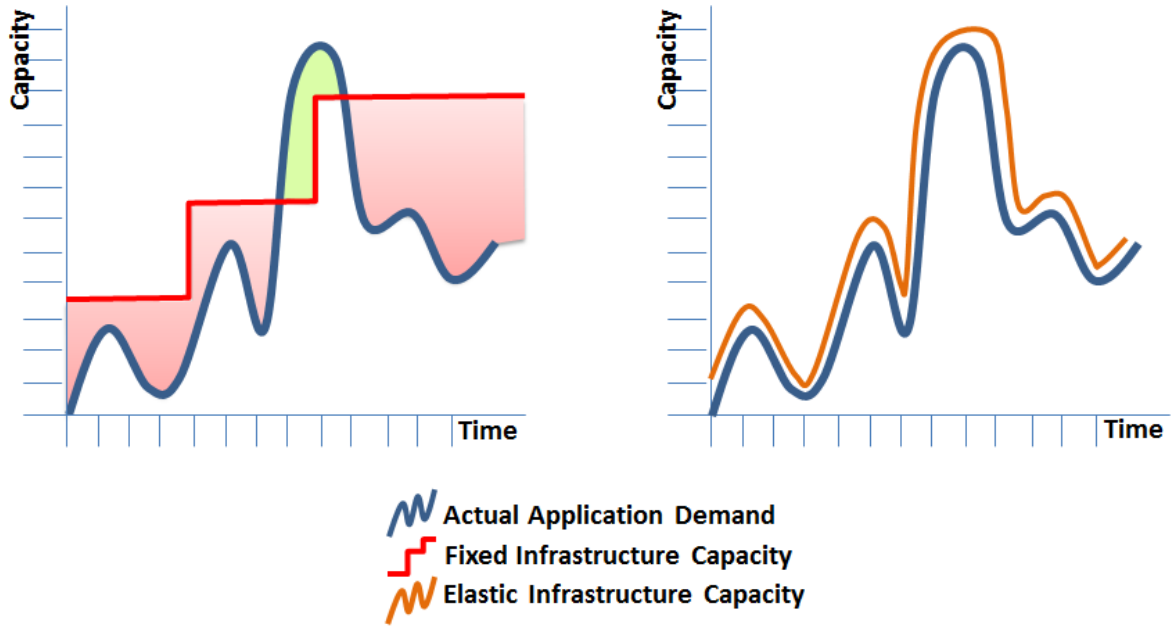
- How do you know what software is installed and how is it configured?
- How do you know what vulnerabilities are present on your systems?
- How do you patch your systems?
- How do you remediate insecure configurations?
- Use a SCAP compliant scanner:
  - https://scap.nist.gov/validation/



Patching

- How often do you patch?
- Do you patch?
- If you don’t patch since you rebuild your systems from scratch, how often do you update your AMI?
- Do you know if your AMI is up to date?
  - What about 3rd Party AMIs? Community, Vendor, Internal
- Is the patched AMI free of vulnerabilities and/or configuration issues?
- Stability of an old AMI that has been patched repeatedly vs. a new AMI (built from scratch)
- Patching with AWS EC2 Systems Manager (if you have Windows systems) https://aws.amazon.com/blogs/mt/windows-ami-patching-and-maintenance-with-amazon-ec2-systems-manager-2/

Auto Scaling



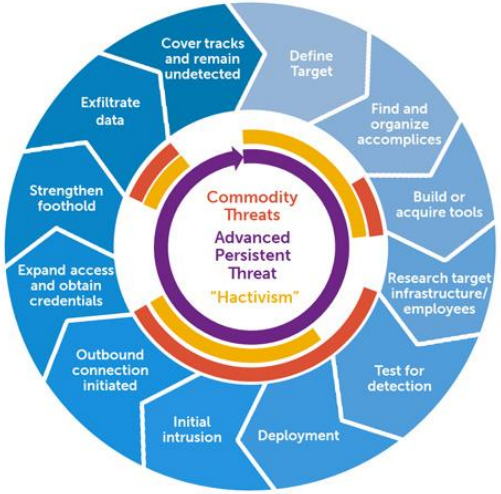
- Where did the AMI come from?
- When was it updated?
- How long will the instance(s) run?
  - Do you have a policy regarding length of instance lifetime in an auto scaling configuration?
- Maximum age of AMI before required replacement
  - Reduces possibility of APT
- Many of these principles apply to Elastic Beanstalk as well

Building your instances

- Start with an absolute minimal OS, barely enough packages to run networking and login
- Use vendor or 3rd party hardening documents / checklists – freely available
- Use Config Management (puppet, chef, SCCM, etc.)
- Layer your software onto the instance, only install what you absolutely need
  - If it is not installed, you don't have to protect it or patch it
  - You are reducing your attack surface and potential vulnerabilities
- Don't run services as root unless privileged port is required and use a proxy service if possible
- Run agents that report on the software vulnerability status (Qualys, Nessus, etc.)
- Patch on a regular basis
- Stop or terminate instances not needed, if it is not running, it cannot be hacked

Config Management

- The goal with configuration management is to have a consistent and repeatable environment. While being unique as individuals is a good thing, it becomes unsustainable as far as supporting an infrastructure
- Cloud formation – define your environment such as VPC's, SG's, Instances – makes for a quick and repeatable deployment
- AWS CLI – automate tasks such security group changes, can be scripted and run automatically
- Lamda functions
  - Alert on non-standard implementation, i.e. spinning up an instance with everything "wide open"
  - Automate tasks such as security groups: https://github.com/marekq/aws-lambda-firewall



Instance – Life Cycle Management

- The longer an instance runs, the more likely it is to be compromised
- In order to protect against advanced persistent threats (APTs), you should recycle your instances on a periodic basis (weekly, monthly, quarterly) – the shorter the less likely an APT can exist
- If you are using Auto Scaling or Elastic Bean Stalk, make sure your AMI's are current – Also validate those base images on a periodic basis, just because something is not vulnerable today, it doesn't mean it won't be vulnerable tomorrow

Accessing your instances

- Configure your security groups to allow access to the instance (SSH, RDP, etc) only via trusted IP addresses/network ranges
- Use strong passwords (sufficient length >16 chars) if you CANNOT use keys
- Integrate with your internal directory services (AD, LDAP) using federation if possible (ADFS, SAML, etc)
- If using keys, make sure you delete the keys for personnel that have left your group/company and don’t need to have access to the instance, define this responsibility
- If using a Bastion host, ensure it is HIGHLY secure

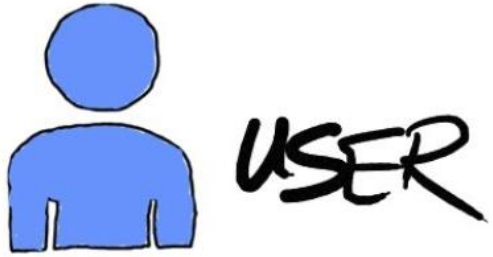
Account Management

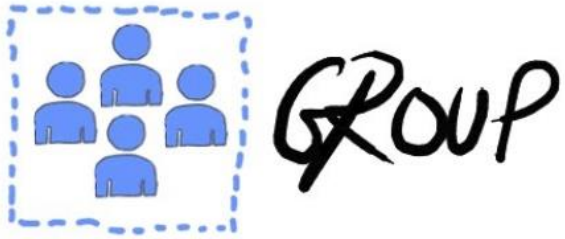
Do you know who is doing what, why and if they should be?

Users, Groups & Roles

- Users, Groups and Roles
  - Users are assigned to Groups, then you assign permissions to the groups
  - Roles are similar to users, but roles can be assumed by users to perform other tasks (if the role has appropriate permissions) that are assigned to those roles
- When to use roles
  - When using federated logins and you don't users to have to provide a second set of credentials
  - When creating applications that access AWS resources
  - For simplified management across multiple AWS accounts

  - https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html



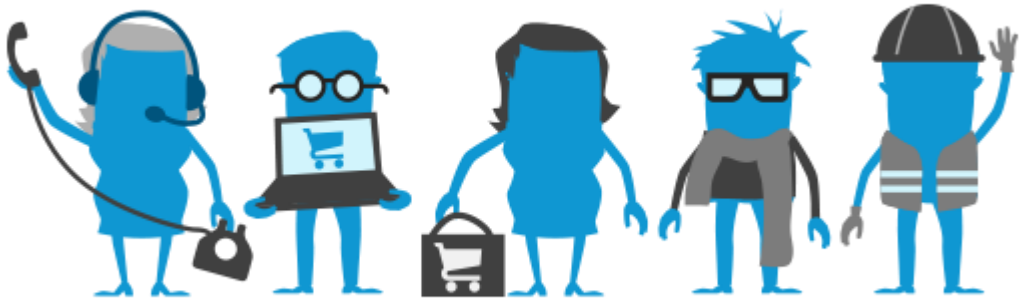


Securing IAM accounts

- Create and apply a default policy that enforces key items such as:
  - Password length and complexity
  - Password duration
  - Other password parameter such as reuse, how frequently they can change, etc.
- Require MFA on all logins via the console
  - Use free or commercial software tokens such as Google Authenticator, RSA, etc.
  - Use hardware based password tokens such as Gemalto token

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html
- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

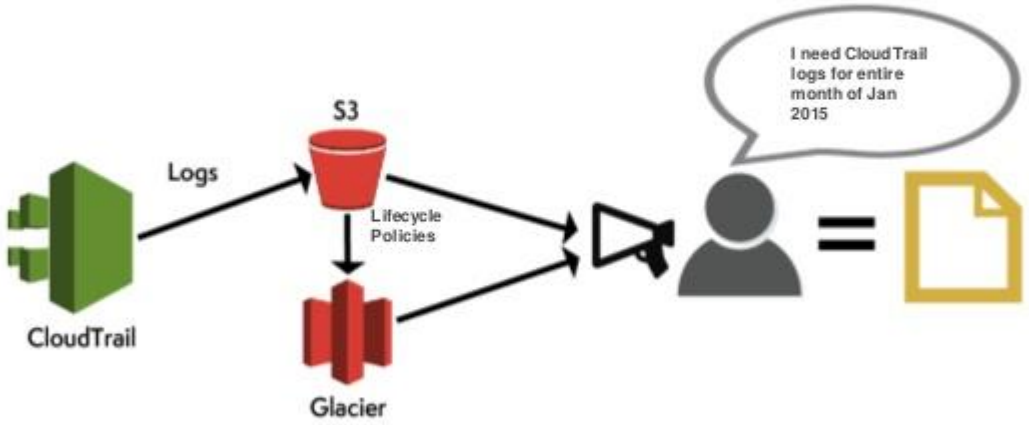
Account Management



- Remove users in a timely fashion if they no longer need access to the account
  - This includes terminated employees or employees that have changed jobs/roles and no longer need to have access to the account
  - If you are using federated logins, this is much easier
- Only add users that have a need to access the console
  - Make sure the access has been approved by management
  - Assign appropriate permissions, don’t give them more rights than they need to accomplish their job
  - If they have rights to create and terminate resources, make sure they have the proper training in processes and procedures and that they follow security rules for configuration

Logging

Needs to be enabled before something happens to be useful



CloudTrail

- Every account gets 1 free CloudTrail
- Use it to log all API access, CLI, GUI, etc. – anything account related
- Send the CloudTrail to an S3 bucket for storage and further analysis
- For additional security, send the trail to an external SIEM (Security information and event management), such as Splunk ES, ArcSight Logger, OSSIM (AlienVault) – The SIEM can alert based on certain events, otherwise it will be investigate after the fact
- Are you actually reviewing these logs on a regular basis??

Centralized logging

- Good practice to send all logs to a centralized log server for correlation (ELK, Splunk, ArcSight Logger, Kiwi, Graylog, syslog-ng)
  - This log server should be in a different VPC, account (preferred), etc. to reduce the likelihood of data removal during a breach
- Instances will have to have syslog (Security logs [minimum] on Windows) forwarding configured or a log collection agent installed on them in order to forward logs to a centralized log server
- Ideally the security (wtmp, utmp, btmp, Windows security access logs, web server access logs, etc.) related logs should be forwarded to your SIEM for detection and alerting purposes
- When in doubt, log it …..(make sure you are not logging sensitive data)
- When you are later investigating a breach or looking for root cause on an issue, you have to have the data. Logging after the fact is too late!!!

Tools

AWS and 3rd party tools to make your life easier

Some of tools we use

- SCAP Scanners (Nessus & Qualys)
- Lambda functions
- Cloud Formation
- Scripts (JSON, AWS CLI, Python, Etc)
- Patching tools (Ivanti – just rolling this one out)
- Excel
- Security Monkey
- AWS Trusted Advisor
- Custom home grown tools, ie. Zeus

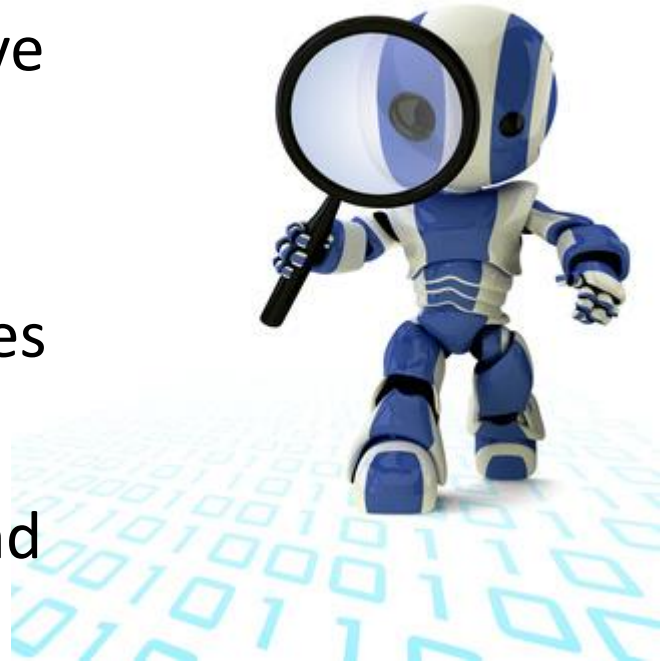
Software

Deploying, maintaining and knowing the security state of your custom software

Static Code Analysis (if you are creating code)

Static Application Security Testing (SAST)

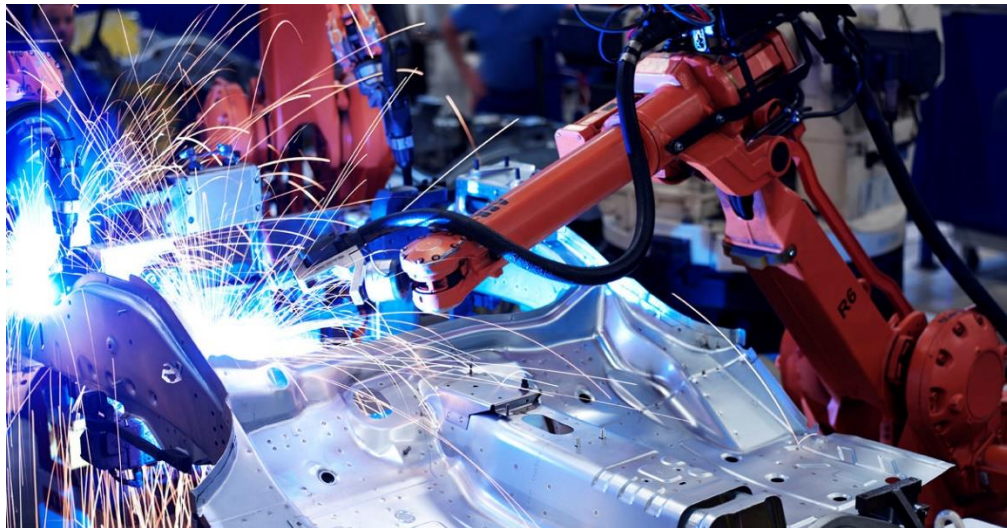
- Scan code upon checking into repo
- If possible, integrate this into your CI/CD pipeline if you have one
- Cheaper to fix issues before they are rolled out to production
- Will need to review the findings and mark any false positives to ensure that your dev's can focus on real issues and not noise
- Work with the development teams to help them understand how to code securely
- If you are using third party including Open Source components in your code, how do you know those don't have security issues?
  - Interesting area, quite a few new vendors venturing into this space



Dynamic testing of code

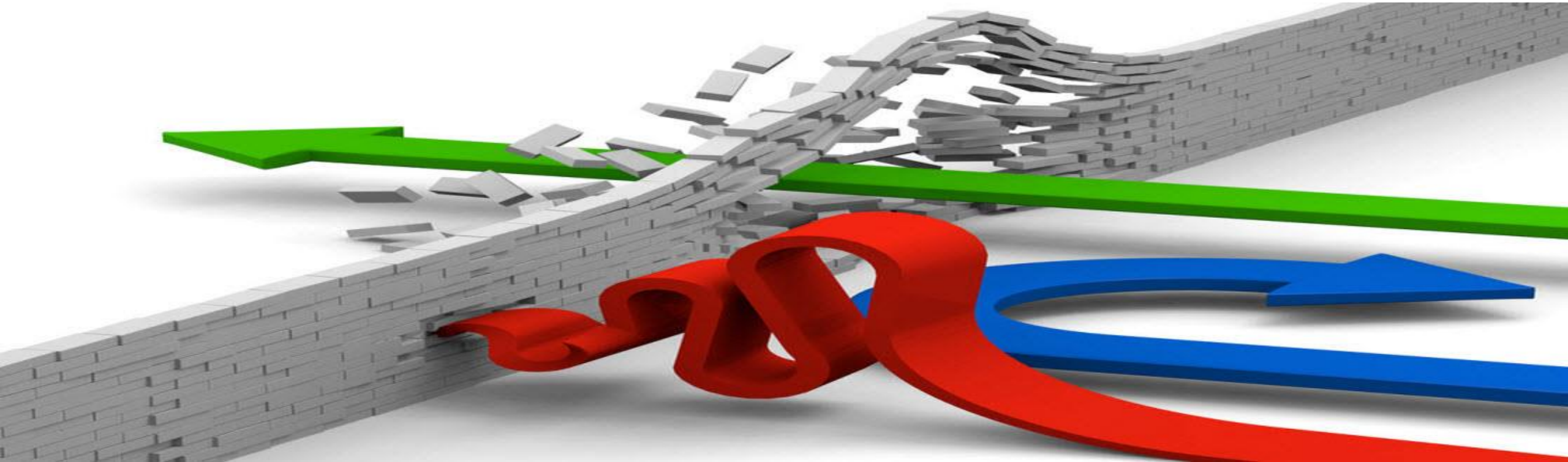
Dynamic Application Security Testing (DAST)

- Test your code as it is running on infrastructure after it has been compiled (if required)
- You will discover issues that you cannot find if just running static code analysis – such as system calls, DB interaction, load issues
- Use tools to continually test your applications, but make sure you are testing non production stacks, otherwise you might cause a DoS on your own site
- Set it up once, let it run continuously
- Review the results of the test
  - Scanning without remediation is a waste of time, it might even prove negligence in a legal proceeding



Vulnerability Scanning / Pen Testing

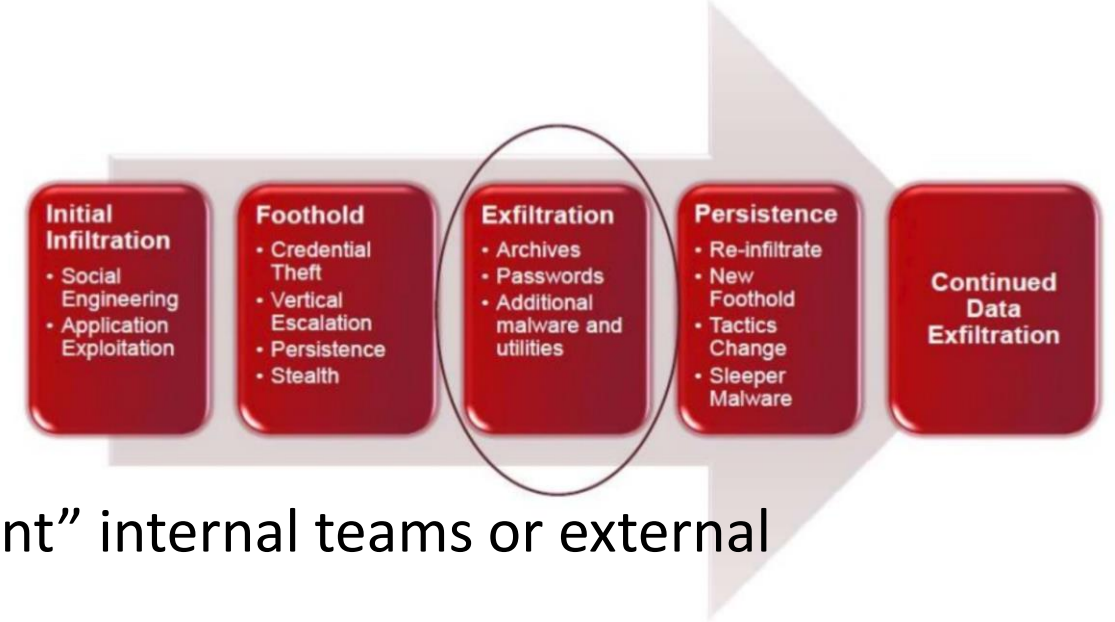
Automatic testing, manual testing and getting permission



Live Application / System testing (automated)

- Use automated tools to continually test your systems and applications
  - Once scripts are defined, the testing is essentially free
  - This will simulate users and/or attackers utilizing your site
  - Your testing tool will actually login to the application in an attempt to find flaws
  - You might even define tests that utilize users with different privilege levels, this might be especially important if you have additional screens for higher privileged users – remember, many of the attacks are from “insiders”
- Where to test
  - Non-prod environment vs. prod – most testing should be done from non production so you don’t impact site performance, but you might want to periodically test the production site as there are often much larger data sets involved. At the very least, before going live
- Automated tools can find a lot of issues, mostly low hanging fruit, but are unable to find deep logic bugs….

Pen Testing



- Conduct regular pen tests, either by “independent” internal teams or external companies that specialize in this type of work
- Have a clearly defined scope – watch out for scope creep
- If you want to inform your Blue Team that this is coming is entirely up to you – pros/cons
- Get written permission from internal management (executive staff) and Amazon
- Try to perform Pen Tests on non-production environment if possible
- Include social engineering in your pen tests, your security is only as good as the users
- If you discover a show stopper or break something, stop the test and report it immediately to get it rectified
- Provide a comprehensive report
- Share the findings with your blue team (red informs blue)

Data Security

Give access to the data to those who should have it and denying it from those who shouldn’t

Who should have access to data

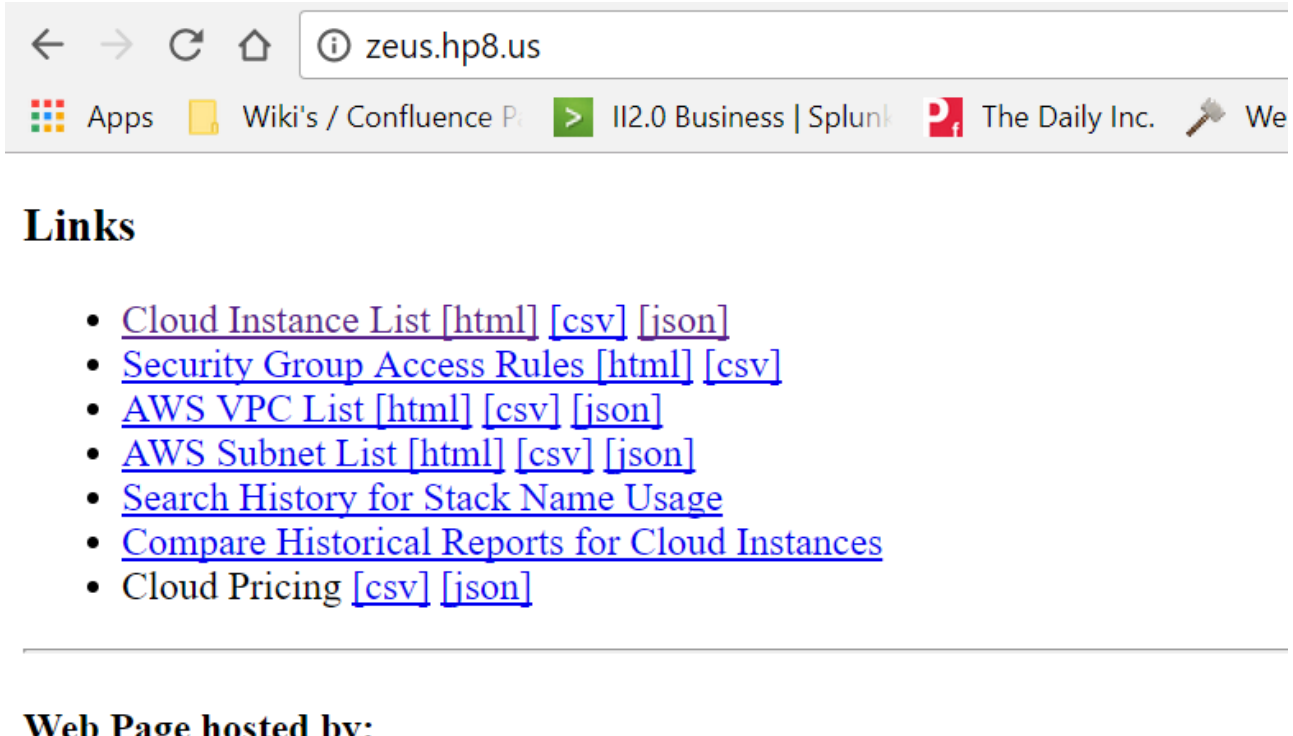
- Who needs access to the data?
  - Why do they need access?
  - What is the risk if they have access?
- Can we restrict developer access to the data and still function or troubleshoot?
  - Perhaps have a DevOps person with the access and they can screen share with the Dev when needed
- Compliance with regulations, think GDPR, PCI, PHI, PII, SOX, etc…….
  - GDPR will be a game changer for those of you who are or will be doing business in the EU. It goes into effect on May 25, 2018…..not a lot of time but certainly a lot of changes
- Separation of duties
  - Don’t give a single person all the rights, try to separate those rights across multiple people – obviously this won’t work in very small teams

Demo (Screen Shots) of the apps we use

- Zeus
- Nessus
- Qualys
- Correlation of data
- Acunetix
- Fortify SSC
- Tool challenges - API problems, vendor problems, ongoing feedback

Zeus

- Custom developed tool, using API calls on all of our accounts to pull the data we care about



Cloud Resources

Cloud Resources - Updated Mon Oct 02 at 15:50 2017 UTC [server local: Mon Oct 02 at 08:50 2017]

Note: Events Are Pending for the Following Instances

Instance Name	Instance ID	IP Address	Region/AZ	Tenant	Age (days)	Status	Event Code	Event Description
Splunk-OWS-SH01-lv2	i-	34	N. Virginia / us-east-1b	tech-ops-tools	373	running	instance-stop	[Completed] The instance is running on degraded hardware
PIE_PRINTER_SIMULATOR	i-	52	Oregon / us-west-2a	wppgen2-dev	809	running	system-reboot	[Completed] scheduled reboot

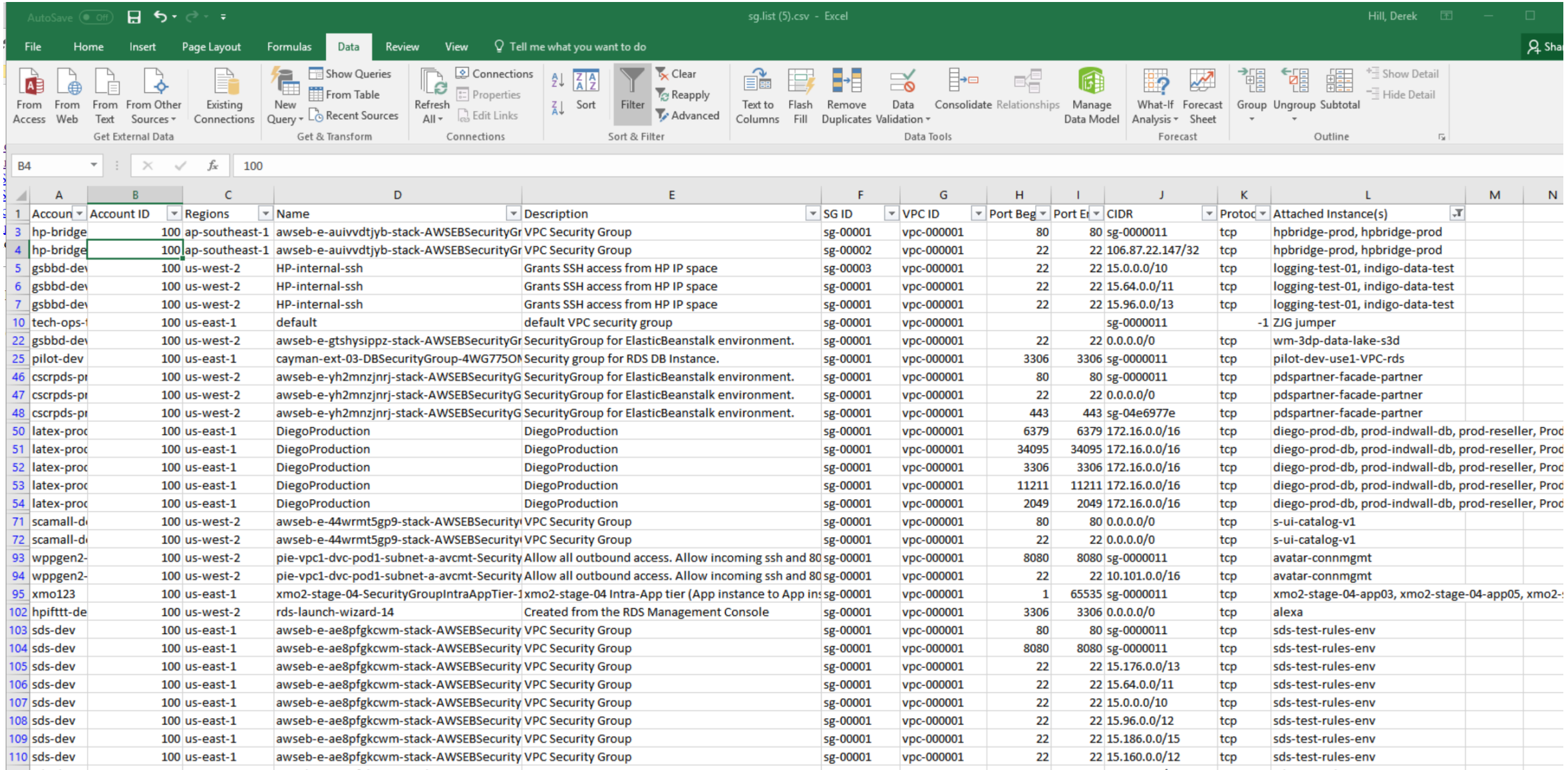
Search:

Instance Name	Instance ID	IP Address	Region/AZ	Tenant	Age (days)
!!! UTK phase3 prod instance (2017-01-22)	i-0	5	Frankfurt / eu-central-1a	indigo-svc-supt-prod	34
*** R@G - PROD (ETL)	i-1	5	Frankfurt / eu-central-1b	indigo-svc-supt-prod	106
*** R@G - PROD (WEB)	i-8	5	Frankfurt / eu-central-1b	indigo-svc-supt-prod	887
*** RAG DB NEW	i-c	5	Frankfurt / eu-central-1b	indigo-svc-supt-prod	551
123-dev1	i-7	54	Oregon / us-west-2c	xmo123	803
123-dev2	i-c		N. Virginia / us-east-1d	xmo123	802
123-prod1	i-8	5	Oregon / us-west-2b	xmo123	782
123-prod2	i-4		N. Virginia / us-east-1d	xmo123	782
123-prod3	i-8		Oregon / us-west-2c	xmo123	782
123-prod4	i-3		N. Virginia / us-east-1b	xmo123	782
123-stage1	i-3		Oregon / us-west-2b	xmo123	797
123-stage2	i-4	54.1	N. Virginia / us-east-1d	xmo123	797

	Event Deadline	Creator
d hardware	2017-10-12T14:00:00.000Z	no tag
	2017-09-25T22:00:00.000Z	no tag

Age (days)	Status	Events	Size	Cost/day*	Creator	Provider	VPC
34	running		m4.large	3.46	no tag	Amazon	vp
106	running		m3.xlarge	16.33	no tag	Amazon	vp
887	running		m3.large	8.18	no tag	Amazon	vp
551	running		r3.xlarge	11.52	no tag	Amazon	vp
803	running		m3.medium	1.93	no tag	Amazon	
802	running		m3.medium	1.93	no tag	Amazon	
782	running		m4.large	2.88	no tag	Amazon	
782	running		m4.large	2.88	no tag	Amazon	
782	running		m4.large	2.88	no tag	Amazon	
782	running		m4.large	2.88	no tag	Amazon	
797	running		m3.medium	1.93	no tag	Amazon	
797	running		m3.medium	1.93	no tag	Amazon	

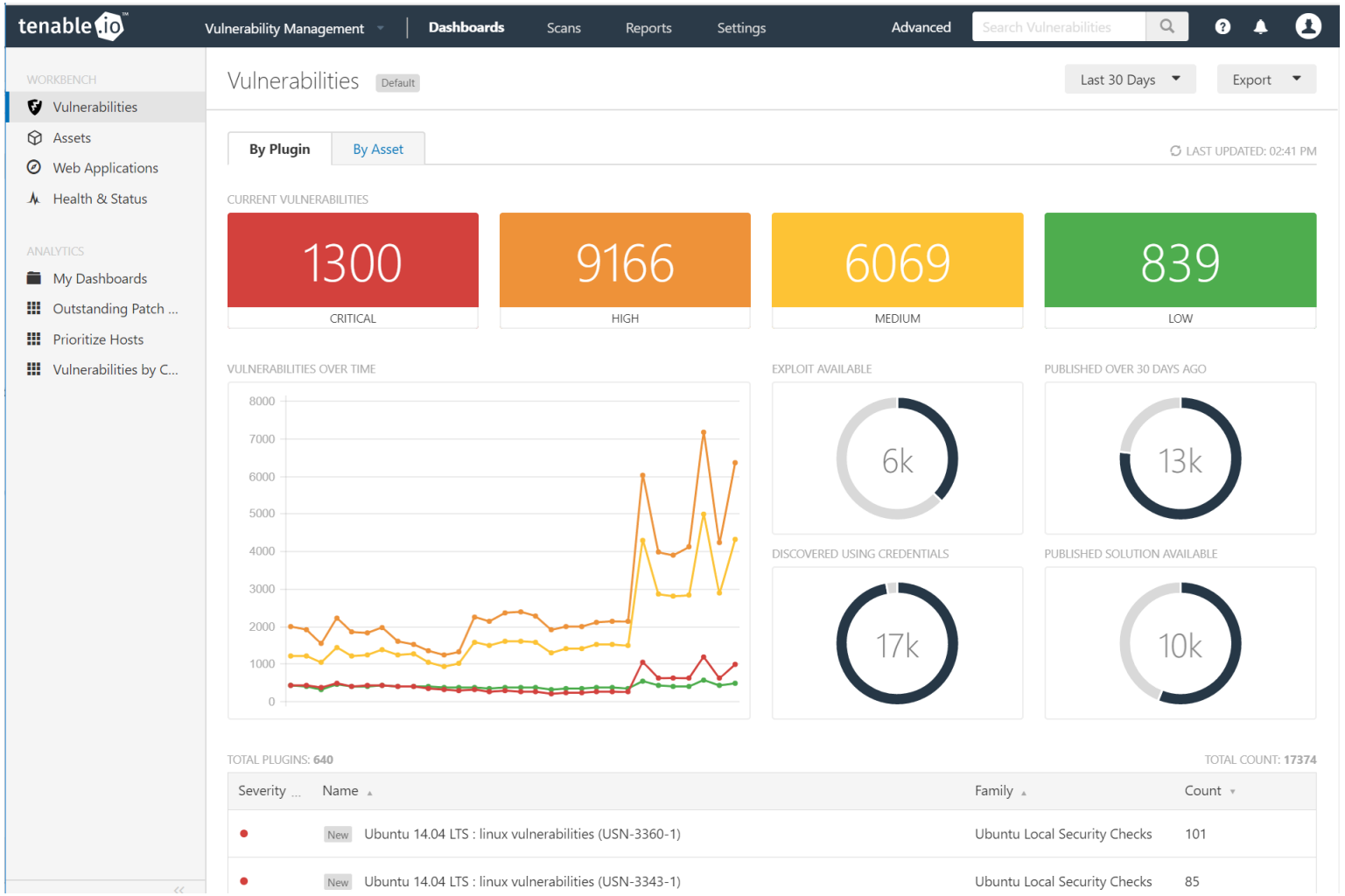
Security Groups

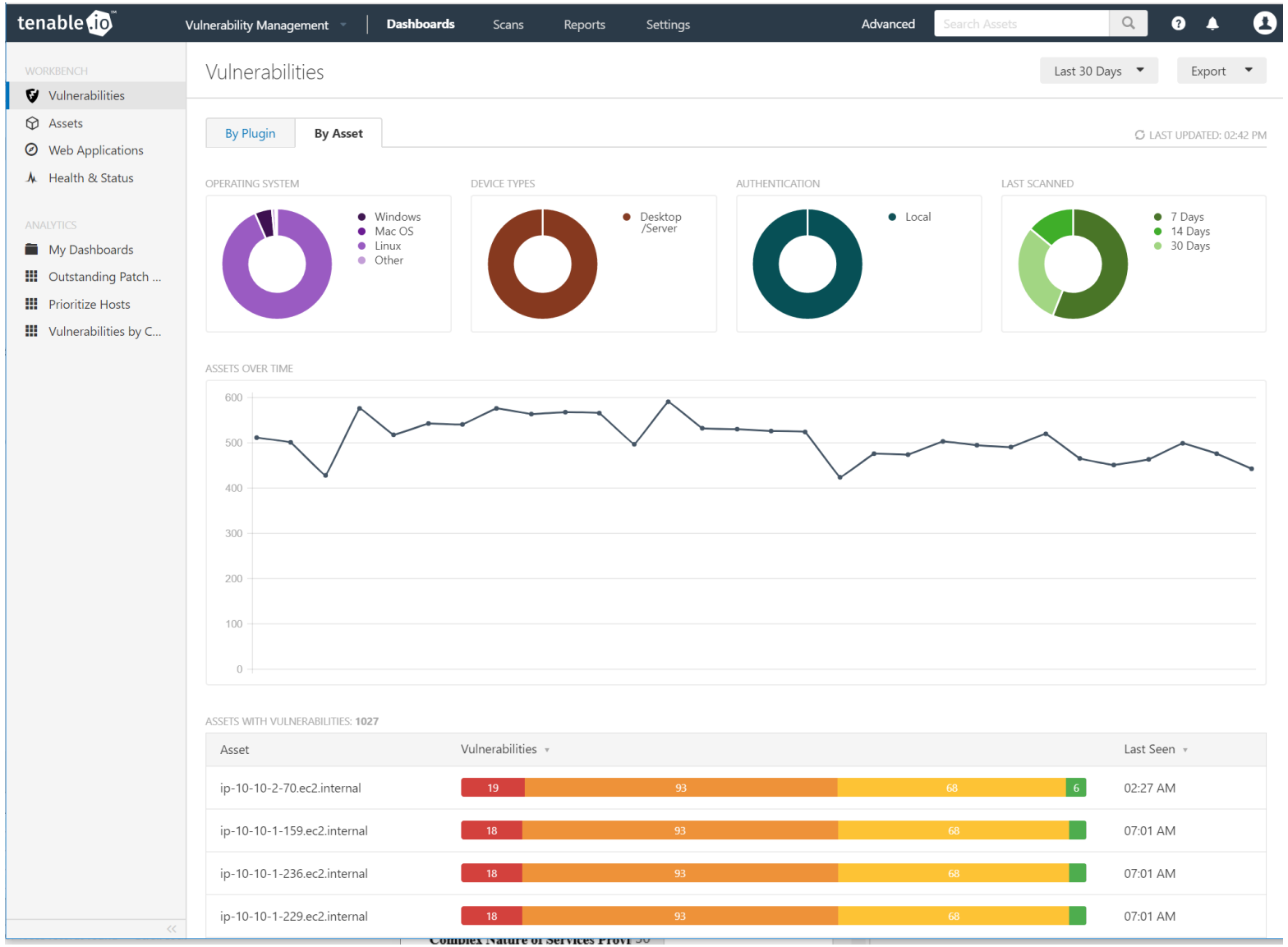


sg.list (5).csv - Excel

	A	B	C	D	E	F	G	H	I	J	K	L
1	Accoun	Account ID	Regions	Name	Description	SG ID	VPC ID	Port Beg	Port Er	CIDR	Protoc	Attached Instance(s)
3	hp-bridge	100	ap-southeast-1	awseb-e-auivvdtjyb-stack-AWSEBSecurityGr	VPC Security Group	sg-00001	vpc-000001	80	80	sg-0000011	tcp	hpbridge-prod, hpbridge-prod
4	hp-bridge	100	ap-southeast-1	awseb-e-auivvdtjyb-stack-AWSEBSecurityGr	VPC Security Group	sg-00002	vpc-000001	22	22	106.87.22.147/32	tcp	hpbridge-prod, hpbridge-prod
5	gsbbd-dev	100	us-west-2	HP-internal-ssh	Grants SSH access from HP IP space	sg-00003	vpc-000001	22	22	15.0.0.0/10	tcp	logging-test-01, indigo-data-test
6	gsbbd-dev	100	us-west-2	HP-internal-ssh	Grants SSH access from HP IP space	sg-00001	vpc-000001	22	22	15.64.0.0/11	tcp	logging-test-01, indigo-data-test
7	gsbbd-dev	100	us-west-2	HP-internal-ssh	Grants SSH access from HP IP space	sg-00001	vpc-000001	22	22	15.96.0.0/13	tcp	logging-test-01, indigo-data-test
10	tech-ops-	100	us-east-1	default	default VPC security group	sg-00001	vpc-000001			sg-0000011	-1	ZJG jumper
22	gsbbd-dev	100	us-west-2	awseb-e-gtshysippz-stack-AWSEBSecurityGr	SecurityGroup for ElasticBeanstalk environment.	sg-00001	vpc-000001	22	22	0.0.0.0/0	tcp	wm-3dp-data-lake-s3d
25	pilot-dev	100	us-east-1	cayman-ext-03-DBSecurityGroup-4WG775OM	Security group for RDS DB Instance.	sg-00001	vpc-000001	3306	3306	sg-0000011	tcp	pilot-dev-use1-VPC-rds
46	cscrpds-pr	100	us-west-2	awseb-e-yh2mnzjnrj-stack-AWSEBSecurityG	SecurityGroup for ElasticBeanstalk environment.	sg-00001	vpc-000001	80	80	sg-0000011	tcp	pdspartner-facade-partner
47	cscrpds-pr	100	us-west-2	awseb-e-yh2mnzjnrj-stack-AWSEBSecurityG	SecurityGroup for ElasticBeanstalk environment.	sg-00001	vpc-000001	22	22	0.0.0.0/0	tcp	pdspartner-facade-partner
48	cscrpds-pr	100	us-west-2	awseb-e-yh2mnzjnrj-stack-AWSEBSecurityG	SecurityGroup for ElasticBeanstalk environment.	sg-00001	vpc-000001	443	443	sg-04e6977e	tcp	pdspartner-facade-partner
50	latex-proc	100	us-east-1	DiegoProduction	DiegoProduction	sg-00001	vpc-000001	6379	6379	172.16.0.0/16	tcp	diego-prod-db, prod-indwall-db, prod-reseller, Prod
51	latex-proc	100	us-east-1	DiegoProduction	DiegoProduction	sg-00001	vpc-000001	34095	34095	172.16.0.0/16	tcp	diego-prod-db, prod-indwall-db, prod-reseller, Prod
52	latex-proc	100	us-east-1	DiegoProduction	DiegoProduction	sg-00001	vpc-000001	3306	3306	172.16.0.0/16	tcp	diego-prod-db, prod-indwall-db, prod-reseller, Prod
53	latex-proc	100	us-east-1	DiegoProduction	DiegoProduction	sg-00001	vpc-000001	11211	11211	172.16.0.0/16	tcp	diego-prod-db, prod-indwall-db, prod-reseller, Prod
54	latex-proc	100	us-east-1	DiegoProduction	DiegoProduction	sg-00001	vpc-000001	2049	2049	172.16.0.0/16	tcp	diego-prod-db, prod-indwall-db, prod-reseller, Prod
71	scamall-d	100	us-west-2	awseb-e-44wrmt5gp9-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	80	80	0.0.0.0/0	tcp	s-ui-catalog-v1
72	scamall-d	100	us-west-2	awseb-e-44wrmt5gp9-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	0.0.0.0/0	tcp	s-ui-catalog-v1
93	wppgen2-	100	us-west-2	pie-vpc1-dvc-pod1-subnet-a-avcmt-Security	Allow all outbound access. Allow incoming ssh and 80	sg-00001	vpc-000001	8080	8080	sg-0000011	tcp	avatar-connmgmt
94	wppgen2-	100	us-west-2	pie-vpc1-dvc-pod1-subnet-a-avcmt-Security	Allow all outbound access. Allow incoming ssh and 80	sg-00001	vpc-000001	22	22	10.101.0.0/16	tcp	avatar-connmgmt
95	xmo123	100	us-east-1	xmo2-stage-04-SecurityGroupIntraAppTier-1	xmo2-stage-04 Intra-App tier (App instance to App ins	sg-00001	vpc-000001	1	65535	sg-0000011	tcp	xmo2-stage-04-app03, xmo2-stage-04-app05, xmo2-
102	hpifttt-de	100	us-west-2	rds-launch-wizard-14	Created from the RDS Management Console	sg-00001	vpc-000001	3306	3306	0.0.0.0/0	tcp	alexa
103	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	80	80	sg-0000011	tcp	sds-test-rules-env
104	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	8080	8080	sg-0000011	tcp	sds-test-rules-env
105	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	15.176.0.0/13	tcp	sds-test-rules-env
106	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	15.64.0.0/11	tcp	sds-test-rules-env
107	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	15.0.0.0/10	tcp	sds-test-rules-env
108	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	15.96.0.0/12	tcp	sds-test-rules-env
109	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	15.186.0.0/15	tcp	sds-test-rules-env
110	sds-dev	100	us-east-1	awseb-e-ae8pfgkcwm-stack-AWSEBSecurity	VPC Security Group	sg-00001	vpc-000001	22	22	15.160.0.0/12	tcp	sds-test-rules-env

Nessus – SCAP (security content automation protocol) compliant scanner




tenable.io
Vulnerability Management
Dashboards
Scans
Reports
Settings
Advanced
Search Assets
WORKBENCH
Vulnerabilities
Assets
Web Applications
Health & Status
ANALYTICS
My Dashboards
Outstanding Patch ...
Prioritize Hosts
Vulnerabilities by C...
Vulnerabilities
Last 30 Days
Export
By Plugin
By Asset
LAST UPDATED: 02:42 PM
OPERATING SYSTEM
Windows
Mac OS
Linux
Other
DEVICE TYPES
Desktop /Server
AUTHENTICATION
Local
LAST SCANNED
7 Days
14 Days
30 Days
ASSETS OVER TIME
600
500
400
300
200
100
0
ASSETS WITH VULNERABILITIES: 1027
Asset
Vulnerabilities
Last Seen
ip-10-10-2-70.ec2.internal
19
93
68
6
02:27 AM
ip-10-10-1-159.ec2.internal
18
93
68
07:01 AM
ip-10-10-1-236.ec2.internal
18
93
68
07:01 AM
ip-10-10-1-229.ec2.internal
18
93
68
07:01 AM

Prod-LW-Web2

‹ Back to latex-prod

Configure | Launch | Audit Trail | Export

Switch Host: Prod-LW-Web2

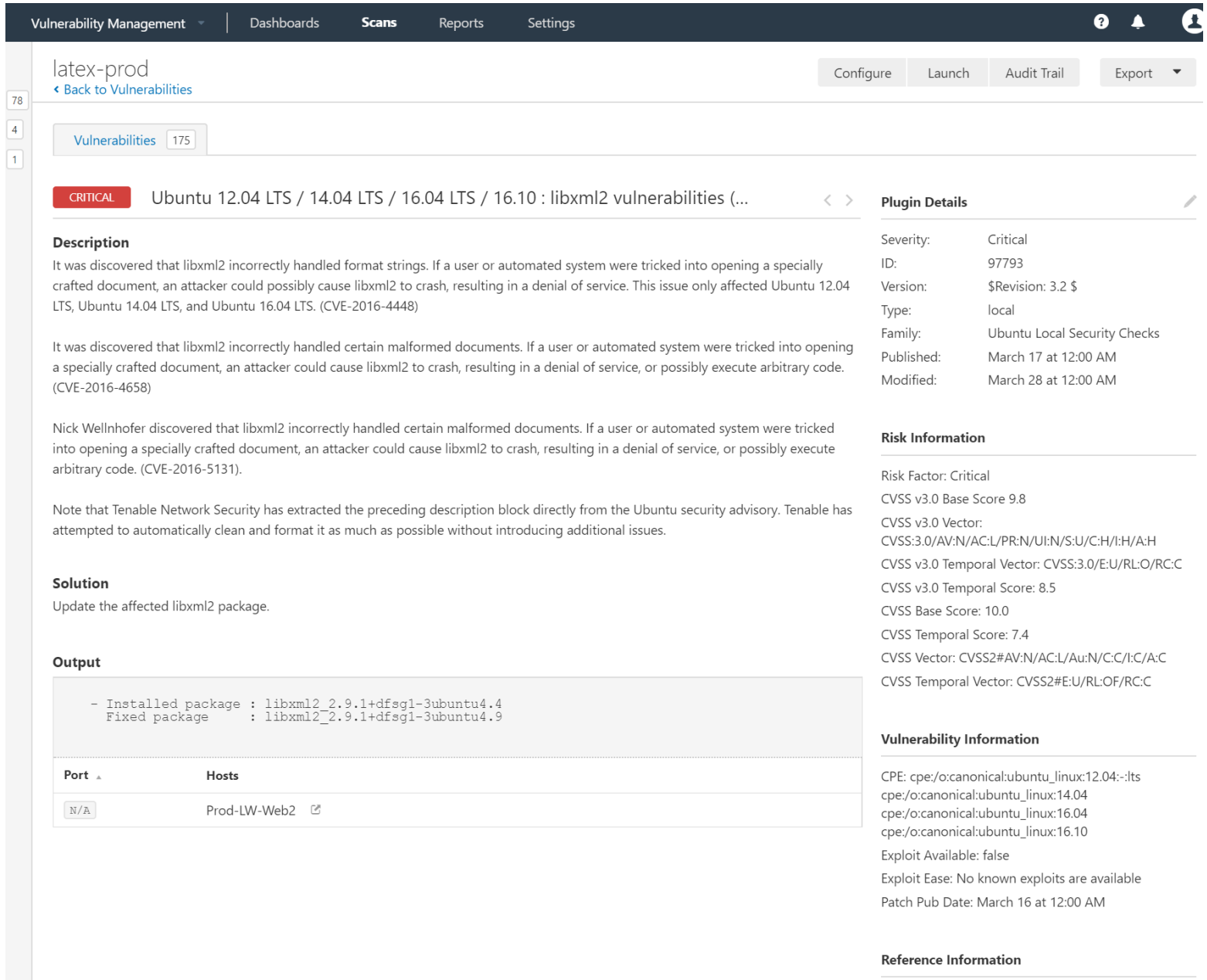
Vulnerabilities 175

Sev	Name	Family	Count
●	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : imagemagick vulner...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libxml2 vulnerabilitie...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : git vulnerabilities (USN-2938-1)	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : icu vulnerabilities (U...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxml2 vulnerabilitie...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python2.7, python3.2, pytho...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS : libdbd-mysql-perl vulnerabilities (USN-...	Ubuntu Local Security Checks	1
●	Ubuntu 14.04 LTS : lcms2 vulnerability (USN-2961-1)	Ubuntu Local Security Checks	1
●	Ubuntu 14.04 LTS : linux vulnerabilities (USN-3343-1)	Ubuntu Local Security Checks	1
●	Ubuntu 14.04 LTS : linux vulnerabilities (USN-3360-1)	Ubuntu Local Security Checks	1
●	Ubuntu 14.04 LTS : linux vulnerability (USN-3188-1)	Ubuntu Local Security Checks	1
●	Ubuntu 14.04 LTS : linux, linux-meta vulnerabilities (USN-3335-1) (Stac...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : apport vulnerability (US...	Ubuntu Local Security Checks	1
●	Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : dpkg vulnerability (USN-...	Ubuntu Local Security Checks	1

Host Details

IP:	172.16.1.6
DNS:	Prod-LW-Web2
MAC:	12:fa:42:8e:11:0b
OS:	Linux Kernel 3.13.0-65-generic on Ubuntu 14.04
Start:	Today at 1:26 AM
End:	Today at 1:26 AM
Elapsed:	a few seconds
KB:	Download

Vulnerabilities


Vulnerability Management
Dashboards
Scans
Reports
Settings
78
4
1
latex-prod
Back to Vulnerabilities
Configure
Launch
Audit Trail
Export
Vulnerabilities 175
CRITICAL
Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxml2 vulnerabilities (...
Description
It was discovered that libxml2 incorrectly handled format strings. If a user or automated system were tricked into opening a specially crafted document, an attacker could possibly cause libxml2 to crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 LTS, Ubuntu 14.04 LTS, and Ubuntu 16.04 LTS. (CVE-2016-4448)
It was discovered that libxml2 incorrectly handled certain malformed documents. If a user or automated system were tricked into opening a specially crafted document, an attacker could cause libxml2 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-4658)
Nick Wellnhofer discovered that libxml2 incorrectly handled certain malformed documents. If a user or automated system were tricked into opening a specially crafted document, an attacker could cause libxml2 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-5131).
Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.
Solution
Update the affected libxml2 package.
Output
- Installed package : libxml2_2.9.1+dfsg1-3ubuntu4.4
Fixed package : libxml2_2.9.1+dfsg1-3ubuntu4.9
Port
Hosts
N/A
Prod-LW-Web2
Plugin Details
Severity: Critical
ID: 97793
Version: $Revision: 3.2 $
Type: local
Family: Ubuntu Local Security Checks
Published: March 17 at 12:00 AM
Modified: March 28 at 12:00 AM
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 8.5
CVSS Base Score: 10.0
CVSS Temporal Score: 7.4
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/o:canonical:ubuntu_linux:12.04:-:lts
cpe:/o:canonical:ubuntu_linux:14.04
cpe:/o:canonical:ubuntu_linux:16.04
cpe:/o:canonical:ubuntu_linux:16.10
Exploit Available: false
Exploit Ease: No known exploits are available
Patch Pub Date: March 16 at 12:00 AM
Reference Information

78
4
1

CRITICAL

Ubuntu 14.04 LTS : linux, linux-meta vulnerabilities (USN-3335-1) (Stack Clash)

Description

It was discovered that the stack guard page for processes in the Linux kernel was not sufficiently large enough to prevent overlapping with the heap. An attacker could leverage this with another vulnerability to execute arbitrary code and gain administrative privileges (CVE-2017-1000364)

It was discovered that a use-after-free vulnerability in the core voltage regulator driver of the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2014-9940)

It was discovered that a buffer overflow existed in the trace subsystem in the Linux kernel. A privileged local attacker could use this to execute arbitrary code. (CVE-2017-0605)

Roee Hay discovered that the parallel port printer driver in the Linux kernel did not properly bounds check passed arguments. A local attacker with write access to the kernel command line arguments could use this to execute arbitrary code. (CVE-2017-1000363)

Li Qiang discovered that an integer overflow vulnerability existed in the Direct Rendering Manager (DRM) driver for VMware devices in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.
(CVE-2017-7294)

A double free bug was discovered in the IPv4 stack of the Linux kernel. An attacker could use this to cause a denial of service (system crash). (CVE-2017-8890)

Andrey Konovalov discovered an IPv6 out-of-bounds read error in the Linux kernel's IPv6 stack. A local attacker could cause a denial of service or potentially other unspecified problems. (CVE-2017-9074)

Andrey Konovalov discovered a flaw in the handling of inheritance in the Linux kernel's IPv6 stack. A local user could exploit this issue to cause a denial of service or possibly other unspecified problems.
(CVE-2017-9075)

It was discovered that dccp v6 in the Linux kernel mishandled inheritance. A local attacker could exploit this issue to cause a denial of service or potentially other unspecified problems.
(CVE-2017-9076)

It was discovered that the transmission control protocol (tcp) v6 in the Linux kernel mishandled inheritance. A local attacker could exploit this issue to cause a denial of service or potentially other unspecified problems. (CVE-2017-9077)

It was discovered that the IPv6 stack was doing over write consistency check after the data was actually overwritten. A local attacker could exploit this flaw to cause a denial of service (system crash).
(CVE-2017-9242).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

Solution

Update the affected packages.

Output

```
  - Installed package : linux-image-3.13.0-87-generic_3.13.0-87.133
    Fixed package     : linux-image-3.13.0-121-generic_3.13.0-121.170

  - Installed package : linux-image-virtual_3.13.0.65.71
    Fixed package     : linux-image-virtual_3.13.0.121.131
```

Plugin Details

Severity:	Critical
ID:	100933
Version:	$Revision: 3.5 $
Type:	local
Family:	Ubuntu Local Security Checks
Published:	June 20 at 12:00 AM
Modified:	August 16 at 12:00 AM

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:ND

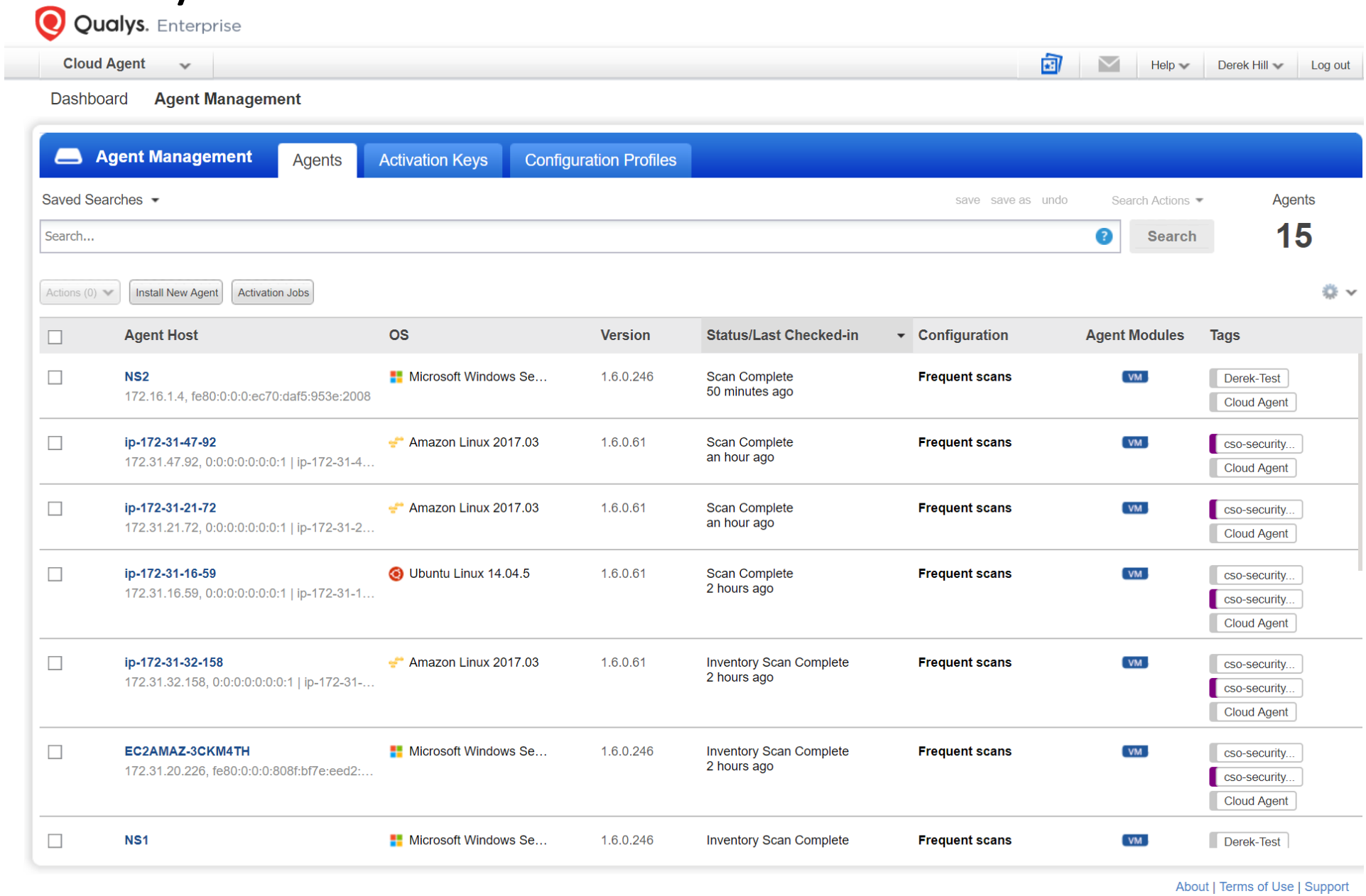
Vulnerability Information

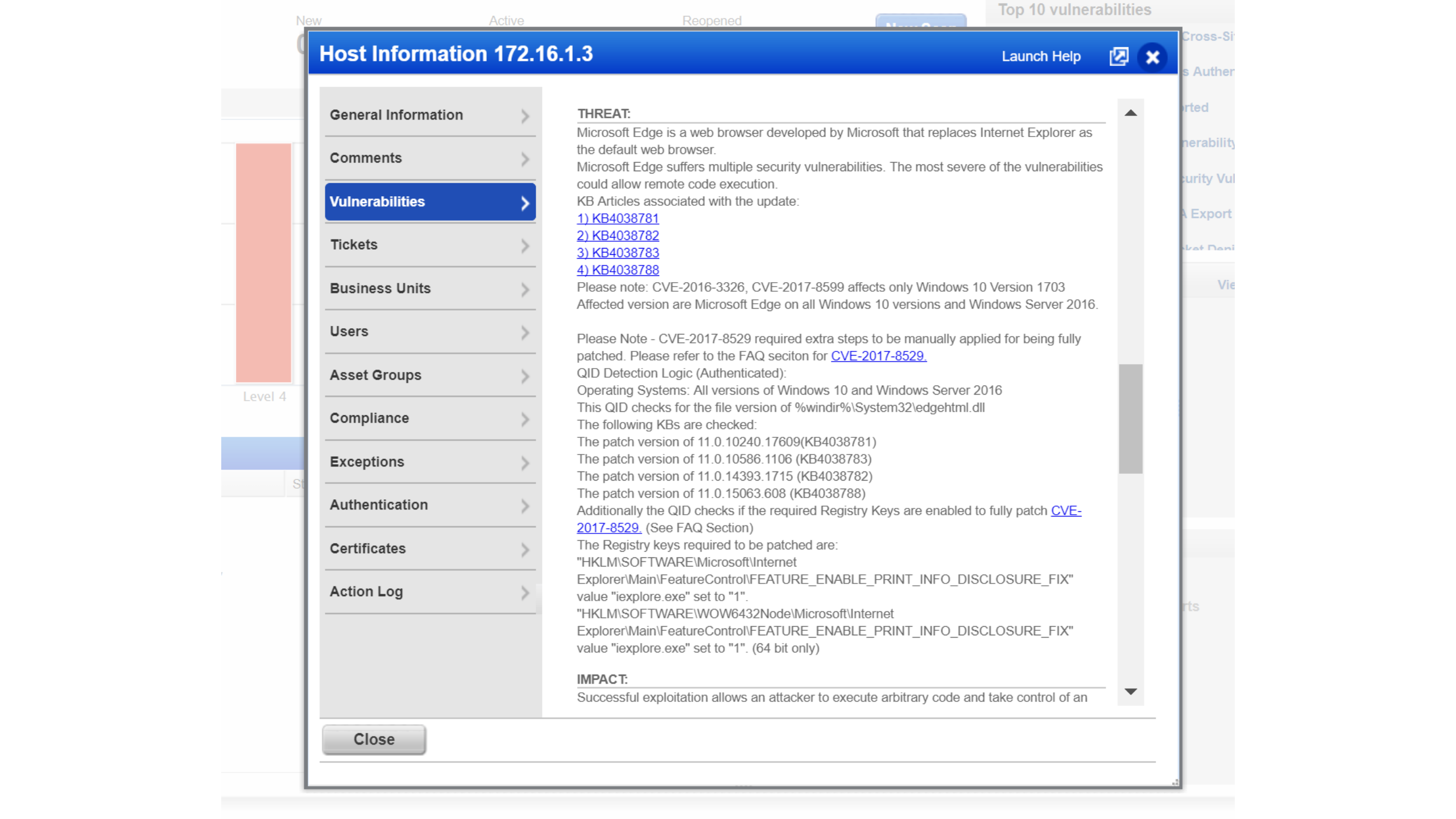
CPE: cpe:/o:canonical:ubuntu_linux:14.04
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: June 19 at 12:00 AM
In the news: true

Reference Information

USN: 3335-1
OSVDB: 154548, 156817, 157027, 157334, 157813, 157814, 157815, 157876, 158030, 158171, 159367
CVE: CVE-2014-9940, CVE-2017-0605, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-7294, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242

Qualys – another SCAP scanner

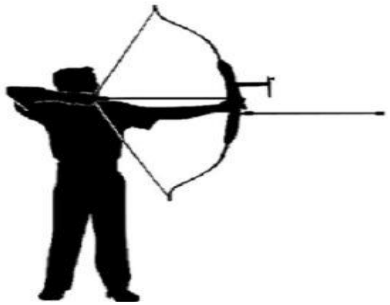


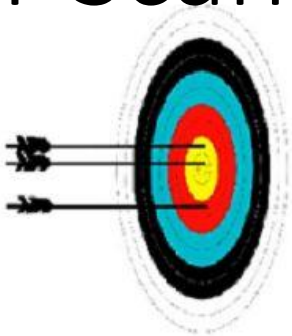

Host Information 172.16.1.3
Launch Help
General Information
Comments
Vulnerabilities
Tickets
Business Units
Users
Asset Groups
Compliance
Exceptions
Authentication
Certificates
Action Log
THREAT:
Microsoft Edge is a web browser developed by Microsoft that replaces Internet Explorer as the default web browser.
Microsoft Edge suffers multiple security vulnerabilities. The most severe of the vulnerabilities could allow remote code execution.
KB Articles associated with the update:
1) KB4038781
2) KB4038782
3) KB4038783
4) KB4038788
Please note: CVE-2016-3326, CVE-2017-8599 affects only Windows 10 Version 1703
Affected version are Microsoft Edge on all Windows 10 versions and Windows Server 2016.
Please Note - CVE-2017-8529 required extra steps to be manually applied for being fully patched. Please refer to the FAQ seciton for CVE-2017-8529.
QID Detection Logic (Authenticated):
Operating Systems: All versions of Windows 10 and Windows Server 2016
This QID checks for the file version of %windir%\System32\edgehtml.dll
The following KBs are checked:
The patch version of 11.0.10240.17609(KB4038781)
The patch version of 11.0.10586.1106 (KB4038783)
The patch version of 11.0.14393.1715 (KB4038782)
The patch version of 11.0.15063.608 (KB4038788)
Additionally the QID checks if the required Registry Keys are enabled to fully patch CVE-2017-8529. (See FAQ Section)
The Registry keys required to be patched are:
"HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX" value "iexplore.exe" set to "1".
"HKLM\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX" value "iexplore.exe" set to "1". (64 bit only)
IMPACT:
Successful exploitation allows an attacker to execute arbitrary code and take control of an
Close

Correlating the data

- How do know if all of your instances have agents/scanners installed?
- How do you do this across multiple accounts/regions?
- Often this requires custom solutions, in our case we are using python scripts to extract the data into CSV format and then correlate in Excel. We are currently in the process of getting this data into a database for automated correlation
- Have you done this in your environment?
  - How many unauthorized systems do you have?
  - How many of them are running production sites?

Acunetix – Web-based DAST Scanning



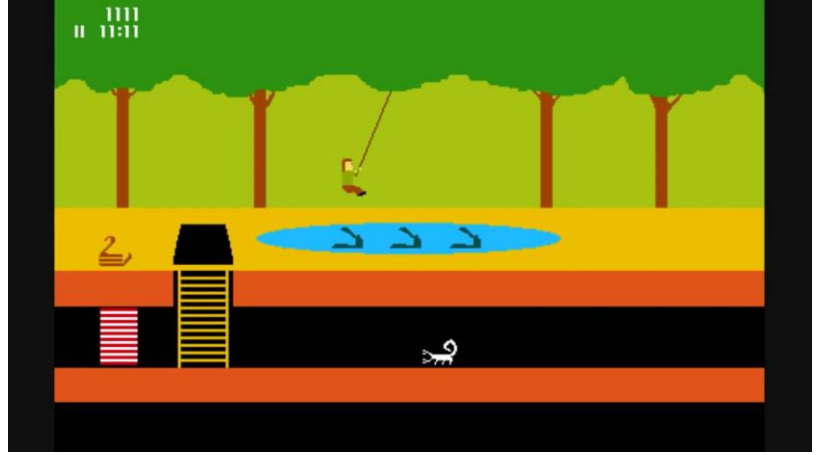


- Blackbox external scanning for web endpoints – User sites, Management Portals, APIs, anything using HTTP/S
- Relatively mature method of scanning applications.
- DAST scanning over HTTP/S is generally considered “language independent”, even though you could be injecting code as part of an attack.
- Large amount of tools available, great for comparisons on the same site to be inspected. List helpfully provided by OWASP https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
- Another helpful list of DAST scanner list http://projects.webappsec.org/w/page/13246988/Web%20Application%20Security%20Scanner%20List

Acunetix – Continued, Common Encounters

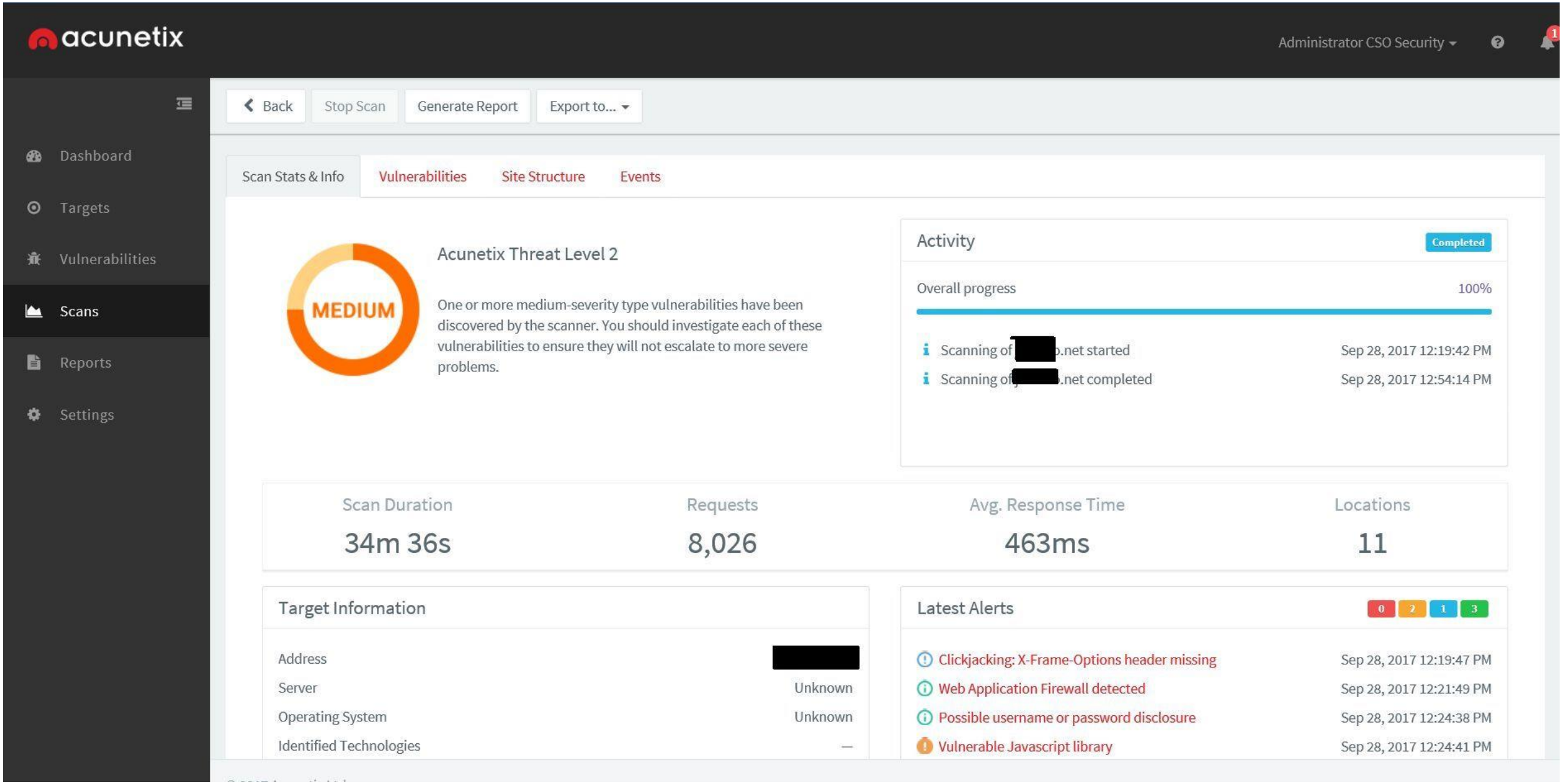
- Authenticated and Unauthenticated - Both absolutely necessary!
  - Authenticated - The more complex the login requirements, the more flexible the tool needs to be at following a “login script” – Proxies, Load Balancers, etc
  - Unauthenticated – Will turn up common misconfigurations with the web server, DNS, certs. Things that an attacker would immediately see and attempt to seize up on to begin building the attack.
- On-prem vs. Cloud – **What’s the right answer?** As Always, It Depends on your company, your product and
  - Wider Geo location availability easily achieved with Cloud, but maybe you already have that with your own network and systems.
  - Localized language and dash boarding for remote teams. People don’t use tools they can’t find value in.

DAST Pitfalls



- Lot’s of Work! Management Approval, gathering Red team suggestions and info for specific areas of concern, coordination with one or more dev/ops/NOC/SOC
- Need approval from AWS if doing suspicious looking things from their instances, however a wide variety of services are available. Your home connection from behind 7 proxies for example
- Hard to get approval for testing production, but black box should be easier to get a “yes” and should be done. Free Tools, More info! Provide results and graphs diagrams for any PHB
- Too much fun. You will realize how insecure everything is and will begin having nefarious thoughts.

Acunetix Results



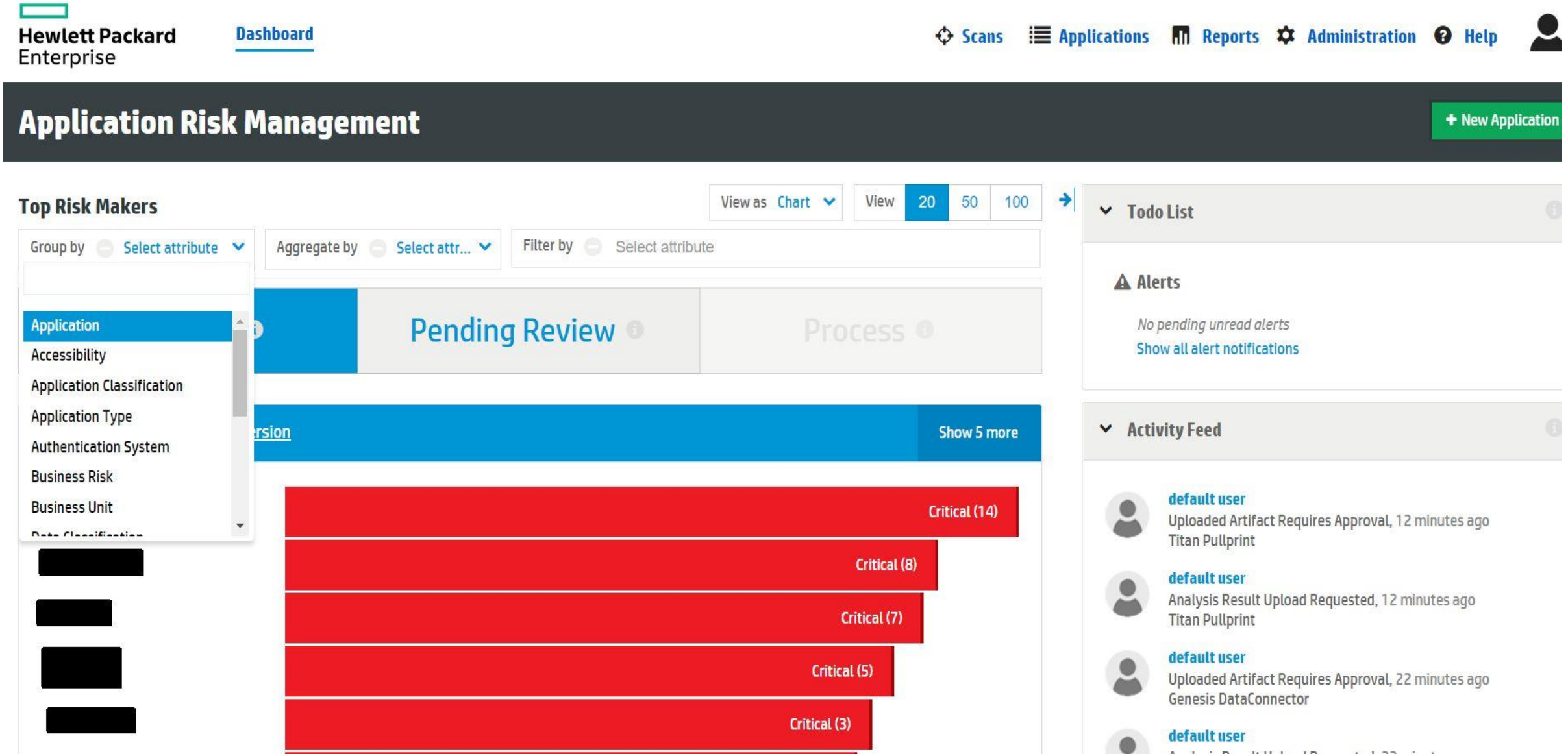
HP Enterprise Fortify Code Scanning – SAST

- Fortify has two main parts (fairly common setup for this type of tool)
  - The scanner, Fortify Static Code Analyzer (SCA)
  - The reporting interface, Fortify Software Security Center (SSC)
- Robust. Wide range of IDEs, build platforms and code support
- My Experience with Fortify, is that it has a distinct DIY flavor to it. That kind of functionality not really available in Cloud-based offerings.
- Just exactly how custom does your does your build environment need to be to get a successful test run to complete, maybe a non-cloud based SAST saves you a little bit of time and money, but can be lacking language support in some area’s, ECMA6 for example.

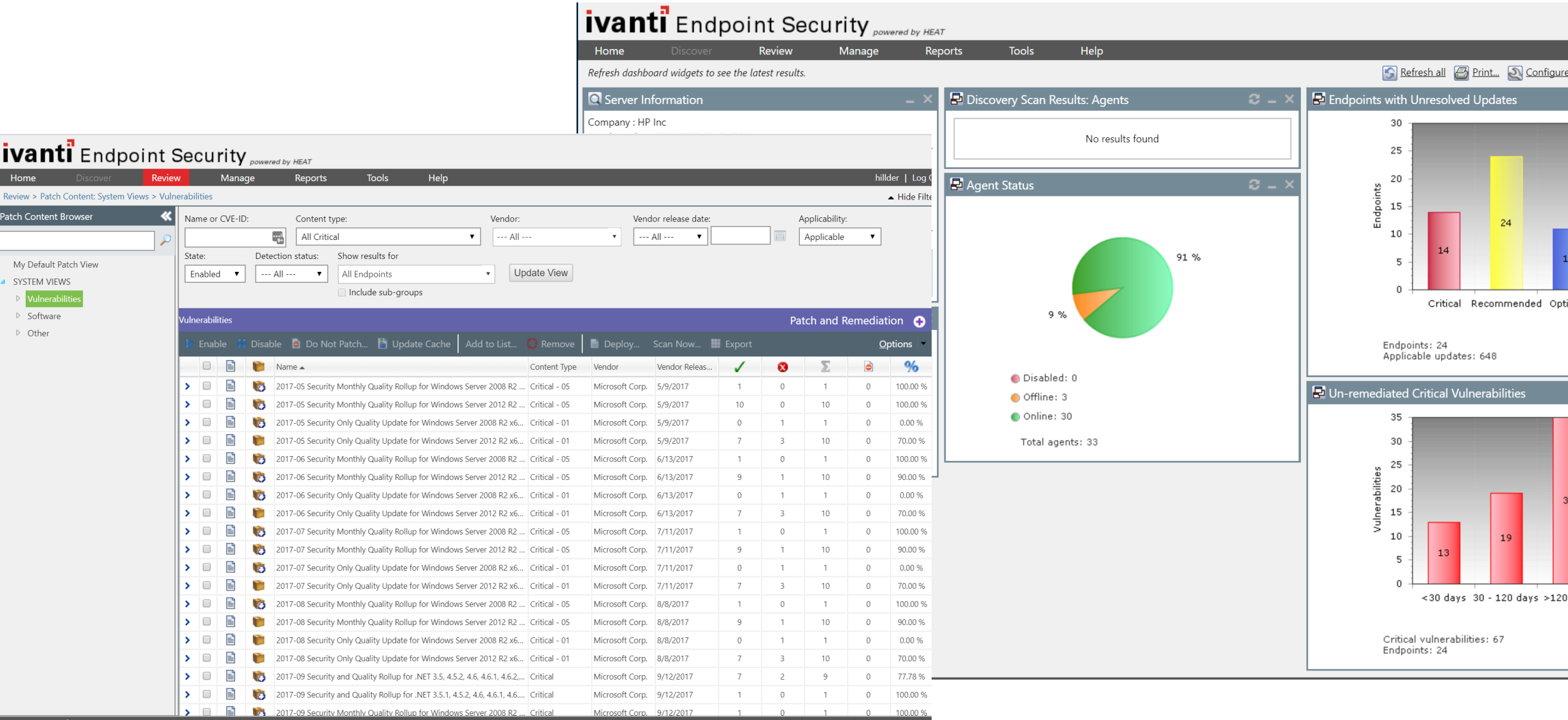
SAST Pitfalls

- Also can be a VERY large amount of work to setup and maintain. Ongoing relatively “boring” work that needs to be done by Highly Technical and Security Trained individuals.
  - Initial scoping of project sizes, platforms, resource utilization, necessary access defining roles and responsibilities
  - Depending on the original code, properly acquiring 3rd party libraries can be a real hassle for true bytecode assembly and analysis
  - Suppression of false positives. This can be monotonous depending on the code, but also an opportunity to suppress forever warnings that are not well understand and can introduce problems during development of new modules, functions
- High proficiency in programming and communication. No one likes to have their mistakes pointed out. Bugs can be new and mysterious, but also sometimes can be obvious and 20 years old. Patience and empathy.

Fortify SSC


Hewlett Packard Enterprise
Dashboard
Scans
Applications
Reports
Administration
Help
Application Risk Management
+ New Application
Top Risk Makers
View as Chart
View 20 50 100
Group by Select attribute
Aggregate by Select attr...
Filter by Select attribute
Application
Accessibility
Application Classification
Application Type
Authentication System
Business Risk
Business Unit
Pending Review
Process
Show 5 more
Critical (14)
Critical (8)
Critical (7)
Critical (5)
Critical (3)
Todo List
Alerts
No pending unread alerts
Show all alert notifications
Activity Feed
default user
Uploaded Artifact Requires Approval, 12 minutes ago
Titan Pullprint
default user
Analysis Result Upload Requested, 12 minutes ago
Titan Pullprint
default user
Uploaded Artifact Requires Approval, 22 minutes ago
Genesis DataConnector
default user

Ivanti – multi platform patching tool



Tool challenges

- There are so many tools, each one handles a specific task, it is impossible to keep track of what tools are out there
- Find tools that work for you and make your processes fit the tools
- Often teams will try to make a tool work with a process – customizing tools can be expensive and prevent you from upgrading
- Don’t chase the latest tool, but rather learn how to use the tools you have more effectively. Are you using all the features?
- This should be an ongoing learning process -- improve and evolve
- Collect user feedback and work with vendors for features and bug fixes

Further reading

- Look into cyber security frameworks/controls
- NIST 800-53
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- ISO 27002 (while not a subset of the NIST 800-53, it has a much smaller focus)
  - https://www.iso.org/standard/54533.html
- Critical Security Control (my recommendation) – good real world controls
  - 20 controls that should be implemented (it will take several years) and most of them can be automated.
  - https://www.cisecurity.org/controls/

Questions?

Presentation can be downloaded from here:

https://github.com/derekhillhp/AWS-Security-Class

Survey

- Please complete a short survey (10 questions) on today's event
  - https://www.surveymonkey.com/r/2D3WC5H
- Your feedback will help us measure the effectiveness of this training and to improve it for the next year