A primer to incident handling / response

Not meant as a substitute for proper training & implementation, but rather just to create interest and shine a light on the subject area

Derek Hill
@secureITtoday
derek@dh-solutions.com or derek.hill@forgerock.com

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 2018
A Big “Thank You” to Our Sponsors

Survey

- Please complete a short survey (10 questions) on this workshop
- https://tinyurl.com/pdxowasp2018w4
- Your feedback will help us measure the effectiveness of this training and to improve it for the next year

Session sponsored by:

ForgeRock

Access Management
Identity Management
Edge Security
Identity Gateway
Directory Services
Profile & Privacy Management

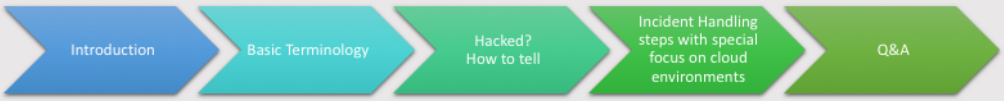
www.forgerock.com

We are always looking for talented people:
https://www.forgerock.com/about-us/careers

Located across the river in Vancouver, WA

FORGEROCK®

Agenda


Introduction
Basic Terminology
Hacked?
How to tell
Incident Handling steps with special focus on cloud environments
Q&A

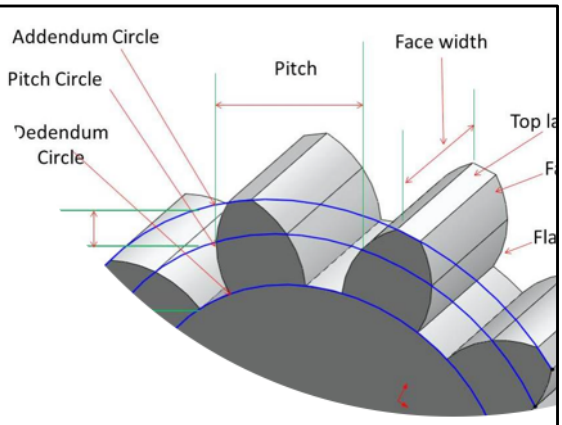
About me

- Geek at heart
- 25+ years in IT and Security
- Been with small startups, Fortune 50 companies and everything in between
- Security and Privacy are passions of mine
  - CISSP, 6 SANS security certifications, IAPP, Microsoft, etc.
  - SANS mentor instructor
  - Active participant in OWASP & ISSA and a member
- Hobbies: Things that go fast
  - Cars
  - Skiing
  - Boating

About you

- Name
- What do you currently do?
- What are you looking to learn today?

- What is an event?
  - Any observable occurrence in a system (computer, network, etc.)
- What is an incident?
  - Adverse event
  - There is an intent to harm
- Who decides when an event becomes an incident?
  - You want this role clearly defined (more on this later)
  - What are the deciding factors?
    - Evidence, how many sources?
    - What is the context?



Some basic terminology

Ask questions to the class

Event or Incident

–you decide

- Successful login attempt
- Failed login attempt
- 500 failed login attempts
- 500 failed login attempts followed by a successful login attempt
- An executive assistant using the bosses credentials
- Webserver crash
- Webserver crash that results in permissions being reset
- Webserver crash that results in permissions being reset and unusual activity

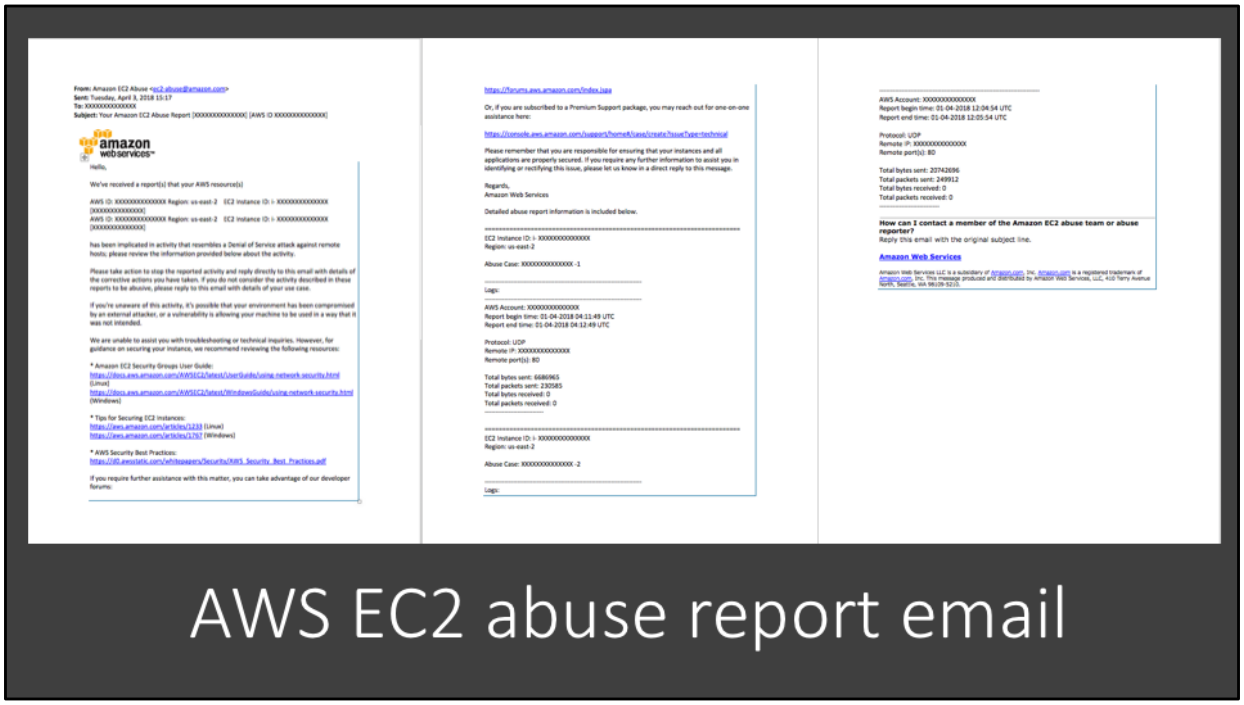
Lots of scary stories

- News
  - Lots of great websites, a great aggregator for security news is
    - http://www.newsnow.co.uk/h/Technology/Security
    - https://www.databreaches.net/
    - Others, such as Brian Krebs https://krebsonsecurity.com/ , Reddit NetSec https://www.reddit.com/r/netsec/ , and many, many more

Verizon DBIR: https://www.verizonenterprise.com/verizon-insights-lab/dbir/
Fortinet Threat Landscape Report: https://ready.fortinet.com/q2-2018-threat-landscape-report/q2-2018-threat-landscape-report

How do I know we have been hacked?

Contact by an outside company, customer, gov't agency	Detection by internal systems	Detection by outside security vendor	Threat hunting exercises
Surprisingly this is the most common way •The dreaded AWS EC2-Abuse email •Call from a 3 letter agency •A customer calling about strange behavior…	Alarm bells going off, SOC notification, deviation from the baseline (you do have baselines?)	MSSP - outsourced security provider that watches your logs/alerts	While this sounds like the coolest way of finding breaches, it is also the least common



From: Amazon EC2 Abuse <ec2-abuse@amazon.com>
Sent: Tuesday, April 3, 2018 15:17
To: XXXXXXXXXXXX
Subject: Your Amazon EC2 Abuse Report [XXXXXXXXXXXXXX] [AWS ID XXXXXXXXXXXXXX]

amazon web services

Hello,

We've received a report(s) that your AWS resource(s)

AWS ID: XXXXXXXXXXXXXX Region: us-east-2 (EC2 Instance ID: i- XXXXXXXXXXXXX [XXXXXXXXXXXXXX]
AWS ID: XXXXXXXXXXXXXX Region: us-east-2 (EC2 Instance ID: i- XXXXXXXXXXXXX [XXXXXXXXXXXXXX]

has been implicated in activity that resembles a Denial of Service attack against remote hosts. please review the information provided below about the activity.

Please take action to stop the reported activity and reply directly to this email with details of the corrective actions you have taken. If you do not consider the activity described in these reports to be abusive, please reply to this email with details of your use case.

If you're unaware of this activity, it's possible that your environment has been compromised by an external attacker, or a vulnerability is allowing your machine to be used in a way that it was not intended.

We are unable to assist you with troubleshooting or technical inquiries. However, for guidance on securing your instance, we recommend reviewing the following resources:

* Amazon EC2 Security Groups User Guide:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html (Linux)
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html (Windows)

* Tips for Securing EC2 Instances:
https://aws.amazon.com/articles/1233 (Linux)
https://aws.amazon.com/articles/1767 (Windows)

* AWS Security Best Practices:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

If you require further assistance with this matter, you can take advantage of our developer forums:

https://forums.aws.amazon.com/index.jspa

Or, if you are subscribed to a Premium Support package, you may reach out for one-on-one assistance here:

https://console.aws.amazon.com/support/home#/case/create?issueType=technical

Please remember that you are responsible for ensuring that your instances and all applications are properly secured. If you require any further information to assist you in identifying or rectifying this issue, please let us know in a direct reply to this message.

Regards,
Amazon Web Services

Detailed abuse report information is included below.

EC2 Instance ID: i- XXXXXXXXXXXXX
Region: us-east-2

Abuse Case: XXXXXXXXXXXXX -1

Logs:

AWS Account: XXXXXXXXXXXX
Report begin time: 01-04-2018 04:11:49 UTC
Report end time: 01-04-2018 04:12:49 UTC

Protocol: UDP
Remote IP: XXXXXXXXXXXXX
Remote port(s): 80

Total bytes sent: 6686965
Total packets sent: 230585
Total bytes received: 0
Total packets received: 0

EC2 Instance ID: i- XXXXXXXXXXXXX
Region: us-east-2

Abuse Case: XXXXXXXXXXXXX -2

Logs:

AWS Account: XXXXXXXXXXXX
Report begin time: 01-04-2018 12:04:54 UTC
Report end time: 01-04-2018 12:05:54 UTC

Protocol: UDP
Remote IP: XXXXXXXXXXXXX
Remote port(s): 80

Total bytes sent: 20742696
Total packets sent: 249912
Total bytes received: 0
Total packets received: 0

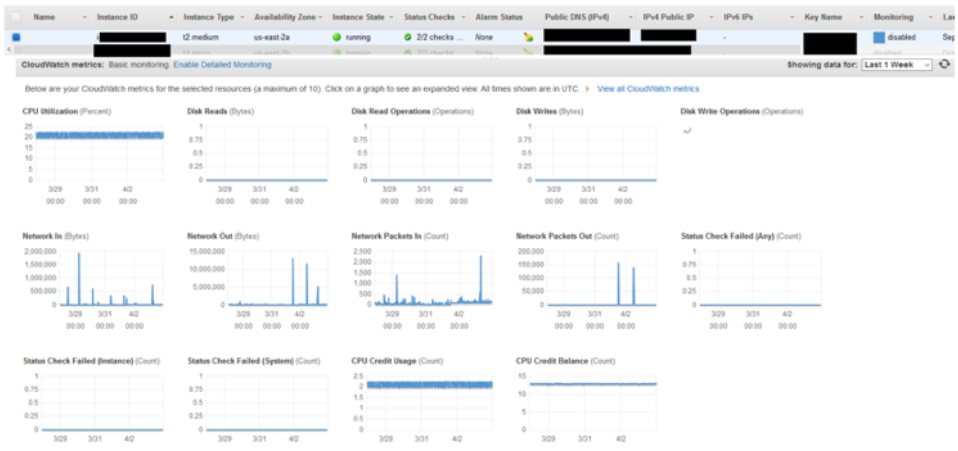
How can I contact a member of the Amazon EC2 abuse team or abuse reporter?
Reply this email with the original subject line.

Amazon Web Services

Amazon Web Services LLC is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message produced and distributed by Amazon Web Services, LLC, 410 Terry Avenue North, Seattle, WA 98109-5210.

AWS EC2 abuse report email

Monitoring in AWS (normal or abnormal?)



Question for the class

- Has your company experienced a breach?
  - Specifics if you can share (Don't name the company)
- How long did it take to detect?
  - Approximately in months/days
- How was it detected?
  - Internally
  - From external sources?
- Do you know for sure that you are currently not experiencing a breach?
  - No need to answer, but just to create some thought

Incident Handling, what does that mean?

- Sometimes referred to as Incident Response, but there is much more to it than simply responding to an incident
- Not something done overnight – unfortunately
- The short answer is:
  - Put your organization into a position where you can detect and respond to an incident in a timely fashion and that you are prepared and have the resources to contain and eradicate the incident effectively.
- A lot of key words in that sentence, we will use an established approach using PICERL

PICERL

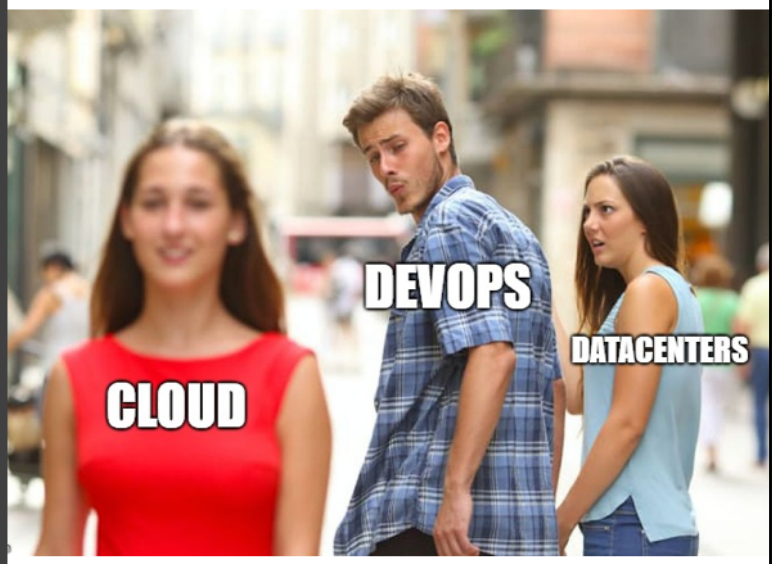
- Preparation – Plan for incidents, practice your plan
- Identification – How can we tell there is an incident vs. just an event
- Containment – Stop the bleeding, but don't kill the patient
- Eradication – Remove the adversary out of your network/systems
- Recovery – Getting back to business
- Lessons Learned – What happened, how can we get better at all of the above?

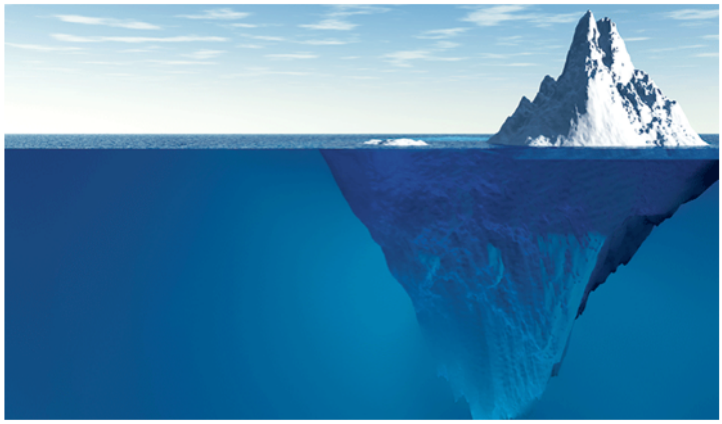
Img source: https://medium.com/@aubsec/incident-response-culture-ee678b1e9ecf

PICERL - visualized

Focusing on the cloud

- The cloud is a slight paradigm shift from the way thing have traditionally been done. I will highlight some of the differences.





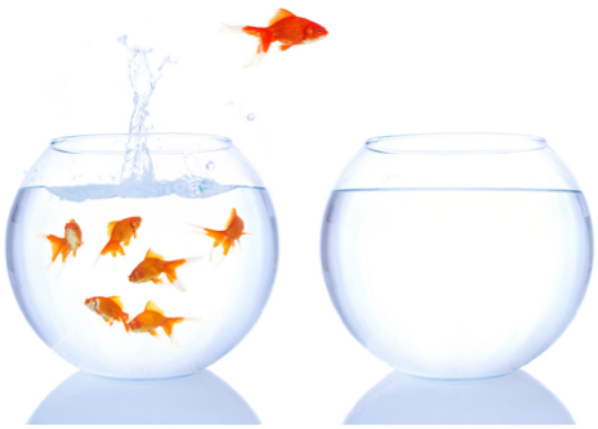
Focusing on the cloud

- What makes the cloud different than traditional in-house networks
  - Lack of visibility
    - Where is your stuff, especially data
    - How is it protected
  - Lack of control / too many "cooks" in the kitchen
    - i.e. no network team protecting you from yourself
    - Uninformed decisions/configurations being made about infrastructure
      - Wide open S3 buckets
      - Security groups not locked down

Focusing on the cloud

-What makes the cloud different than traditional in-house networks

- Change control
  - Hard to do in the cloud with a lot of people having rights to "do things"
- User Access
  - Since many cloud accounts are not tied into company Directory Services, make sure you disable accounts for terminated users
  - Restrict access for only thing things people need access to, don't have everyone be an admin

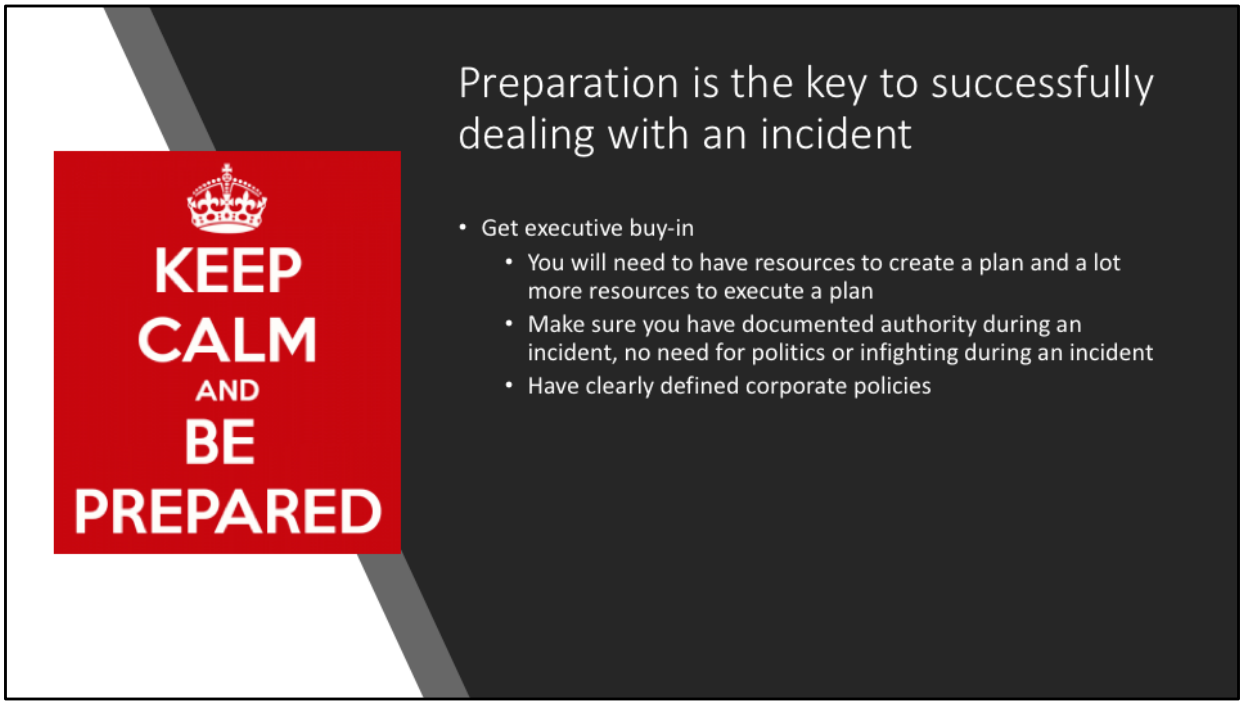


Focusing on the cloud

-more differences

- Ownership
  - Keep production and non productions environment separate
- Sprawl
  - Does this remind people of VM's
  - Things get turned on when they are needed, but often never turned off or simply forgotten

Preparation



Without executive buy in this is almost a pointless exercise as you will have to secure funding, resources and department commitment in order to be successful

Preparation is the key to successfully dealing with an incident

- Build a plan
  - How detailed the plan is will depend on the size of your organization
  - Create a list of roles and responsibilities, you don't need any infighting during an incident – update this as people change
  - Have an offline copy you can distribute in case the electronic version is not available or it has been compromised
- Have your legal department involved in this
  - Legal and privacy issues could cause problems
  - CAN be a really big issue if you are dealing in multi-national companies and your actions can be subject to multiple jurisdictions – think privacy laws here

Without executive buy in this is almost a pointless exercise as you will have to secure funding, resources and department commitment in order to be successful

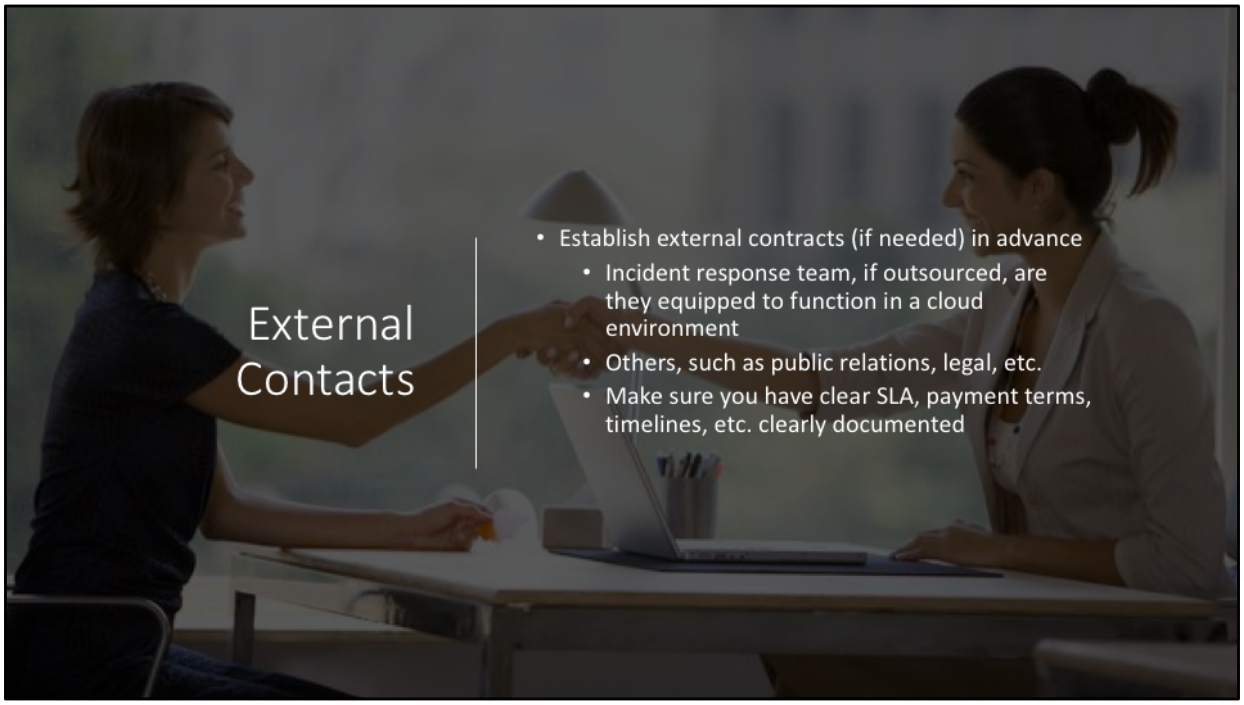
Communication

- Create a communications plan
- Establish external contracts (if needed) in advance
- Establish contacts with law enforcement as well as peers before an incident

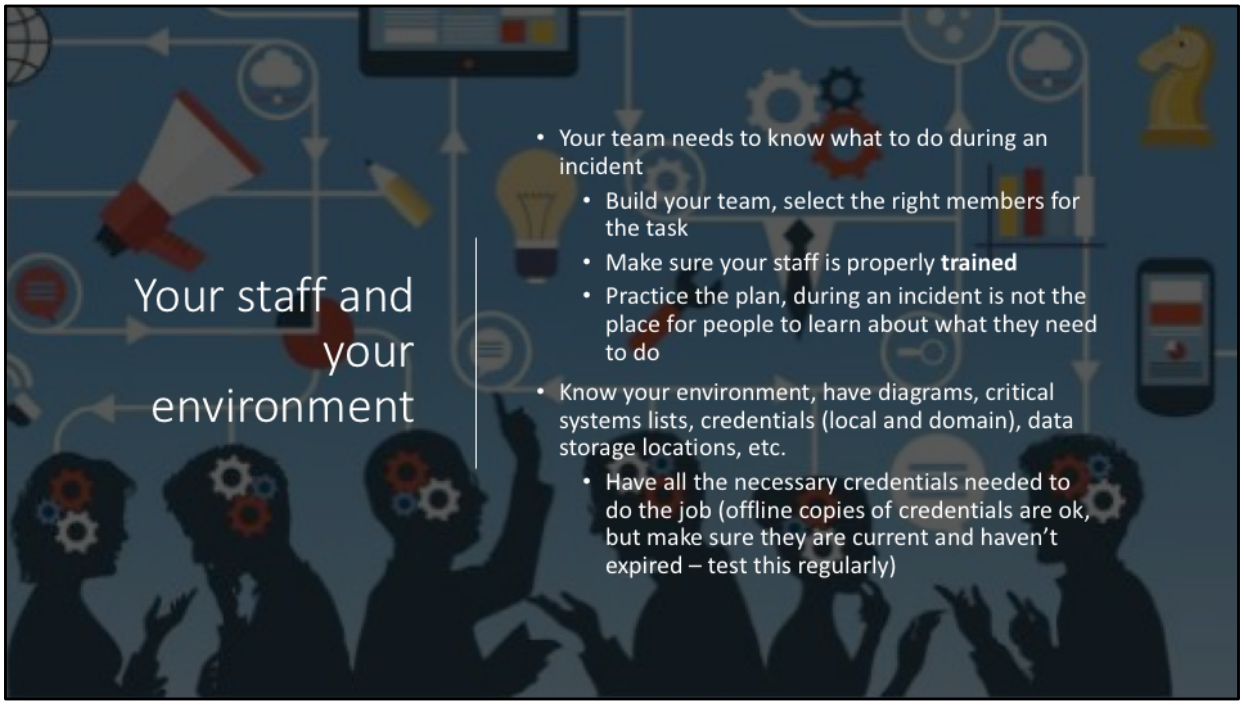
How many people here have an alternate communication channel setup and ready to go, at the very least a list of email addresses that are not corporate, cell numbers, home numbers, etc.

Communications Plan

- Avoid using company systems email/phone during an incident, the adversary can be in your system and see all communication
  - Setup alternate email accounts ahead of time
    - Make sure people know about them
    - Trusted outside accounts
- Establish the communication stakeholders


External Contacts
• Establish external contracts (if needed) in advance
• Incident response team, if outsourced, are they equipped to function in a cloud environment
• Others, such as public relations, legal, etc.
• Make sure you have clear SLA, payment terms, timelines, etc. clearly documented


Contacts with Law Enforcement
• Join and participate in chapter meetings (ISACA, ISSA, InfraGard, OWASP, etc)
• Meet on a regular basis and keep connections active
• They are more likely to work with you if you have an established relationship
• More likely to believe you
• More likely to trust
• More likely to share information with you
POLICE LINE DO NOT CROSS
POLICE LINE



Ask a question to the class to see if they have all of these items such as diagrams, documentation, etc.

Your staff and your environment

- Enable logging on all your devices
  - You cannot use data you don't have
  - Centralized (remote) logging is more effective and harder to tamper with by the adversary
  - Log correlation via a SIEM is often a way an incident is detected
- Define a war room, both physical and on-line
- Most important – Practice your plan, not just once, but on a regular basis

Note Taking

- Be meticulous and record every detail
  - Be calm
  - Note everything, you would be surprised how much usefulness the little details can have later
  - Hand written notes can be hard to organize, but there are times when they are appropriate
    - Use a bound notebook, that way you won't lose pages and they are in order (also number every page – think chain of evidence)
    - Juries love them (in case of prosecution)
    - Easy to draw diagrams
    - Pencils and pens are always around and don't run out of battery
    - Harder to steal
      - If taking notes on the computer, it might make sense to use an offline computer that a hacker cannot see on the network that they have compromised
  - Don't go faster than your note taking ability – when in doubt slow down and contemplate the next course of action
  - Take pictures with your digital camera/phone and record voice memos if appropriate

Jump bag
--yes even for the cloud

- Make sure you have all the required equipment
  - Yes, cloud based incidents could have portions of the attack happen on your local networks, especially if they have been connected
  - Notebooks (pages pre-numbered), pens and pencils, incident handling forms
  - Computers with the appropriate OS's and specifications [memory, disk space], make sure they are updated regularly (OS installation media if necessary, also Virtualization software preinstalled)
  - Flash drives, hard drives, disk duplicators, etc.
  - Network cables, hubs, taps, switches, power cords

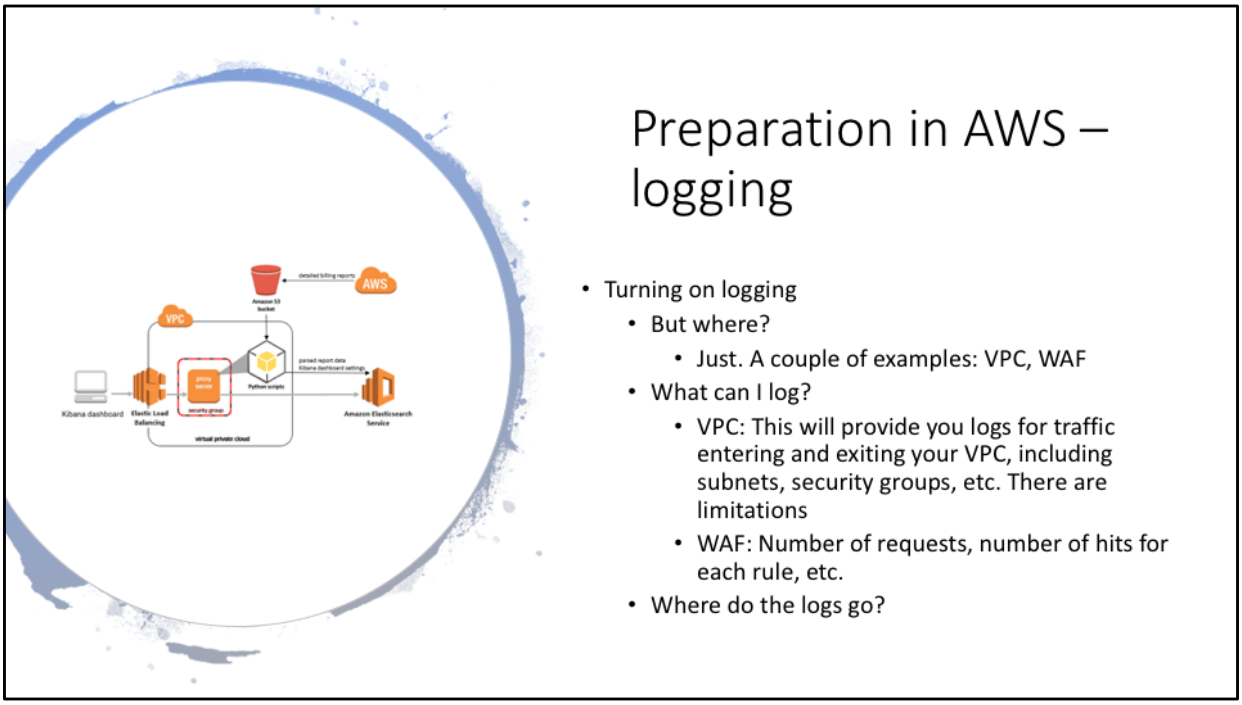
Jump bag
--yes even for the cloud

- Make sure you have all the required equipment
  - Software
    - More on this later
  - Alternate cloud accounts with the appropriate permissions
    - Local not LDAP, ADFS, SAML
    - Don't forget the MFA tokens if you are using hardware based ones
  - Cell phones, chargers and extra batteries (if appropriate)
    - Call lists (good to have hard copies – make sure the lists are updated regularly)
  - Change of clothes including personal hygiene items
    - You might be there for a while

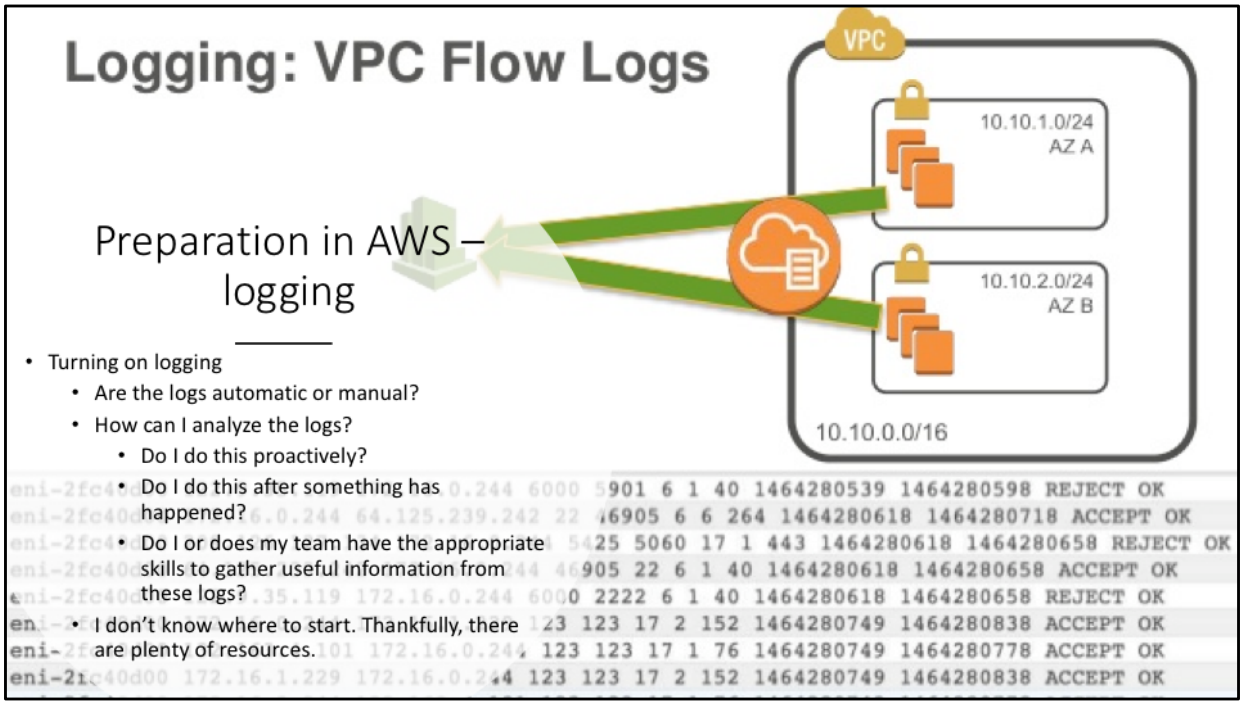

Focusing on the Cloud
• Have to proactively turn on additional logging, such a VPC flow logging.....this pretty much applies to all cloud vendors
• AWS and Google Cloud - VPC flow logging
• Azure – Network Security Group (NSG) flow logging
• Now what, what do you do with this data
• Cloud Trail -> S3 buckets -> to where now?
• In house analysis
• 3rd party analysis
• Do you even look at this data unless there is an issue?
• Detection is the key here
• Nice to have evidence, but by then the bad stuff has already happened

Focusing on the Cloud

- Know your normal billing amounts, you would be surprised that some customers have discovered they had a breach after bills skyrocketed
- Do you have software that monitors your cloud size?
  - Use tools such as Cloud Watch to monitor for unusual resource utilization
- Is your cloud deployment clearly defined and monitored
  - New regions being brought online
  - New VPC created
- Do you have the right tools in place or know how to use the free tools available
  - Ie. Memory capture, log analysis, timelining, etc….



VPC Logging: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
WAF Logging: https://docs.aws.amazon.com/waf/latest/developerguide/monitoring_automated_manual.html and https://docs.aws.amazon.com/waf/latest/developerguide/monitoring_overview.html



WAF Logging:
https://docs.aws.amazon.com/waf/latest/developerguide/resources.html


Identification

Identification
Can you determine if an incident has occurred

- Is it an event or an incident?
  - Look for correlating evidence
  - Even if you suspect something, but are not 100% sure, it is good to declare an incident early – better err on the side of caution
- Correlation is a key in finding the incident
  - A SIEM can help tremendously in this
  - Properly trained personnel are invaluable in this area, no automated system can fully find these issues
  - Unless you have the data (logs), events, etc. you are going to be blind
  - Don't just look at new events, look for things already inside your network – go threat hunting
- Look for indicators of compromise (IOC)

Target is a good example of where people didn't declare an incident even though the evidence was there. Part of the problem was cultural – elaborate a bit more on this.

Ok something if fishy here

- Determine severity, urgency and initial impact
- Document everything meticulously
  - Create a timeline of when, who, what – this might need to be used in a criminal investigation and could become evidence. Even better if you have trained evidence handlers on your team (think preparation)
- Review and take the appropriate actions based on your plan
  - This could include calling in outside resources previously retained, law enforcement, legal council, etc.
- Communicate to stakeholders
  - Make sure you have up to date information

Incident Handling – things are getting real

- Have a primary person in charge of the incident
  - Last thing you need is power grabs during an incident
  - Primary person assigns roles within the team (delegate)
  - There should be an assistant to the primary person to speed things up and not have bottle necks
- Keep things need to know, but know when to communicate
  - Keep the number of people to a minimum (make sure they know to keep things quiet)
  - Use offline methods (discussed earlier) until you can confirm that the company email, IM, voicemail and other communication systems have not been compromised
- If storing notes online, make sure they data is sufficiently protected (encryption at rest and transit)

IR in AWS

- How to approach
  - Attack surface (services running on system)
  - Infrastructure configuration (security groups, S3 bucket policies, IAM user permissions)
  - IOC (malware deployed), evidence of file system changes (permissions), cron jobs, init/startup scripts
  - Log analysis to correlate any of the above (application logs, system logs, etc.)
  - Timeline everything, it will help piece the puzzle together
  - Preserve evidence, ie. Capture memory, snapshot filesystem, isolate system form rest of infrastructure (block inbound and outbound access)
- Tools to use
  - Variety of AWS provided tools, open source tools, commercial tools (key is to know how to use the tools)
    - Using SHODAN search engine to see what else is exposed
  - Tools are also OS specific

IR in AWS (2)

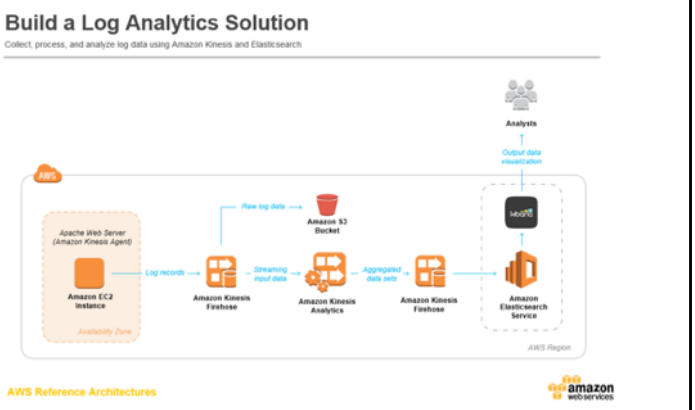
- Root causes
  - Often very simply basic omission of security practices
    - Lack of patches of commercial software
    - Custom code that has security flaws
    - Permissions too open (file system) (credentials i.e. DB server account)
    - Insufficient infrastructure protections in place
      - Mixing of production and development environments
      - User accounts with too many permissions
      - Running services as root
    - Not subscribing to defense in depth
- Determine what they took (Exfil) (or had access to)
  - You might have to notify authorities, customers, etc. in case of data loss
- What if systems were destroyed and you didn't have backups (not that uncommon in non mature cloud adoption)
  - Automated configuration i.e. Cloud Formation, Infrastructure as Code to restore services
    - What about the data, is is replicated across regions, countries, etc.
    - How do you handle corrupted or deleted data?

Log analysis in AWS – Build or buy

- Over the last year or so the AWS tools to help with analysis has improved tremendously.
- Build your own or "buy" a solution or even outsource it
  - Decision you will have to make
    - Factors:
      - Does your team have the right skills
      - Does your team have the capacity to take on this responsibility
      - Timeline and Budget
      - Is your environment very dynamic or somewhat static
      - What sort of compliance rules do you need to follow (PCI, HIPAA, GDPR, etc.)

Log analysis in AWS – Building made easy

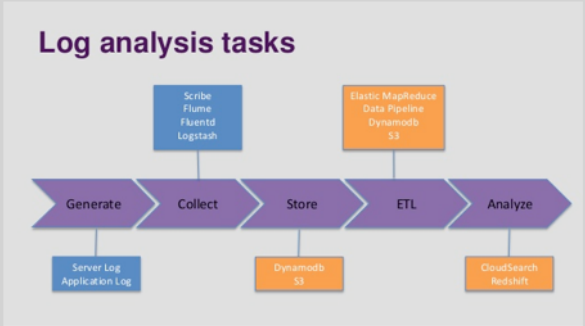
- Build your own using tools in AWS:
  - https://aws.amazon.com/getting-started/projects/build-log-analytics-solution/
  - Cookbook document: https://d1.awsstatic.com/Projects/P4113850/aws-projects_build-log-analytics-solution-on-aws.pdf

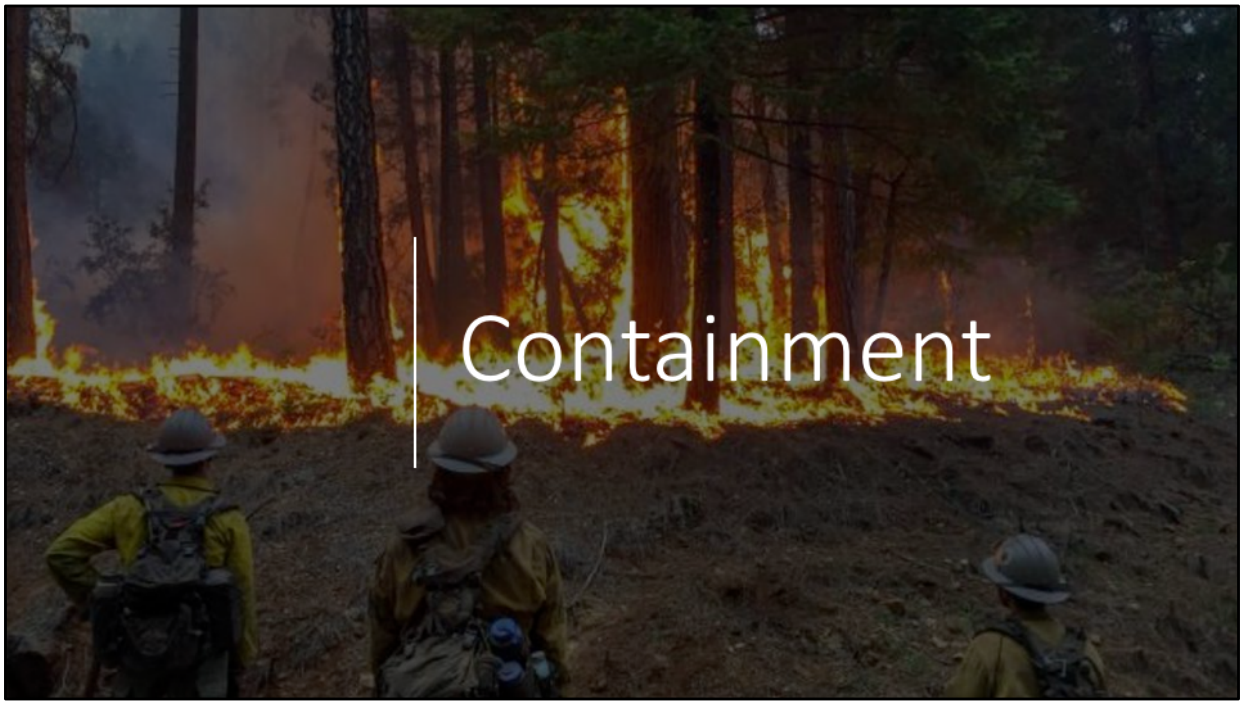


Disadvantages of vendor lock-in, it makes switching costs harder. What if you are not in AWS today, what solutions exist for my cloud solution? What if the vendor discontinues the tools?

AWS use case presentation -- not mine, but very good ☺

- Great presentation on a use case for AWS log analysis use case:
- Use this to help bring the point across to your team members and management:
- https://www.slideshare.net/AmazonWebServices/log-analytics-with-aws



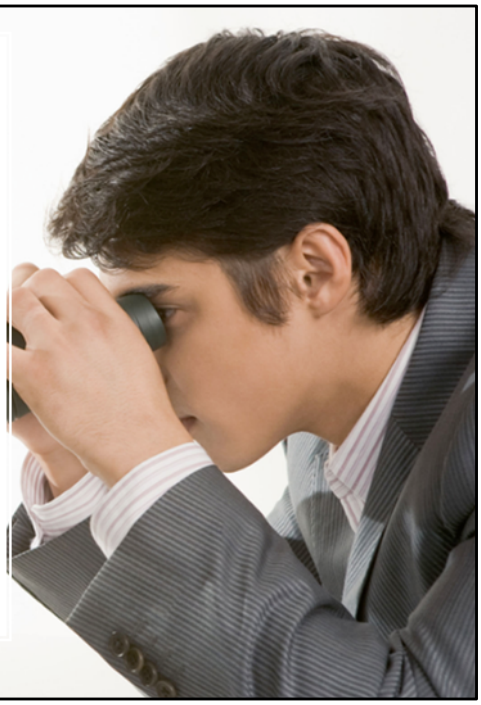

Containment

Containment
-- stop the bleeding

- Implement the incident response playbook (plan) previous rehearsed
- Prevent further damage – don't let the attacker further compromise your network
  - Segregate affected systems onto their own VLAN/Network
  - Restrict access to the systems (no external access in or out)
  - Short term vs long term containment
    - ST is the immediate containment
    - LT is to ensure the adversary cannot dig further into the network

Containment – dig deeper

- Acquire, but preserve any evidence (keep memory in tact, image disks)
  - Keep detailed notes as previously mentioned, this might become evidence in a future criminal proceeding
- Determine the source, what was exploited (vulnerability)
- Conduct damage assessment – the scope
  - What was taken (ie. Confidential data, PII, PHI, financial data, intellectual property, etc.)
  - What was changed (ie. Files, DB records)
  - What was created (ie. Backdoors, user accounts)
- Determine the type of incident and the impact it can have on the business
  - Type of attack (DoS, breach, lost equipment, etc)
  - Determine severity and criticality, this will help with the appropriate response as well as help determine what and who to communicate to (i.e. does Law Enforcement need to be brought in)



Containment – communicate the bad news

- Take copious notes
  - this will help you remember later what, who, when, why, how
  - It is amazing how different people will have different recollections of the incident, having written notes will take out a lot of the emotions later
- Need to weigh risk of continuing operations while under incident investigation
  - Senior management will have to make this decision based on your input, make sure you provide all the facts as well as realistic scenarios (based on what you know at this point in time)
- Communicate to other stakeholders
  - Management
  - Other department heads
  - Legal
  - This might include law enforcement
  - .....but limit the distribution if possible
- Work with your cloud provider if you have support
  - You do have support, right?

Containment in AWS -- first steps

- Isolate instances
  - Block access to the security groups (inbound and outbound), but leave enough access for you to investigation
  - Move instance to another security group that has very limited access (see above)
- Snapshot systems, then hash the snapshot and record the hashes in your notes
- Preserve log files (make copies and create hashes)
- Dump memory – do this before shutting down a system
  - https://www.threatresponse.cloud/
  - Margarita Shotgun to dump memory
  - This will help you preserve the current state of the machine and could help with a criminal investigation later or deeper analysis of the attack, if your team has the skills or if you have outsourced this capability to another organization

Containment in AWS -- longer term steps

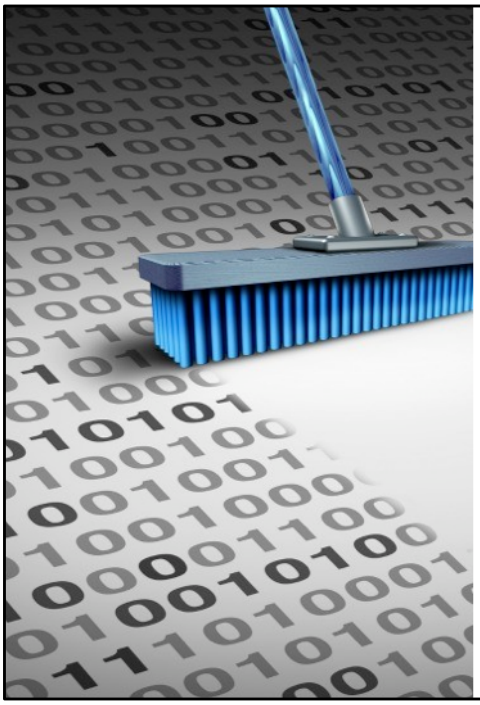
- Change passwords
- Change permissions of users, roles, groups
- Remove any suspicious and unused accounts
- Patch your systems
- Implement WAF's or other preventive or detective controls (if you don't already have them)
- Restrict inter system communication to only required ports/systems
- Shutdown any processes that should not be there
- Be sure to check startup scripts and/or registry entries for unauthorized content
- Communicate to stakeholders, but don't blame anyone (this never helps)

Containment != Eradication

- Goal here is to keep things running while stopping the attacker from causing further damage
- Collect evidence
- Learn more about the attack
  - Vector
  - Targets
  - What was taken
  - How long was the attacker there
  - Did they establish persistence?

Eradication

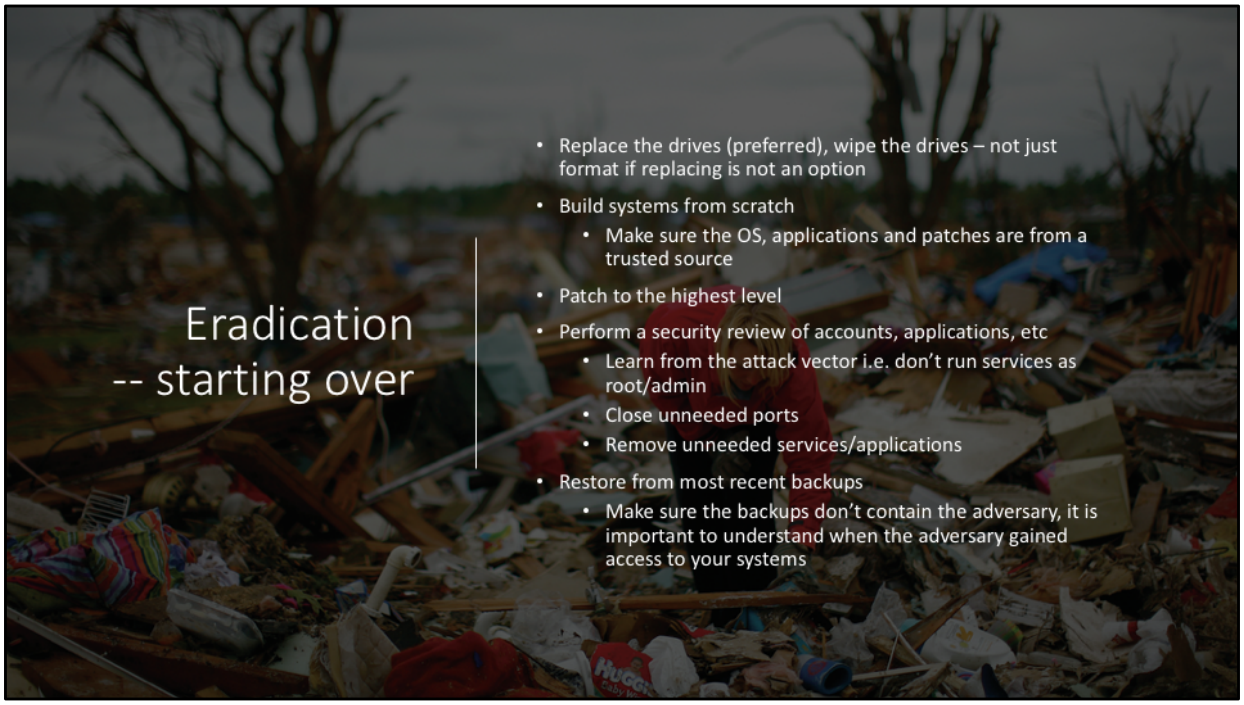

Eradication
– determine best course of action
• Before you can eradicate, you need to have a good understanding of items on the previous slide:
• Vector
• Targets
• What was taken
• How long was the attacker there
• Did they establish persistence?
• What is your confidence level of getting rid of the adversary and all his tracks, tools, persistence left behind?
• How current are your backups?
• Document everything you do and preserve evidence
• If you are going to destroy and reinstall, hash and pull the drives and save and label them properly
• If you cannot save drives, create a forensic image if you haven't already done so

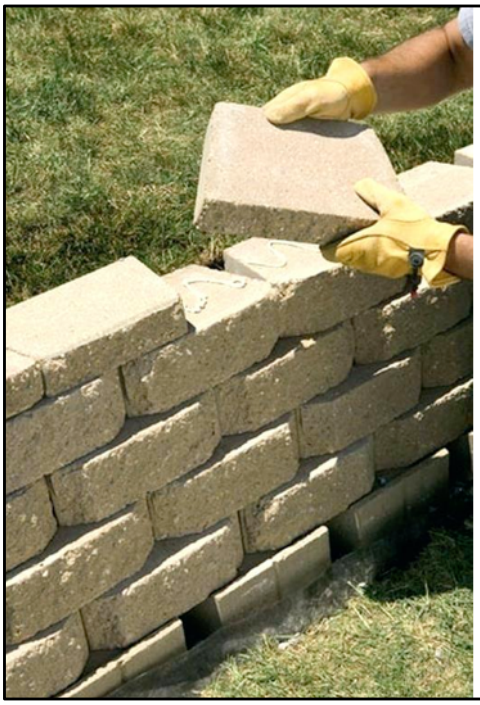


Eradication

-- remove the adversary and their tools from your systems

- Eradicate the incident
  - Remove any indications of vulnerabilities
    - Keep in mind, that good adversaries cover their tracks and know how to hide, this will not be an easy task, be diligent, patient and thorough – you might have to do this repeatedly
    - In a cloud environment, it might be better to delete the instance and start over again, if you are in an physical environment, wipe the disks, or even replace the disks (if you are worried about a root kit) and start over. (more on the next slide)
    - You will most likely find additional systems where the adversary is present, but hasn't exploited yet, follow the same containment and eradication steps
  - Put safeguards in place to prevent reoccurrence of an infection
    - Easier said than done, but you need to really have done your root cause analysis first
    - See the same suggestions as on the next slide


Eradication
-- starting over
• Replace the drives (preferred), wipe the drives – not just format if replacing is not an option
• Build systems from scratch
  • Make sure the OS, applications and patches are from a trusted source
• Patch to the highest level
• Perform a security review of accounts, applications, etc
  • Learn from the attack vector i.e. don't run services as root/admin
  • Close unneeded ports
  • Remove unneeded services/applications
• Restore from most recent backups
  • Make sure the backups don't contain the adversary, it is important to understand when the adversary gained access to your systems



Eradication – final steps

- Check the rest of your network for similar vulnerabilities, you might be surprised to find that is the not the only instance of an incident
  - Why so late in the process?
    - You have a much better understanding of the following:
      - Adversaries tools and path taken
      - IOC
      - Logs, traffic patterns, etc.
  - If you find something, you might have to expand the scope of the incident
- Communicate to stakeholders
  - They will want to have progress reports
  - Better to communicate early rather than have them hang over your shoulder

Eradication in AWS

- Can you determine the extent of the breach
  - If not, is it better to nuke and start over?
    - How much data will you lose?
    - How long will the downtime be?
  - If you decide to re-use your existing account(s), can you guarantee that the adversaries have been eradicated?
    - How do you ensure that keys are not compromised?
    - Revisit the IAM & S3 bucket permissions for all your users & files respectively, restrict the permissions as much as possible
    - Would you bet your job on it?
    - Would you bet the companies reputation on it?
    - What about your customers?

Eradication in AWS

– starting over

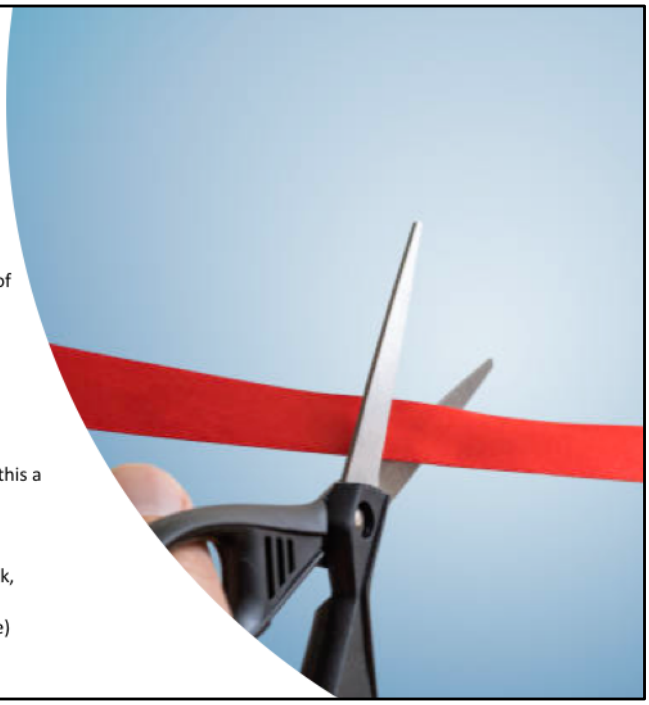
- If you have to create new accounts, do you have a credit card that can be used for billing purposes?
- You might have to re-establish VPN tunnels (back to the corporate network or other VPC's)
- Rely on your network diagrams to re-create the infrastructure, including load balancers, security groups, WAF's, VPC's, logs, etc.
  - It will be a lot of work
  - When recreating permissions, be more restrictive than before, can you limit the amount of damage an adversary can do by restricting permissions and access?


Recovery

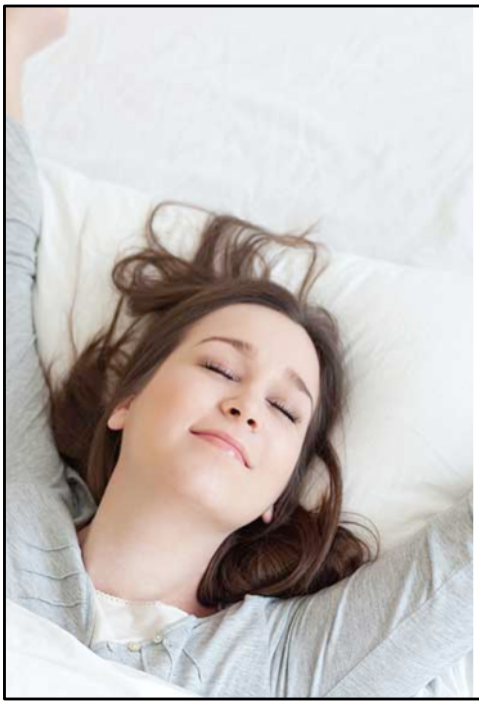
Recovery
-- Getting back to Normal

- Now that you have rebuilt or sanitized your systems, it is time to get back up and running
- Validate your systems
  - Run smoke tests
  - Regression tests
  - Integrity and Transaction tests
  - System owner signoff (they will most likely want to run their own tests)
  - Check your logs for errors and for any signs of continued infestation
- Communicate to stakeholders on the status
  - Might have to get signoff/approval to restart operations

Recovery – opening the front door, once approval has been given



- If you are going to "go live" again, try for a typical slow period of your normal transactions
  - Allows you to follow transactions and pinpoint abnormal behavior
  - Allows you to fix issues quickly
  - Limit your exposure to business logic/system errors
- Monitor the operations with a sharp eagle eye
  - Note anything that doesn't look right and determine if is this a system configuration issue or if this a sign on continued infestation
    - Are artifacts returning?
    - System performance vs. baseline (CPU, memory, disk, network I/O)
  - Turn on additional intrusion detection systems (if possible)
    - Update signatures to detect the previous attack

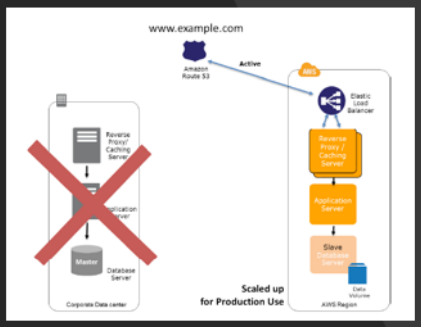


Recovery –the final steps

- Update system documentation
  - System names, users, permissions
  - Network/system diagrams
- Recreate your backups (especially if systems have been rebuilt)
- Take detailed notes as to what exactly was done
  - Will help with troubleshooting
  - Will help validate that everything was done, especially after you have finally had some sleep
- Continue to communicate to stakeholder as to the status of recovery operations

Recovery in AWS

- Many of the same steps apply such as documentation, monitoring, and communication
  - Monitors in AWS will most likely have to be recreated if you went with the starting over scenario
    - Logs and S3 buckets
    - Performance monitors
- After operations are back to normal and you have been given the all clear
  - Delete the old AWS account(s) (unless needed for evidence preservation)
    - Consult with your legal department or possibly law enforcement for criminal proceedings
    - Remove any VPN or peering connections in your other accounts that have previously connected to the now deleted account




Lessons Learned
Little C_T
Aa Bb Cc Dd Ee
Ff Gg Hh Ii Jj Kk
Ll Mm Nn Oo Pp
Qq Rr Ss Tt Uu
Vv Ww Xx Yy Zz
STAY SCHOOL
1,3,5,7,9,11,13
7x2=14
E=MC²
12 cm
12 cm
12 cm
Home Work
6+0=6
15-2=13
10x3=30

Lessons Learned
-- what went right, what didn't and how can we get better

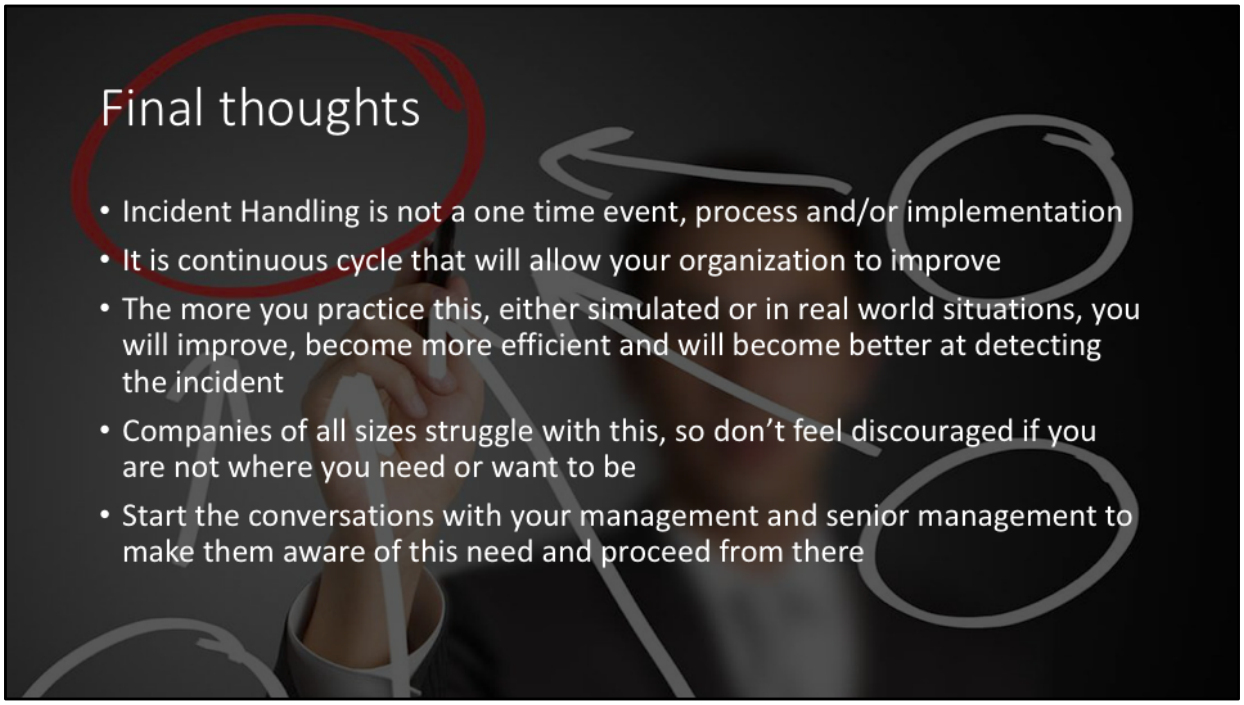
- Try to conduct the Lessons Learned (After Action) session within 7 days if possible, while everything is still fresh but allow enough time to get back to normal
- Use the previously gathered notes to ensure no detail is left out/forgotten
  - Review the timeline
  - How was the incident detected, was is done in a reasonable amount of time
  - Who did what, when, why, how
  - How effective was their action
  - What could have been done better
  - Identify gaps
- Create a detailed report with the finding, including the areas for improvement
  - Forward this report to the executive staff, follow up with a meeting
- Communicate to stakeholders
  - Are you seeing a trend here?

Lesson Learned – corrective action(s)

- After the follow-up meeting with the executive(s), create a proposal to implement the areas of improvement in the executive report
  - Provide full details such as costs and ROI
  - Time it will take to implement
  - Benefits that the investment will provide such as (if appropriate)
    - Faster detection
    - Faster recovery
    - Better trained staff
    - Etc.
- Create future goals and milestones
  - Revisit and measure how you are tracking

Post incident follow up

- Have your findings in Lessons Learned been implemented
- If not:
  - Are they on your roadmap?
  - Are they funded?
    - Tools
    - Personnel
  - Is management being held accountable to implement the findings?
- Continue to update and practice your IR plan, this is a continually improving process


Final thoughts
• Incident Handling is not a one time event, process and/or implementation
• It is continuous cycle that will allow your organization to improve
• The more you practice this, either simulated or in real world situations, you will improve, become more efficient and will become better at detecting the incident
• Companies of all sizes struggle with this, so don't feel discouraged if you are not where you need or want to be
• Start the conversations with your management and senior management to make them aware of this need and proceed from there


Survey Link
https://tinyurl.com/pdxowasp2018w4
Q&A
WHAT?
WHEN?
WHERE?
HOW?
Why?
When?
What?
Where?
WHO?

References

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://www.sans.org/reading-room/whitepapers/incident/
- https://www.cso.com.au/article/600455/six-stages-incident-response/
- https://www.sans.org/reading-room/whitepapers/incident/incident-handling-service-33289
- http://www.verizonenterprise.com/view/solnsbriefs/11411/threat-intel-and-response-services