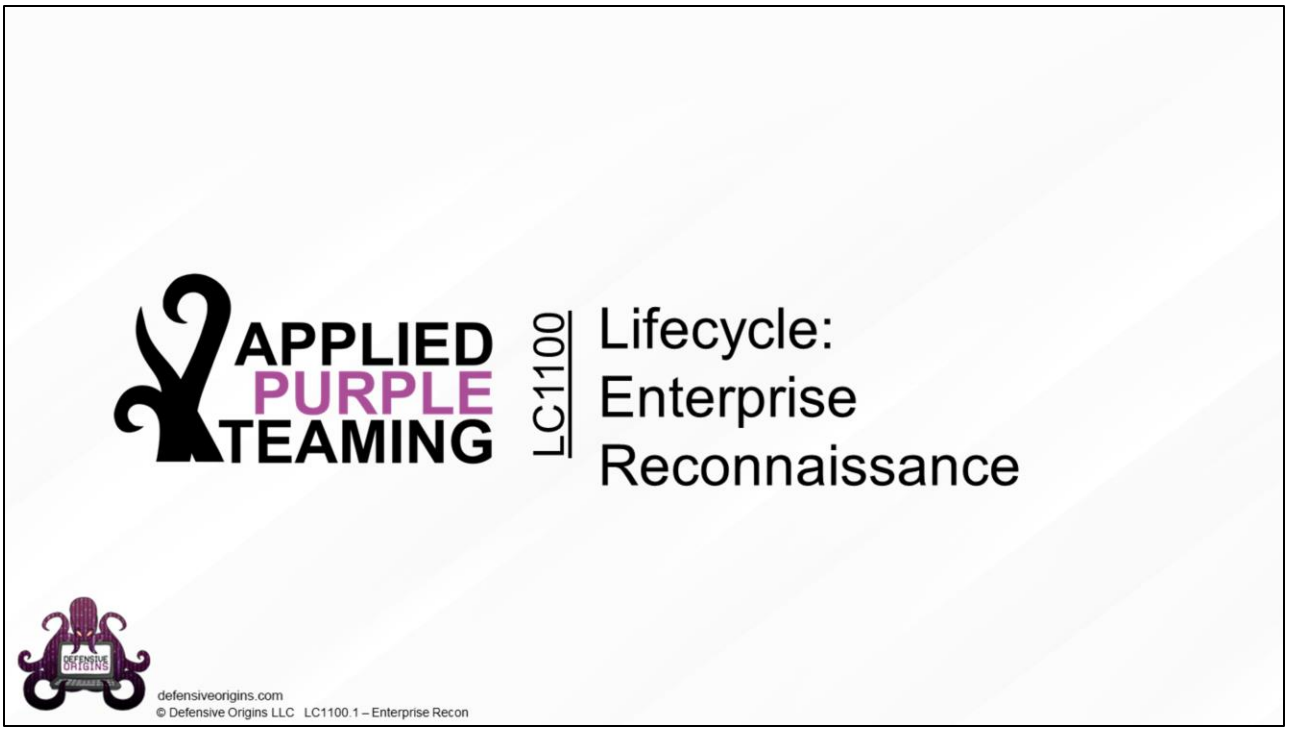
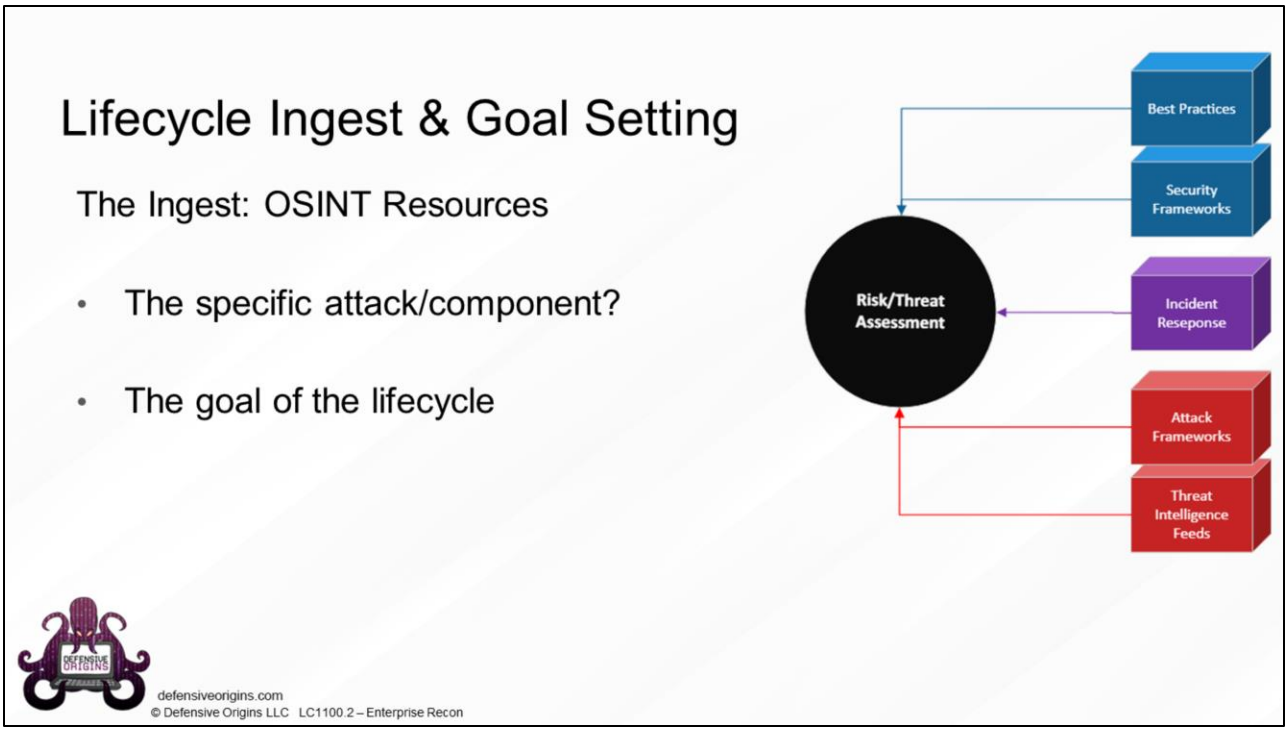


LC1100.1 – Enterprise Recon



Enterprise Recon
Atomic Purple Team Lifecycle Section:: Risk/Threat Assessment

The Ingest: OSINT Resources

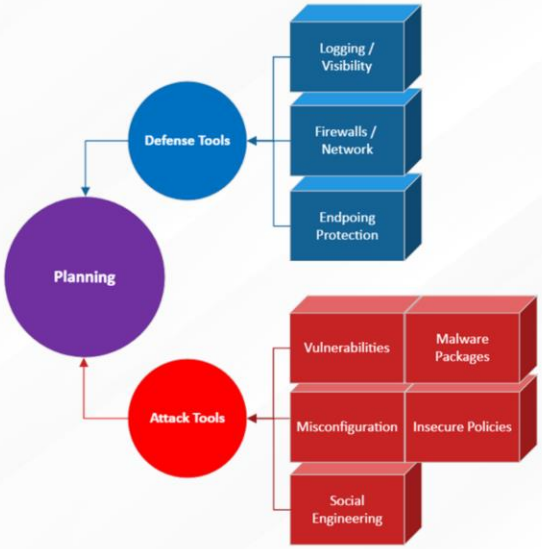
- The specific attack/component?
  - Use known OSINT techniques to find information on organization
- The goal of the lifecycle:
  - Implant tools and methods that allow the organization to understand what is available to an attacker via OSINT
  - If possible, build automation to notify of critical public disclosure

Planning – Methodology

Use OSINT Reconnaissance Tools

Plan method of OSINT Reduction

Cyber Deception



Enterprise Recon
Atomic Purple Team Lifecycle Section: Planning/Methodology

- Use OSINT Recon Tools to identify organizational OSINT
- Identify methods to reduce overall OSINT footprint
- Implement alerting of potential new disclosures

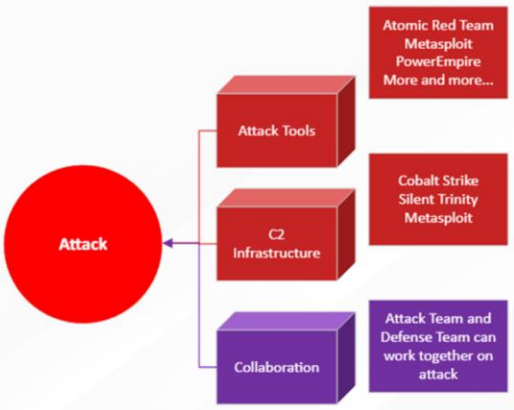
MITRE – TA0043 – Reconnaissance

Attack Methodology

Search / Pillage OSINT

Document your Research

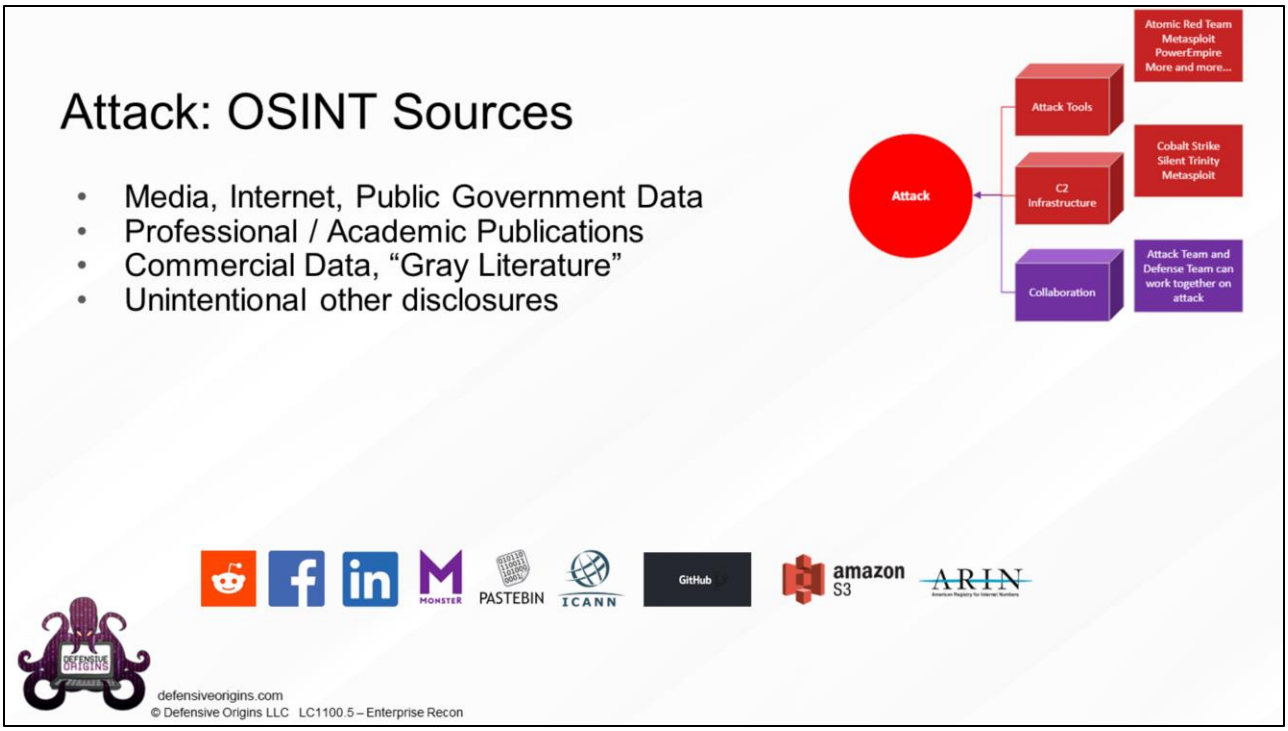
Analyze the Attack for Risk



https://attack.mitre.org/tactics/TA0043/

Enterprise Recon
Atomic Purple Team Lifecycle Section: Attack Methodology

Use OSINT Recon Tools to find information on organization
Document what information can be found
Document how the information can be used to further attack / Analyze the attack for risk



Enterprise Recon
Atomic Purple Team Lifecycle Section: Attack Methodology

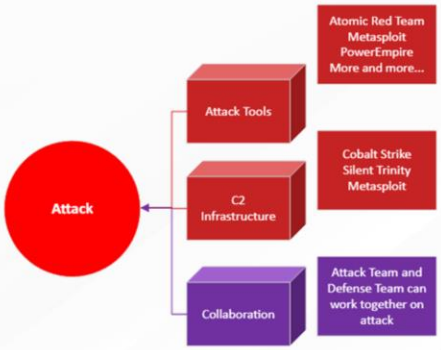
OSINT Sources:
Curated Repo: https://github.com/jivoi/awesome-osint

- Media, Internet, Public Government Data
- Professional / Academic Publications
- Commercial Data, “Gray Literature”
- Unintentional other disclosures

Attack: OSINT Sources

Many sources allow alerting platforms
Many sources have API calls that can be automated
Automate OSINT Profiles

BUT: Information can be true, or false
Deceptive OSINT: Be careful of planted Honey-Information
Re-active Recon Defense – Use Proxies



Hunt and Defend Methodology

- Build strong relationships with HR & Marketing
- Deploy tools to “see what attackers see”
- Know the OSINT landscape for the organization
- Use Deceptive techniques to lead attackers astray
- Build a platform to notify security teams of unexpected OSINT disclosures

Defense: Human Resources

Policies

- Can we really tell an employee what they can't do on their personal profile?
- Company handbook can lay some ground rules

Hiring and Job Posting Processes

- Hiring managers too often add specific technology requirements to job postings?
- Glassdoor integration

Defense: Marketing Department

<u>All Communication and PR / Brand Management!</u>

- Marketing sets the feel for the organization.
- They can manage PR and be your go to SME on social media.
- Can help coordinate reduction of OSINT related to the public website and external communication platforms.
- Teach Awareness: Does the latest media post disclose something sensitive?
  (Building access system, employee badge, etc.)

Defense: R&D Department

<u>You posted those design specs where?</u>

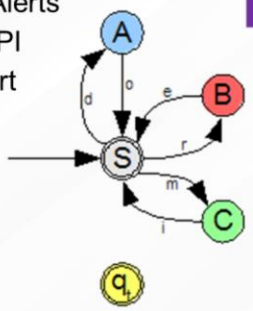
Awareness training:

- Define importance of containing all source code and proprietary IP in secure locations. Limit or prevent the use of non-restrictive or public Git or Subversion repositories.
- Good DevOps is important… But not necessarily a Security Analysts place to demand it.

Defense: OSINT Alerts and API Calls

Pastebin: Alerts and API
Google: Alerts and API
SSLMate: Alerts and API
Shodan.io: Alerts and API
HackerTarget: Alerts and API
MXToolBox: Alerts and API
URLCrazy: Python
PowerMeta: PowerShell

Monster, Glassdoor: Alerts
Been Verified: Alerts
HIBP: Alerts, API
Hunter.IO: API
AutoSPFRecon: Bind, Bash
DMARCAnalyzer: Alerts
GrayhatWarfare: API
CanaryTokens: Alert



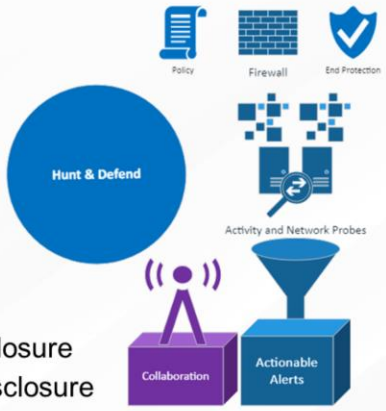
Defense: Deception Dark Arts

Know thy enemy.

- Deny-List.
- Build deception.
- Accounts
- Services
- Information

Tools

- CanaryTokens
- Honey Accounts
- DNS Honey Records
- Deceptive GitHub Disclosure
- Deceptive Pastebin Disclosure
- ADHD
- HoneyBadger



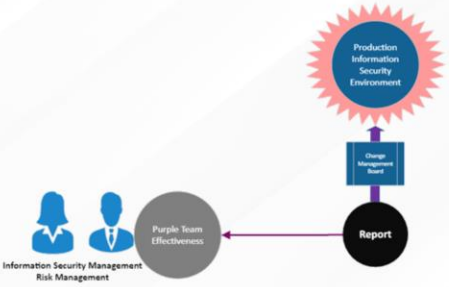
Adjust / Harden

- Identify OSINT objects that are sensitive disclosures and need removed. This may require Legal. Repeat OSINT search after removal to verify.

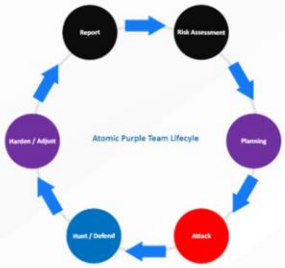
- Deploy Alerting Mechanisms
- Deploy Deception & Alerting Mechanisms
- Consider Re-Active Defense (Deny-list via Deception Trigger)
- Build Automated Persistent Recon Program

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare report for Legal if any Cease and Desist actions are warranted.
- Prepare for Change Management Controls for changes to be deployed in production.
  - Are infrastructure changes needed?
  - Will deceptive information be produced and deployed into the public domain?



Lessons Learned



- New Techniques Learned?
- Gained Experience?
- Has the organization's security posture been improved?

Enterprise Recon Summary

Attack Methodology

OSINT Sources

- Search Engine dorks
- Shodan
- Pastebin
- MXToolbox
- Hunter.io
- DNS Zone Files
- Finance and Corporate Filings
- Glassdoor
- Job postings

defensiveorigins.com

 LC1100.16 – Enterprise Recon

Detect Methodology

HIBP Domain Monitoring Alerting

`https://haveibeenpwned.com/DomainSearch`

MXToolbox Service Monitors

`https://mxtoolbox.com/services_servermonitoring2.aspx`

Pastebin Notifications

`Pastebin.com: sign up, register keywords`

MITRE ATT&CK Maps

`https://attack.mitre.org/tactics/pre/`
`https://attack.mitre.org/tactics/TA0015/`
`https://attack.mitre.org/tactics/TA0043/`
`https://attack.mitre.org/techniques/T1247/`

Defense Methodology

Policies: Corporate Email Usage

Honey Stuff:

- `canarytokens.com/generate`
- `https://github.com/adhdproject`
- `https://github.com/DefensiveOrigins/AutoSPFRecon`