RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

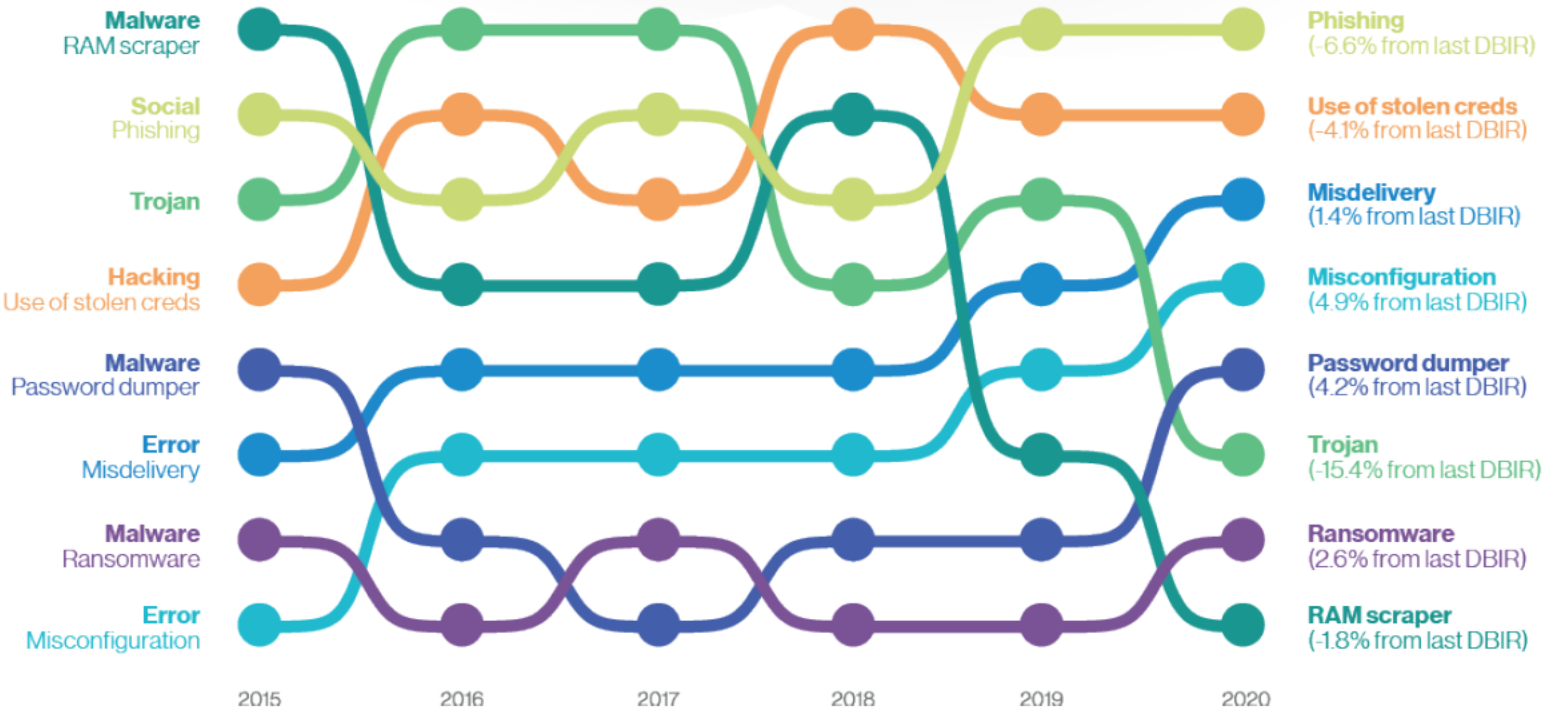
SESSION ID: **AIR-F09**

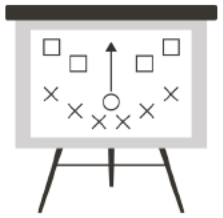
Threat Hunting - Demystified

Ashish Thapar

Managing Principal & Head - AP&J Region
Verizon Threat Research Advisory Center (VTRAC)

Threat Landscape





@_ashish_thapar_
www.linkedin.com/in/ashishthapar

Source: Verizon DBIR 2020

Threat Landscape

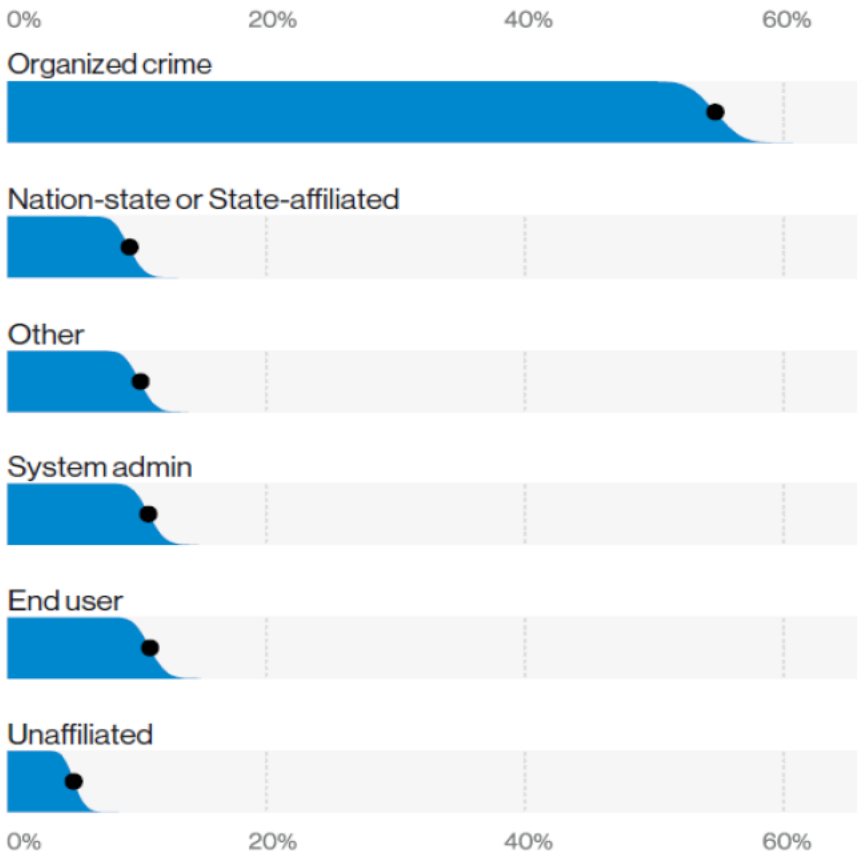


Figure 10. Top Actor varieties in breaches (n = 977)

Top Threat Action Varieties

- Social Engineering (mainly phishing, pretexting, BEC)
- Use of Stolen Credentials
- Error (Misdelivery, Misconfiguration)
- Malware

Hacking Varieties

- Use of Stolen Credentials
- Vulnerability Exploitation
- Use of backdoor or C2

Malware Varieties

- ~40% of the malware belongs to Password dumper category
- Ransomware accounts for 27% of the malware
- Malware is only seen once in ~40% of the cases

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

Source: Verizon DBIR 2020

Finding Evil - In the Sea of Noise

Item	Windows Servers	Network Routers	Firewalls	Linux/Unix Servers	IDS/IPS
Instances	50	7	2	15	2
Events Per Second (EPS)	350	7	480	45	200
Logs (GB/Day)	19.71	0.14	19.31	1.09	4.83

Total EPS - ~1000 | Total Events / Day = ~3.6 Mn

- Signal to Noise Ratio
- Blind Spots in the Asset Inventory
- BYOD / Shadow IT
- Insider Threats
- Third parties galore
- IoT/OT
- The Cloud syndrome
- 0-day vulnerabilities
- IoC Shelf Life

Source: https://www.mixcloud.com/

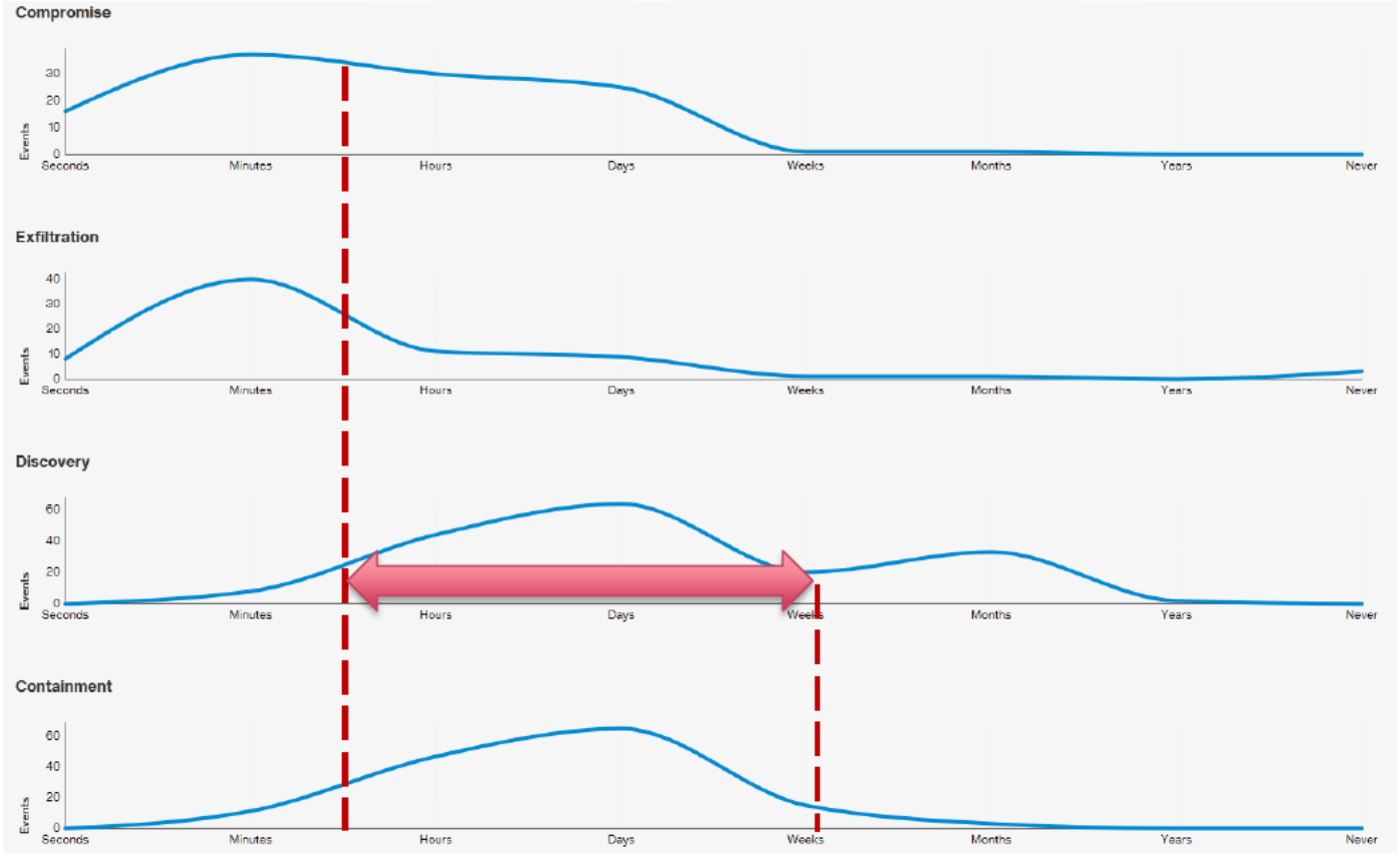
@_ashish_thapar_

www.linkedin.com/in/ashishthapar

The Detection Gap

- Time to Compromise Vs Time to Discover
- More than half of the breaches are discovered by external security researchers
- Discovery in Months or more still accounts for over a quarter of breaches

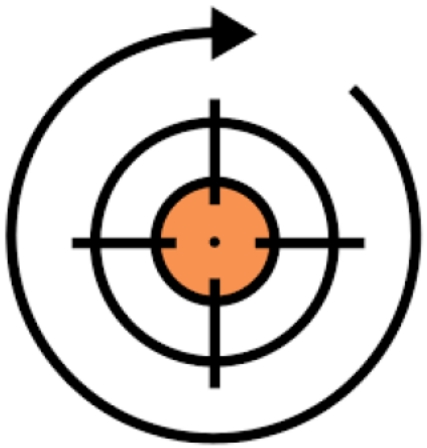
Effective and Efficient *Threat Hunting* can help shorten this gap.



@_ashish_thapar_
www.linkedin.com/in/ashishthapar

Source: Verizon DBIR 2020

Demystifying Threat Hunting



Source: armor.com

What is Threat Hunting:

- ✓ Hypothesis-driven exercise
- ✓ Proactively searching for the threats
- ✓ Helps reducing false negatives / shades of grey
- ✓ Assuming that adversaries are already present in the infrastructure
- ✓ Laying strong focus on IoAs along with IoCs
- ✓ Prioritizing threats

Myth Busters:

- x Meant to replace preventive controls or signature based detection
- x It is a Panacea
- x Expensive… Its benefits outweigh the costs
- x = Shiny tools such as UEBA / NDR / EDR / SOAR

@_ashish_thapar_

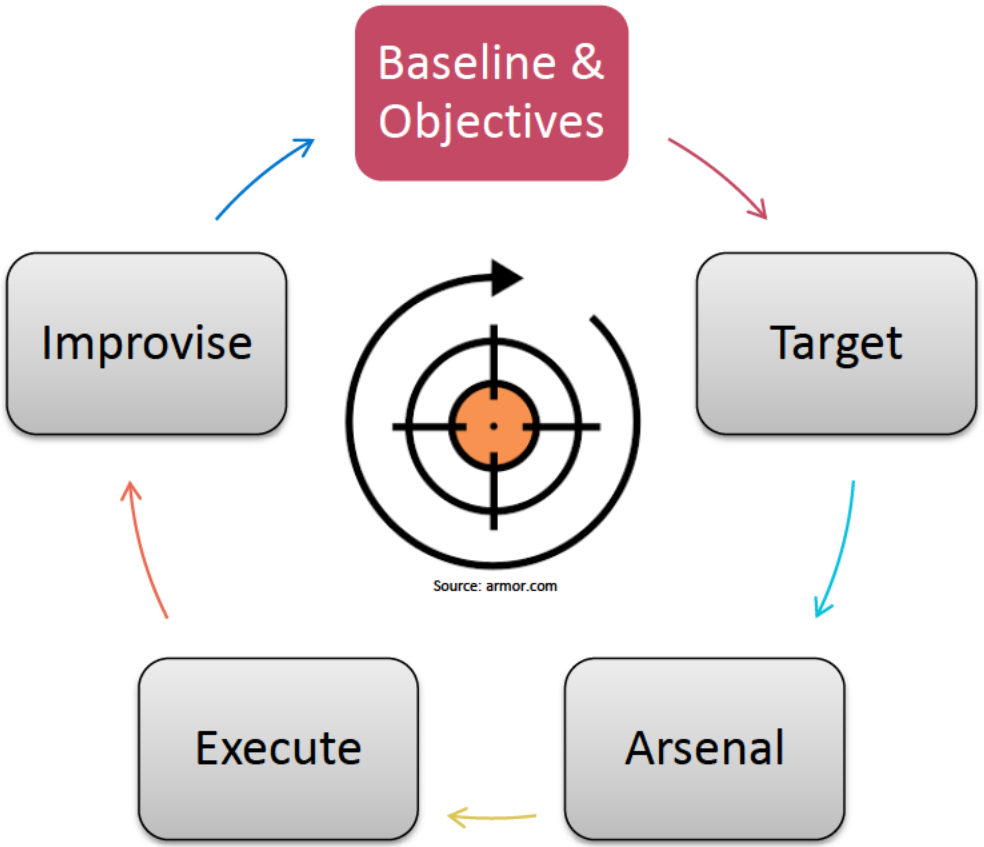
www.linkedin.com/in/ashishthapar

Threat Hunting Model – The Fabulous Five

- Knowing your ground
- Knowing your adversary
- Repeatable approach
- Recurring activities
- Efficient resourcing
- Effective execution

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

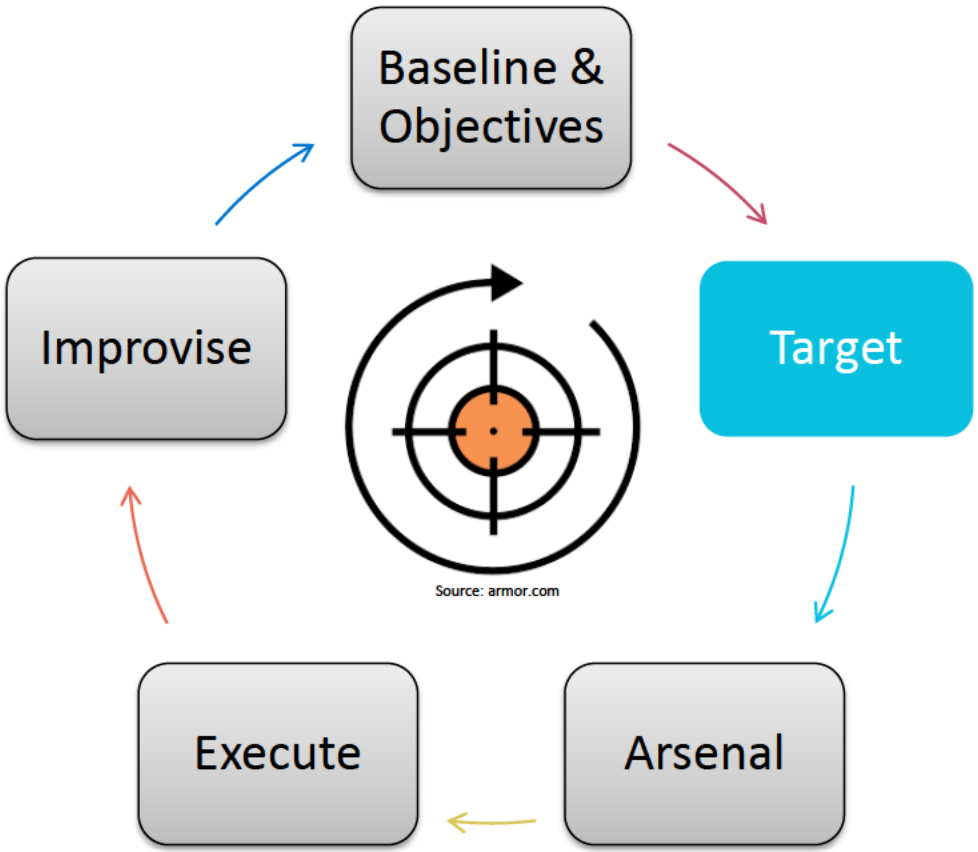
Threat Hunting Model – Phase 1



- Establish a program
- Obtain sponsorship
- Refer a framework
  - e.g. MITRE ATT&CK, Cyber Kill Chain, Diamond
- Define maturity levels
- Get the right personnel with right skills/attitude
- Allocate roles and responsibilities

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

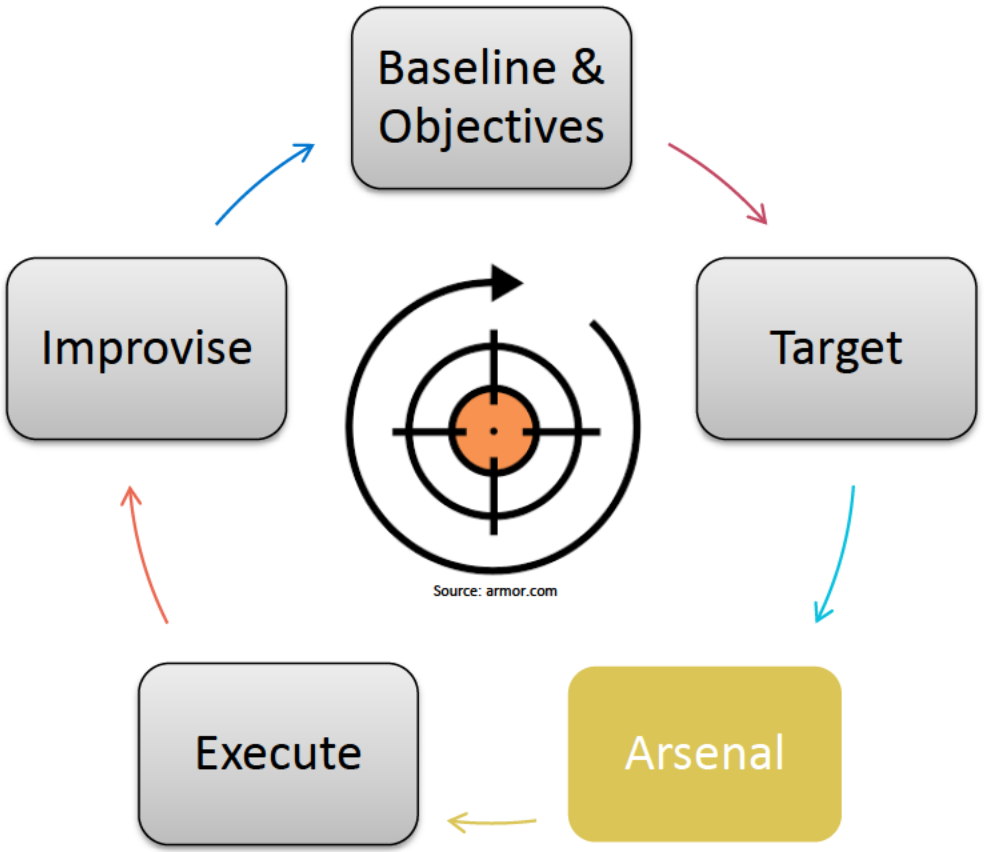
Threat Hunting Model – Phase 2



- Finalize data sources:
  - Network (Netflow, Proxy, DNS, Firewall, FPC etc.)
  - End-points (Logs, MACB, Memory, System artifacts)
  - Cloud based platforms
  - Threat Intel
  - Observables
- Decrease visibility gap
- Review verbosity
- Collect, enrich, normalize
- Leverage automation

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

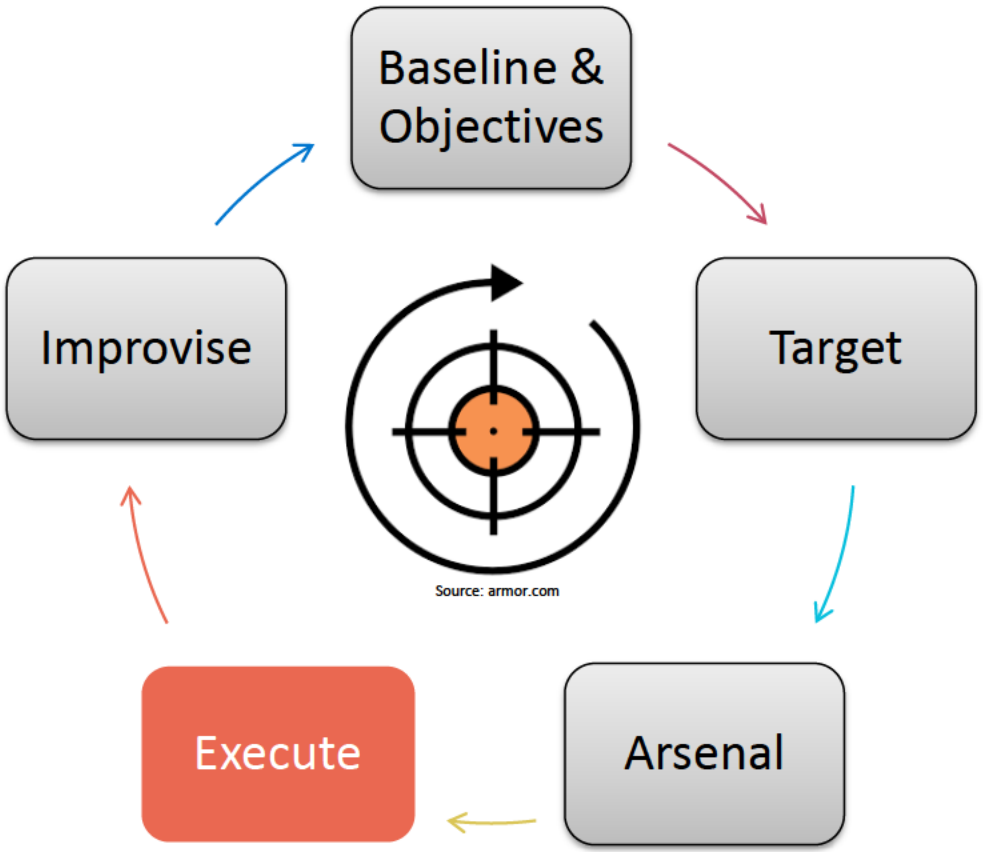
Threat Hunting Model – Phase 3



- SIEM/SOAR
- EDR (Don't forget Sysmon)
- NDR
- AV/EPP
- Geo-Location / Whois
- NSRL Database
- Sandbox environment
- Threat Intel Platform
- TTPs/Playbooks/KBs
- Log Management Platform / Data Lake
- Develop automation & visualization
- Platforms like HELK (The **H**unting **ELK**)

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

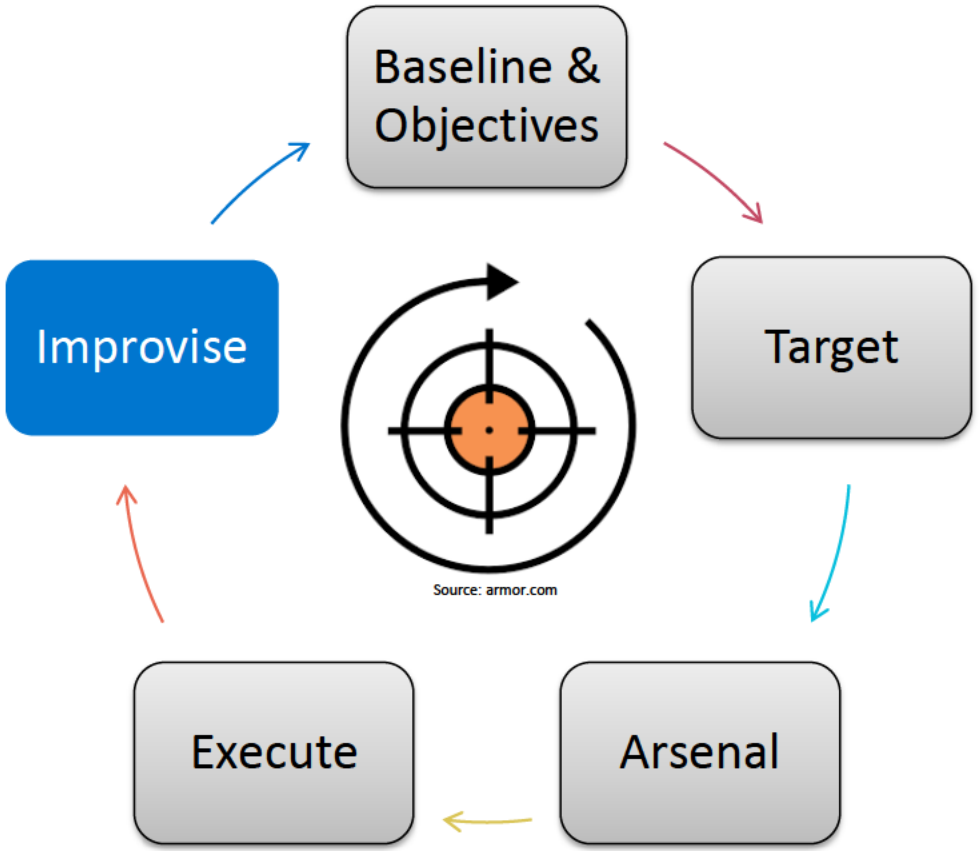
Threat Hunting Model – Phase 4



- Start small
- Focus on crown jewels
- Form a hypothesis
  - 5Ws and 1H (Use cases)
- Hunting Techniques: *Searching, Clustering, Grouping, Frequency Analysis (*Aberrations/Anomalies)
- Be aware of the data/cognitive biases
- Decide hunt frequency
- Leverage automation and visualization
- Bring new perspectives (e.g. from SECOPS team)

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

Threat Hunting Model – Phase 5



- Refine Metrics
- Gauge/Review hunting maturity levels
- Maintain statistics and compare trends
- Identify visibility gaps and remove biases
- Enhance automation
- Feedback for improving the hunting model

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

Sample Use Case: Hunting for C2

- **Baseline & Objectives:** Start with using MITRE ATT&CK framework and with defined hunting team
- **Target: Data sources:** Proxy logs, DNS logs, SMTP logs, NetFlow
- **Arsenal:** SIEM dashboard, EDR console, Joe's Sandbox, GCHQ CyberChef
- **Execute:** C2 channels protocol/port analysis. Example: C2 in Web traffic
  - Make a hypothesis: Attackers operating over a C2 channel that uses custom encryption (uncommon protocol) on TCP-80 port
  - Search for anomalous domains, user-agent strings or URLs
  - Look for odd protocol usage (HTTP connection on port 80 with no/unusual metadata)
  - Frequency analysis/stacking on DNS queries or HTTP GET/POST submissions to websites
  - Check network accounting information (bytes-in, bytes-out, session time)
  - Indicator search – leverage Threat intelligence along with observables
  - Establish 'known good' and 'known bad' examples to build a training dataset for ML based automation
  - Malware analysis of the suspected process that initiates the C2 connection/beacon
- **Improvise:** Identify visibility gaps, build automation models, measure time taken

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

Ten Commandments for Effective Threat Hunting

- *Different organizations face different threats with varied infrastructure and frameworks in use.*
- *Exercise caution when designing your own Threat Hunting program.*

1. Gauge your cyber maturity level
2. Allocate rightly skilled and enough resources
3. Know your ground
   - Asset management (don't forget the software, OT/IoT & cloud assets)
   - Vulnerability management (whitebox, blackbox and greybox)
   - Risk register (focus on crown jewels)
4. Mind the insider threat
5. Ensure network visibility and uncover blind spots
6. Know your adversary
   - Threat intelligence and darkweb
   - TTPs of the threat actors, motivations
7. Leverage a robust framework (e.g. MITRE ATT&CK Navigator)
8. Use automation/machine learning tools as much as possible
9. Define metrics for the threat hunting program
10. Integrate robustly with other threat detection strategies/teams/IR

@_ashish_thapar_

www.linkedin.com/in/ashishthapar

Failing to plan is planning to fail

- Next week you should:
  - Understand and gauge the maturity of your organization w.r.t threat hunting
- In the first 3 months following this presentation you should:
  - Recognize the critical assets, processes and systems of your organization
  - Understand the organization risk profile, threats and typical TTPs
  - Start gathering information from OSINT and other commercial sources on threat intel relevant to your industry and region
- Within 6 months, you should:
  - Implement automation solutions to increase your visibility in the digital ecosystem of the organization
  - Establish a telemetry baseline and build your arsenal for doing threat hunting
  - Define metrics and start measuring your performance/outcomes
  - Run *sprints* and eventually move towards running periodic/defined hunting *campaigns*

@_ashish_thapar_
www.linkedin.com/in/ashishthapar

RSAConference2020 APJ

A Virtual Learning Experience

Thank you!

Questions?

@_ashish_thapar_

www.linkedin.com/in/ashishthapar