Cyber Hygiene Hunting

~ Security Effectiveness Validation for valid security posture ~

Tomohisa Ishikawa, Ph.D., CISSP, CSSLP, CISA, CISM, CFE, PMP

Lead Cyber Security Architect

Tokio Marine Holdings Inc. / TMHD-CSIRT

$whoami : Tomo (Tomohisa Ishikawa)

- ***Lead Cyber Security Architect, Tokio Marine Holdings / TMHD-CSIRT***
  - Dev/Plan : Global Cyber Security Strategy, Security Architecture, Research
  - Ops : CSIRT Ops (Red team, Incident handing, Threat Intel, DFIR etc.)
- ***14+ years experience in Offensive and Defensive Security domain***
- ***Certification Junkie :***
  - Ph.D, CISSP, CSSLP, CISA, CISM, CDPSE, CPE, PMP, AWS Security, GIAC…
- ***External Activity***
  - Speaker : SANFIRE2011, DEFCON24 SE Village, LASCON 2016, BSide Philly 2016 etc.
  - Translator : published 5 translated cyber security books from O'Reilly Japan
  - Author : "Cyber Threat Intelligence" (Japanese)
  - Committee Member : National Exam (JITEE) Committee Member in Japan

Agenda

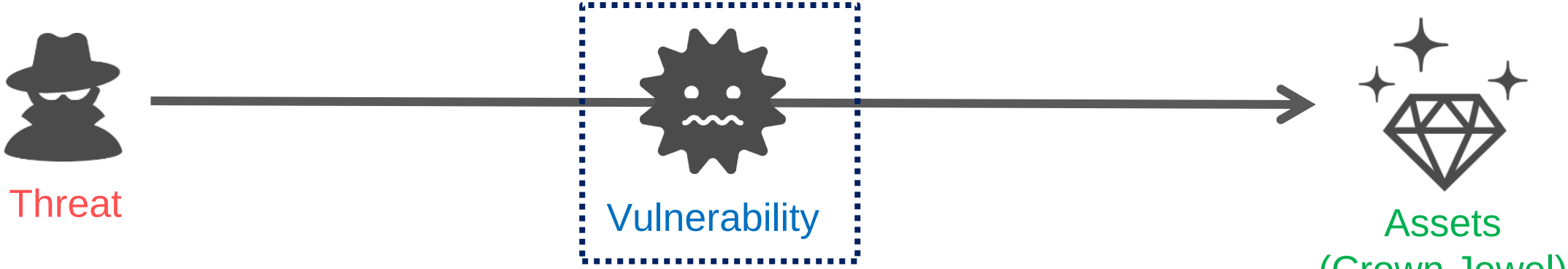
- ***Today's Topic : Cyber Hygiene Hunting***
  - *Basic Concept – Applying proactive approach (threat hunting) to cyber hygiene domain*

- ***Part I: Theory (What?)***
  - CHH theory (including definition, background, concept, and approach etc.)
- ***Part II: Operation and Practice (How?)***
  - Scope and Methods to operationalize Cyber Hygiene Hunting
- ***Part III: Case Study***
  - Actual example and specific example for cyber hygiene hunting

Part I : Theory

Security Management Goal

- Goal = Reduce Security Risks
- Risk = Threat x Vulnerability x Asset



Reduce “Vulnerability” = Cyber Hygiene

Cyber Hygiene Hunting

To proactively and iteratively verify the status of cyber hygiene and security posture that will cause future intrusion

Why “Cyber Hygiene Hunting” is key?

- *Background Story : Tokio Marine Group*
  - Business : Insurance（A lot of PII/PHI, Seller of Cyber Insurance）
  - Operation : 46 countries and regions worldwide (expanded by M&A)
  - Governance : *“federal” governance model*
    → Each GC (group company) has their own security program

- *As HD perspective:*
  - Need to have method to validate that each GC’s security program correctly works
    → *Necessity of Cyber Hygiene Hunting*

- *Cyber Hygiene Hunting should “Be Adaptive”*

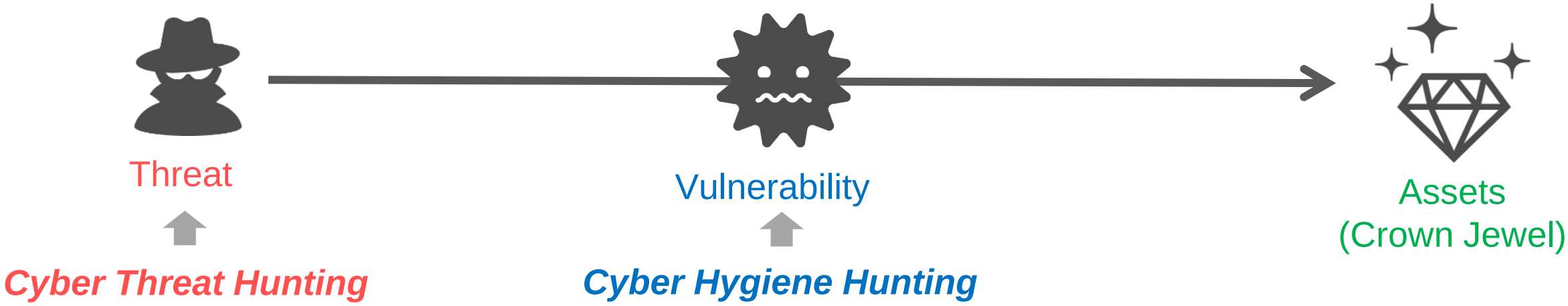
"Be Adaptive" Strategy

- ***"Be Adaptive"* : Be flexible and proactive in Cyber Risk Mgt**
  - Defense Models will be outdated quickly since:
    - Threat trends and landscape are changing
    - Evasion techniques will be sophisticated

- To "*be adaptive*", CHH will satisfy following three principles.
  - **Principle 1 : Proactive Approach on each "Risk" Element**
    - Threat Hunting + **Cyber Hygiene Hunting**
  - **Principle 2 : Continuous Approach**
    - CM / CI (Continuous Monitoring + Continuous Integration)
  - **Principle 3 : Evidenced Based Approach by Tools**
    - Leverage Tools for visualizing security posture

Principle 1 : Proactive Approach on “Risk”

- To “be adaptive”, we proactively identify “risk” component by using hunting approach
  - Technique 1 : Cyber Threat Hunting
  - Technique 2 : Cyber Hygiene Hunting



Principle 1 : Proactive Approach on “Risk”

- Comparison between two technique as follows.

＜Techniques to Achieving Adaptive Security>

	Technique 1 : Cyber Threat Hunting	×	***Technique 2 : Cyber Hygiene Hunting***
Definition.	*“To proactively and iteratively discover current or historical threats that evade existing security mechanisms, and to use that information to improve cyber resilience”* (SecureWorks Definition)		*To proactively and iteratively verify the status of cyber hygiene and security posture that will cause future intrusion, and to use that information to improve cyber resilience*
Target	Threat		Vulnerability
Viewpoint	Past & Present		Future
Outcome	IoC (=Indicator of Compromise)		EoC (=Enabler of Compromise)

Source : https://www.secureworks.com/centers/what-is-threat-hunting

Today’s Focus

Caveat : CHH ≠ VAPT, Red Teaming…

- *CHH = Continuous Evidence-Based Approach by Enabler of Compromise*
  - Example of Scope :
    - Vulnerability Management, Account Management, Attack Detection Capability

- *CHH ≠ VAPT, Red Teaming…*
  - VAPT(vulnerability assessment and penetration test), red teaming are also the part of Cyber Hygiene Hunting
  - *VAPT might be "snap-shot" approach and it is not match to continuous inprovement*
  - *Cyber Hygiene Hunting is much wider concept*

Principle 2 : Continuous Approach

- To “be adaptive”, we proactively identify “risk” elements by continuous approach
  - **CM/CI（Continuous Monitoring & Continuous Improvement）**

<Continuous Approach : CM/CI>

CM

Continuous Monitoring

Continuously validate and monitor the status of cyber hygiene.

×

CI

Continuous Improvement

Iterative improvement based on continuous monitoring results.

Principle 3 : Evidence based Approach

"Data! Data! Data!.. I can't make bricks without clay!"

Sherlock Holmes, The Adventure of the Copper Beeches

Use Tools for evidence-based approach

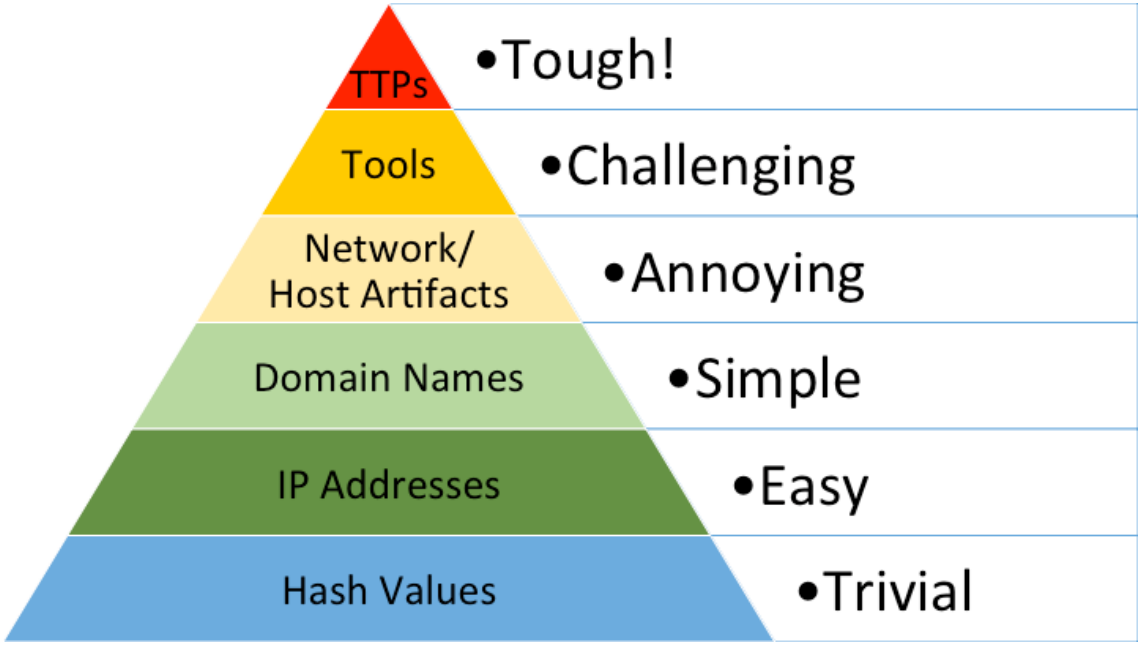
Approach	Original Challenge	Advantage of New Approach
Actual Validation (Stop to use Check-List)	• Check-List may not identify operational errors, unclear scope of R&R, different recognition btw stakeholders (i.e. discussion w/ GCs) • Difficult to set up tangible goal	• Reveal actual operational error • easily set-up clear goal
Real Time Visualization	• Snapshot approach (i.e. VAPT) is NOT workable to identify current security risks	• Realize CM/CI by using tools

Part II : Operation and Practice

Operationalize Cyber Hygiene Hunting

- Scope and validation method is Key (What kind of EOC is in the scope?)
- Applying IOC "Pyramid of Pain" concept to Cyber Hygiene Hunting (EOC)

- "Pyramid of Pain"
  - Created by David Bianco
  - Relationship between IOC types and how much pain it will cause them



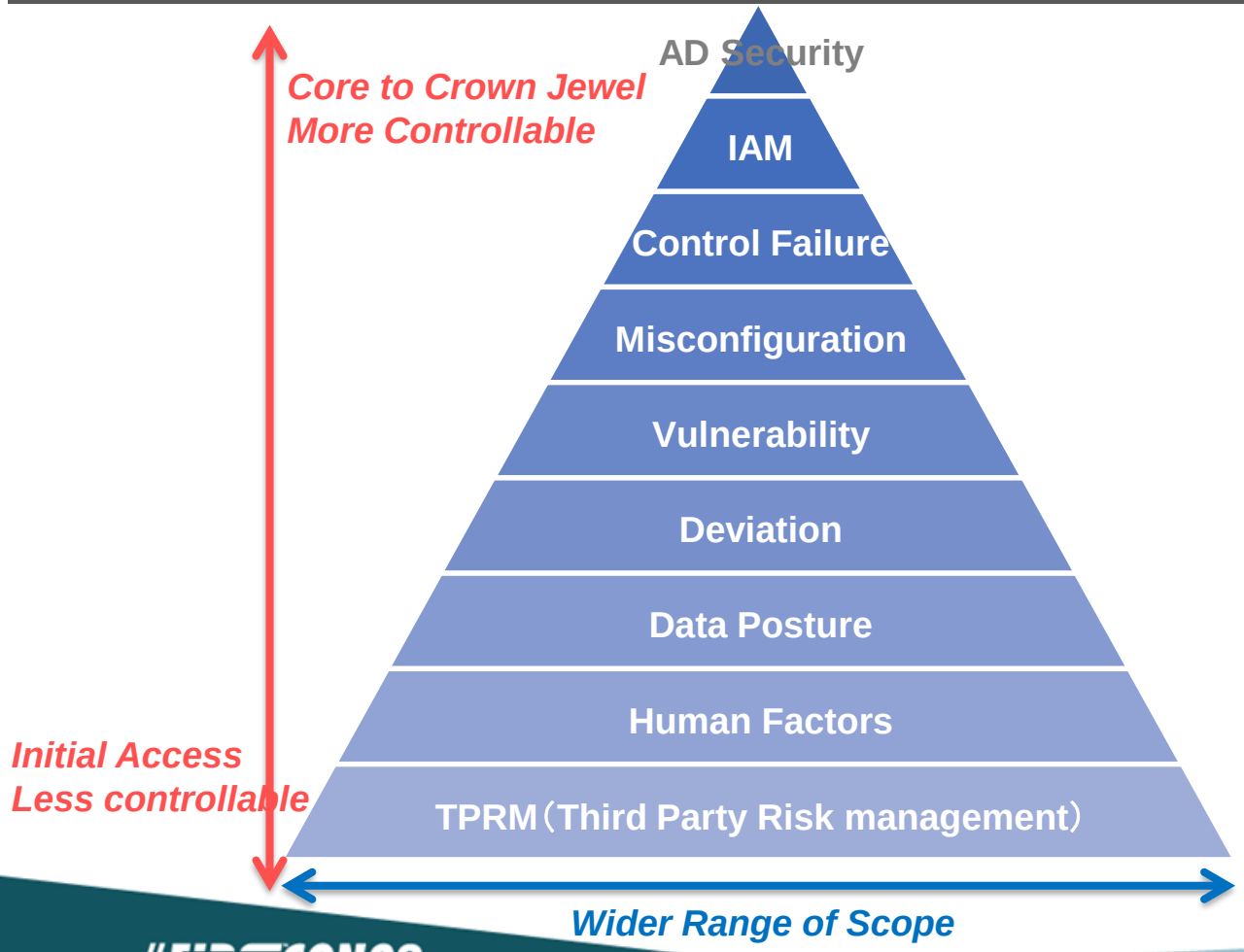
Source : http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Scope of Cyber Hygiene Hunting

Tentative

"Pyramid of Gain for Cyber Hygiene Hunting"

Pyramid of Gain for Cyber Hygiene Hunting



Category	Methods
Active Directory Security → Identify misconfiguration of AD/AAD	AD Audit Tool
Account Hygiene → Use of compromised password strings and improper AuthZ	AD Audit Tool
Security Control Capability → Known attack methods cannot be prevented or detected.	BAS・Red Team
Misconfiguration： → Unnecessary port, Open S3 backet, VPN MFA	Vulnerability Scan SSPM・CNAPP
Failure of Vulnerability Management → Existence of vulnerability	Vulnerability Scan
Non-standard device / service / software： → Shadow IT, unsupported software	Asset Mgt Tools Scanning
Data Posture Management → Data management (improper MGT of PII/PHI)	AWS Macie
Security Awareness Status: → Security Education, Phishing Mail Exercise	Phishing Mail Ex.
Third Party Risk Management： → Continuous check for TPRM	SRS

Part III : Case Study

Case Study:

- We will have various examples for Cyber Hygiene Hunting.

- Case #1: Active Directory Security
- Case #2: Security Control Validation
- Case #3: Compromise Assessment
- Case #4: Result Exploitation

Case #1: Active Directory Security

- Active Directory and Domain Account is a very commonly targeted and proper management is very important.
  - Attack Vector: Golden Ticket, Silver Ticket, Kerberoasting, AS-REP Roasting, DCSync…
  - Vulnerability: Zerologon (CVE-2020-1472), CVE-2021-42287/CVE-2021-42278

- Gartner 2022 Trends : ITDR (Identity Threat Detection and Response)
  - Identity system defense with ITDR is 2022 cyber trends since the abuse of credential is typical attack vectors

Source : https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

Case #1: Active Directory Security

- Commercial Tools
  - Attivo Network AD Assessor https://www.attivonetworks.com/product/adassessor/
  - Bloodhound Enterprise https://bloodhoundenterprise.io/
  - Tenable.ad https://www.tenable.com/products/tenable-ad
  - PingCastle https://www.pingcastle.com/
  - CrowdStrike Falcon ITP/ITD https://www.crowdstrike.jp/products/identity-protection/

- Open/Free Tools
  - AD Audit by @phillips321 https://github.com/phillips321/adaudit
  - Bloodhound https://github.com/BloodHoundAD/BloodHound
  - Active Directory Security Assessment
    - https://4sysops.com/archives/perform-active-directory-security-assessment-using-powershell/

test.mysmartlogon.com - Healthcheck analysis

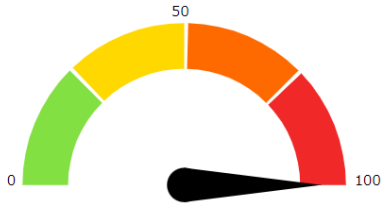
Date: 2022-01-02 - Engine version: 2.10.1.0 Beta

This report has been generated with the Auditor Edition of PingCastle (?).

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 100 / 100

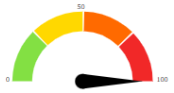
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statictics

Privacy notice

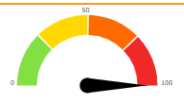
Stale Object : 100 /100 — 14 rules matched

It is about operations related to user or computer objects



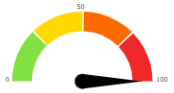
Privileged Accounts : 100 /100 — 20 rules matched

It is about administrators of the Active Directory



Trusts : 100 /100 — 4 rules matched

It is about links between two Active Directories



Anomalies : 100 /100 — 31 rules matched

It is about specific security control points

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

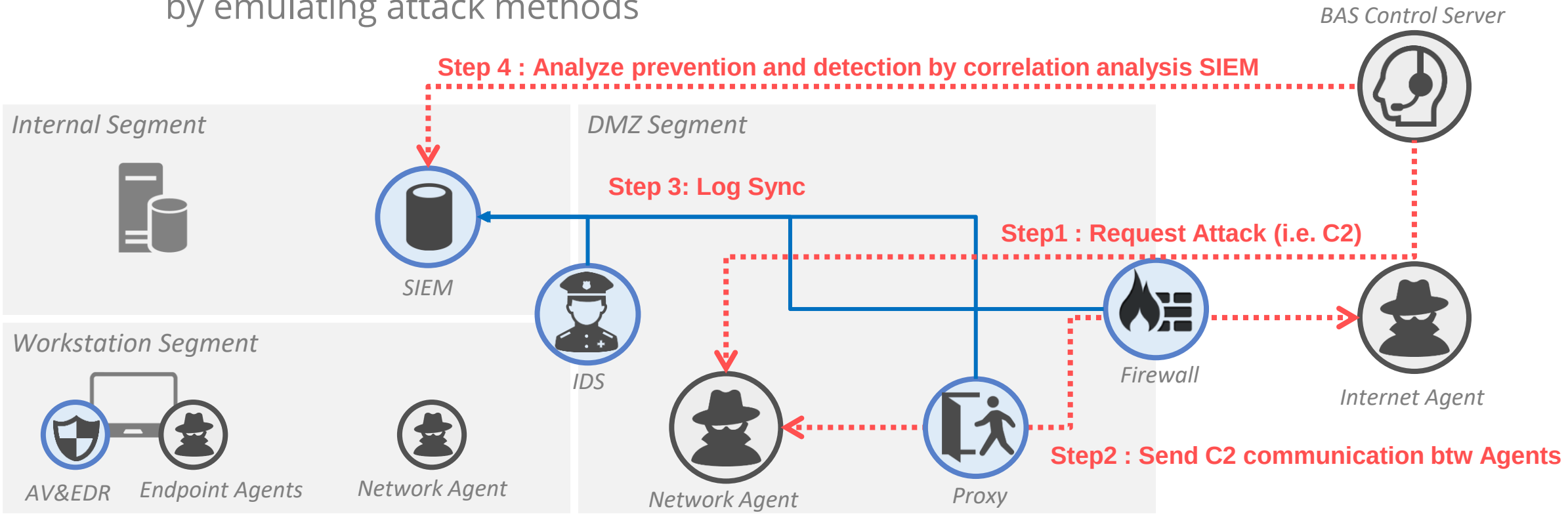
https://www.pingcastle.com/PingCastleFiles/ad_hc_test.mysmartlogon.com.html

Privileged Accounts rule details [20 rules matched on a total of 42]

Number of privileges granted by GPO to any user: 4	+ 60 Point(s)
Number of GPO items that can be modified by any user: 3	+ 45 Point(s)
Anyone can interactively or remotely login to a DC	+ 45 Point(s)
Number of login scripts that can be modified by any user: 2	+ 30 Point(s)
Number of DC with a contrained delegation: 1	+ 25 Point(s)
Everyone can take control of a key domain object by abusing targeted permissions.	+ 25 Point(s)
Presence of Admin accounts which do not have the flag "this account is sensitive and cannot be delegated": 8	+ 20 Point(s)
At least one GPO is deploying a file which can be modified by everyone	+ 15 Point(s)
Presence of delegation where anybody can act: 1	+ 15 Point(s)
Presence of unknown account in delegation: 1	+ 15 Point(s)
At least one GPO grant the right to get in the recovery mode without being admin	+ 15 Point(s)
At least one member of an admin group is vulnerable to the kerberoast attack.	+ 15 Point(s)
1 domain controller(s) have been found where the owner is not the Domain Admins group or the Enterprise Admins group	+ 10 Point(s)
Number of admin with a password older than 3 years: 4	+ 10 Point(s)
The group Schema Admins is not empty: 2 account(s)	+ 10 Point(s)
The Denied RODC Password Replication Group group has some of its default members missing	+ 5 Point(s)
The Allowed RODC Password Replication Group group is not empty	+ 5 Point(s)
Number of members of the Dns Admins group: 1	+ 5 Point(s)

Case #2: Security Control Validation

- BAS (Breach & Attack Simulation)
  - A tool to verify the effectiveness of security controls and understand security posture by emulating attack methods



Case #2: Security Control Validation

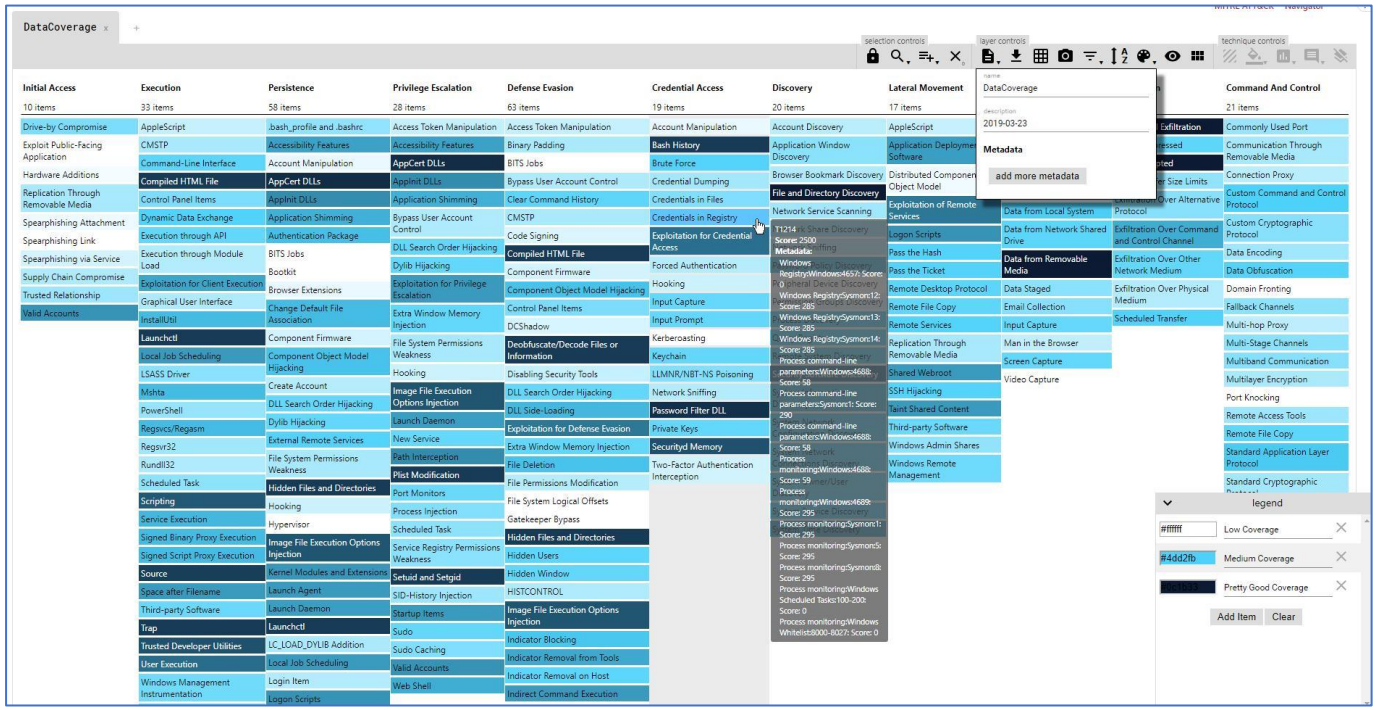
- Commercial Tools
  - XMCyber https://www.xmcyber.com/
  - Safebreach https://www.safebreach.com/
  - AttackIQ https://www.attackiq.com/
  - Cymulate https://cymulate.com/
  - Mandiant Security Validation https://www.mandiant.com/advantage/security-validation

- Open/Free Tools
  - Red Canary Atomic Red Team https://atomicredteam.io/
  - MITRE Caldera https://caldera.mitre.org/
  - Active Countermeasure - Threat Simulator
    - https://www.activecountermeasures.com/free-tools/threat-simulator/

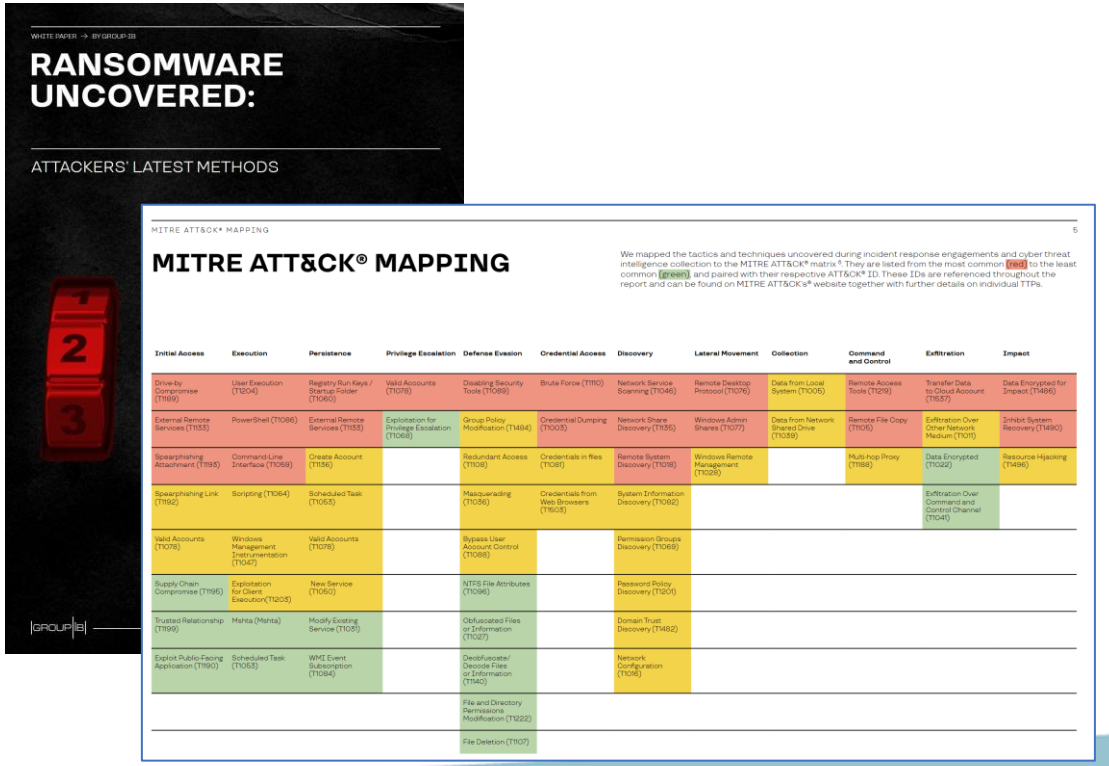
Case #2: Security Control Validation

- **Visualization with MITRE ATT&CK as Common Language**
  - We map Prevention/Detection results with MITRE ATT&CK, and we will visualize the current posture
  - We can easily compare/leverage external reports/data by using standard framework.

<Prevention and Detection Capability Visualization with MITRE ATT&CK>



<Group IB: Ransomware Whitepaper>



Case #3: Compromise Assessment

- Compromise Assessment is intensive analysis of discovering IOC/EOC via security telemetry.
  - Applying fast forensics, PowerShell, log analysis….

Case #3: Compromise Assessment

< Generalized CA Results – data is dummy ☺ >

	Category	# of Issues	Issue Details	
	Scope of Device	**2,500**	-	
IOC	Indicator of APT attack	1	• Mimikatz with evasion is located C:¥tools¥	Start Investigation
IOC	Commodity Malware	156	• Spyware, Adware …	Start Investigation
IOC	Risky Activity	298	• Unusual communication to Country X server	Start Investigation
EOC	Admin Tools	1,490	• PSExec is installed in X% of devices	Continuous Improvement
EOC	Potentially Unwanted Program	549	• Non-standardized VPN (8 types software in 321 devices)	Continuous Improvement
EOC	Vulnerability	535,298	• Averagely, 214 vulnerabilities per devices	Continuous Improvement
EOC	Account / Password	1,071	• 32% of users has Domain Admin Privilege • 276 device has plaintext password (password.txt) • 24% user use potentially compromised password	Continuous Improvement

- **Continuous Improvement:**
  - Technical improvement in short term, Process improvement in long term
  - Use quantitative data as KPI for continuous management

Case #3: Compromise Assessment

- Commercial Services
  - Many vendors has similar services
- Open/Free Tools : Many tools are available
  - Utilize PowerShell or fast forensic tools
    - Velociraptor https://docs.velociraptor.app/
    - Sysmon Search https://github.com/JPCERTCC/SysmonSearch
  - Threat Hunting tools
    - Hayabusa Windows Event Log Fast Forensic Tools
      - https://github.com/Yamato-Security/hayabusa

Case #4: Result Exploitation

- Use KPI/KRI for Senior Leadership
  - # of EOC (Enabler of Compromise) will be good source of KPI/KRI for senior leadership
- Use Cyber Hygiene Hunting for Security Due Diligence
  - IT DD / Security DD is emergingly critical in M&A process


#FIRSTCON23
35TH
ANNUAL
FIRST
CONFERENCE
MONTRÉAL
JUNE 4–9, 2023

Wrap-Up

Wrap-Up & Key Takeaway

- ***Wrap-Up***
  - Cyber Hygiene Hunting is powerful tools to be “Adaptive”
  - We shared various concept such as:
    - *Enabler of Compromise*
    - *Continuous Monitoring and Continuous Improvement (CM/CI)*
    - *Pyramid of Gain (Scope of CHH)*
  - Also, we shared various real-world example for Cyber Hygiene Hunting

- ***Key Takeaway:***
  - Recommend to start Cyber Hygiene Hunting, since we can start easily but very powerful and proactive approach

Thank you !

Any Questions? Any Comments?

@scientia_sec

https://www.linkedin.com/in/tomohisaishikawa/

tomohisa.ishikawa2@tokiomarinehd.com