



Real-time detection of attacks leveraging Domain Administrator privilege

December 5

The University of Tokyo
Wataru Matsuda,
Mariko Fujimoto,
Takuho Mitsunaga

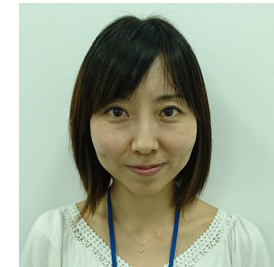
Our profile

- **Wataru Matsuda, Mariko Fujimoto, Takuho Mitsunaga**

- Secure Information Society Research Group,
The University of Tokyo (SiSOC)

- Job description:

- Technical Analysis and Research on cyber security
- Education and Training regarding cyber security



- Publication/Works :

- [Books] CSIRT – from building to operating – (coauthor)
- [Research]
 - “Tracking mimikatz by Sysmon and Elasticsearch”, Hitcon 2017
 - “Real-time Log Analysis Tool with STIX 2.0”, FIRST ANNUAL Conference 2018
 - “Protecting Struts 2 from OGNL related attacks by using Servlet Filter”, ASIA JCIS 2018
 - “Detecting APT attacks against Active Directory using Machine Learning, AINS 2018

Agenda

- Introduction
- Previous research
- Proposed Method
 - Signature based detection
 - Machine Learning
 - Real-time alert
- Demonstration
- Conclusion



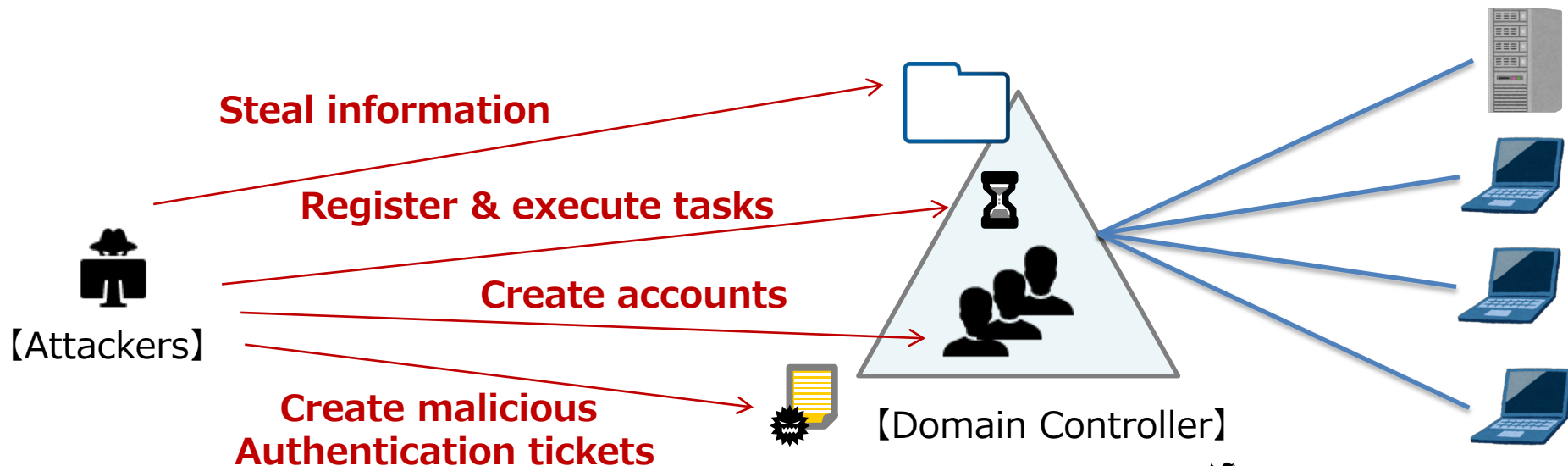
Introduction

Introduction

- In targeted attacks, attackers tend to attack Active Directory (AD) in order to expand infections
- Attackers try to take over Domain Administrator privileges and create a backdoor called the "Golden Ticket"
- Attackers leverage the Golden Ticket to disguise themselves as legitimate administrator accounts to avoid detection for a long period of time
- We've implemented a real-time detection method combining signature-based and machine learning detection that utilizes Domain Controller Event Logs in order to detect attack activities including the use of Golden Tickets

Overview of Active Directory

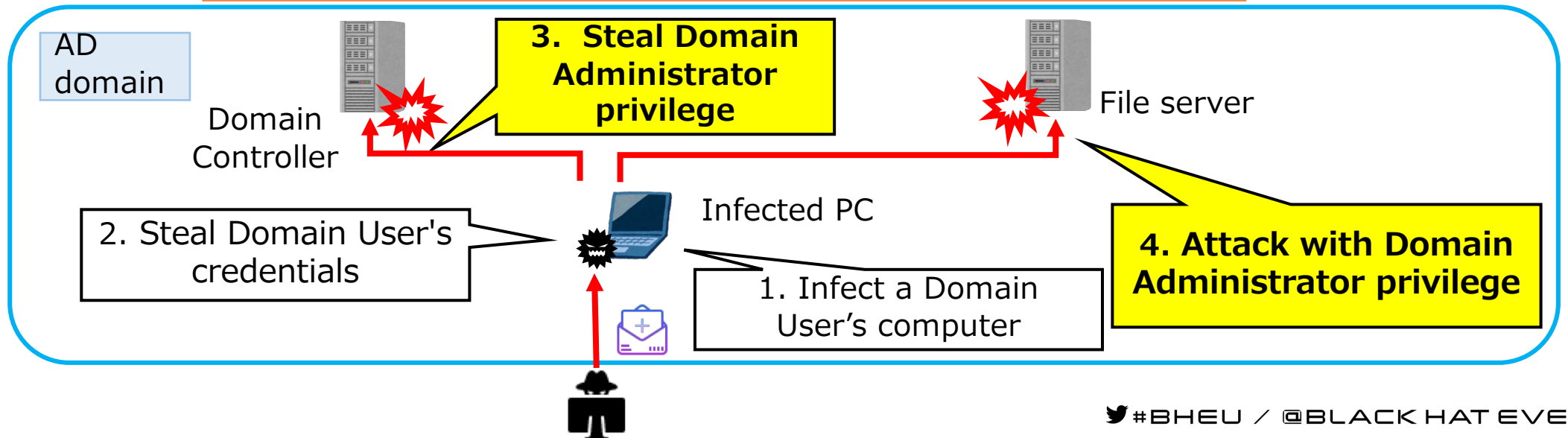
- A centralized management system for Windows computers and accounts
- Domain Controller uniformly processes the authentication of all computers and accounts
- Domain Administrators have the privilege to control all resources in the AD environment
- If attackers compromise the Domain Administrator privileges, they will have almost complete control of the AD environment



Example of attack flow leveraging AD

1. Infect a Domain User's computer with malware
2. Steal Domain User's credentials to prepare for exploiting higher privilege accounts
3. Take over the Domain Administrator privileges (e.g. privilege escalation)
4. Expand infection into the network with the Domain Administrator privilege

In this presentation, we focus on the phase 3 and 4



Golden Ticket Attack

- Attackers that obtain Domain Administrator privileges are likely to create a Golden Ticket
- A Golden Ticket is a TGT※ created by the attackers that has a **legitimate signature** and **a long term of validity** (e.g. ten years)
- Attackers can disguise themselves as arbitrary accounts for a long period of time with the Golden Ticket

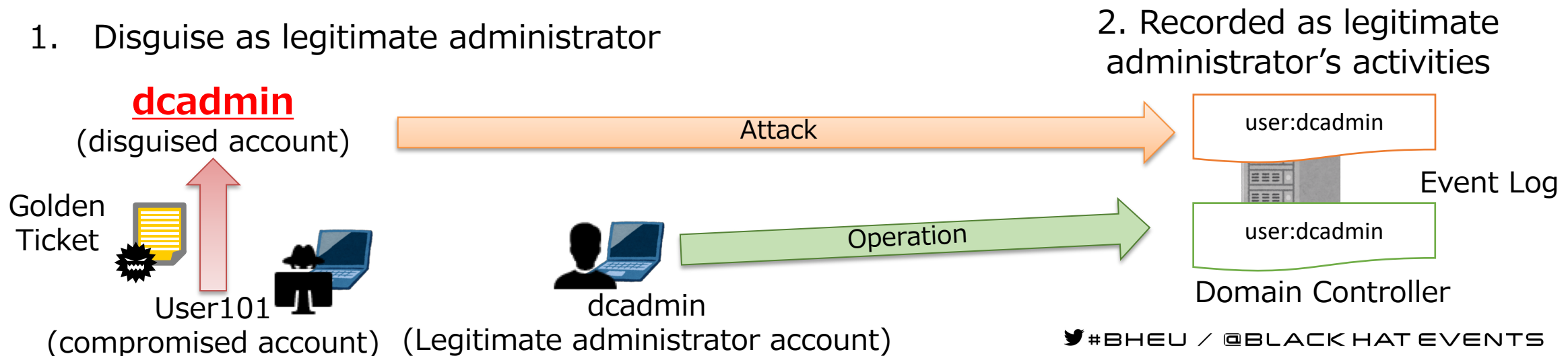
※Ticket-Granting Ticket (TGT): A Kerberos Authentication ticket that proves the authenticity of the user. The default expiration limit of TGT is ten hours

Reference: Abusing Kerberos

<https://www.blackhat.com/docs/us-14/materials/us-14-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It-wp.pdf>

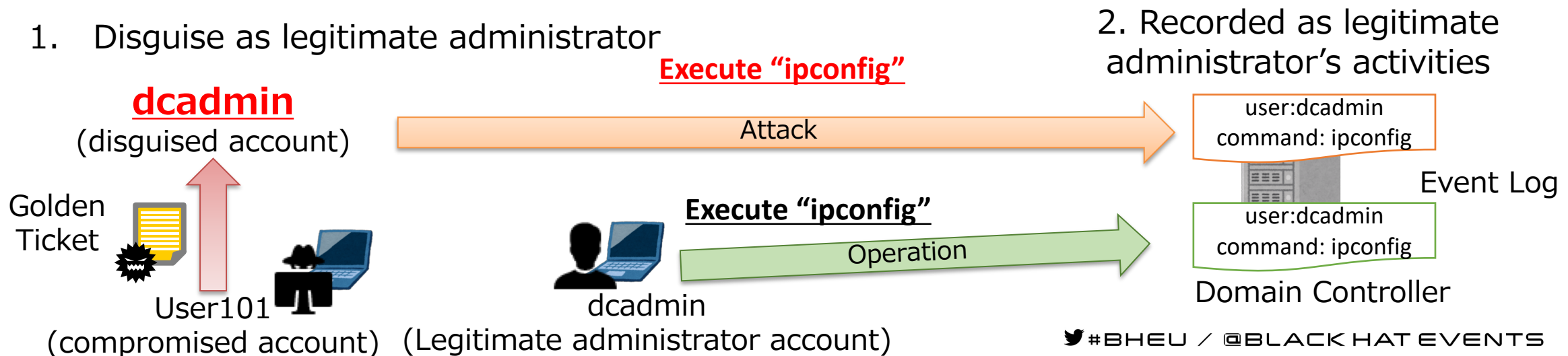
Difficulty of detecting Golden Ticket attacks

- Attackers can disguise themselves as a legitimate Domain Administrator
- Attackers' activities are recorded as those of a legitimate Administrator in the Windows Event Logs
- If attackers could compromise the Domain Administrator's computer, detecting Golden Ticket could be more difficult



Difficulty of detecting Golden Ticket attacks

- Attackers use some **built-in windows commands** in addition to attack tools
- It is difficult to identify attackers' activities if legitimate administrators often use commands in daily operations
- If legitimate administrators use the same commands in daily operations, detection can be more difficult





Proposed method

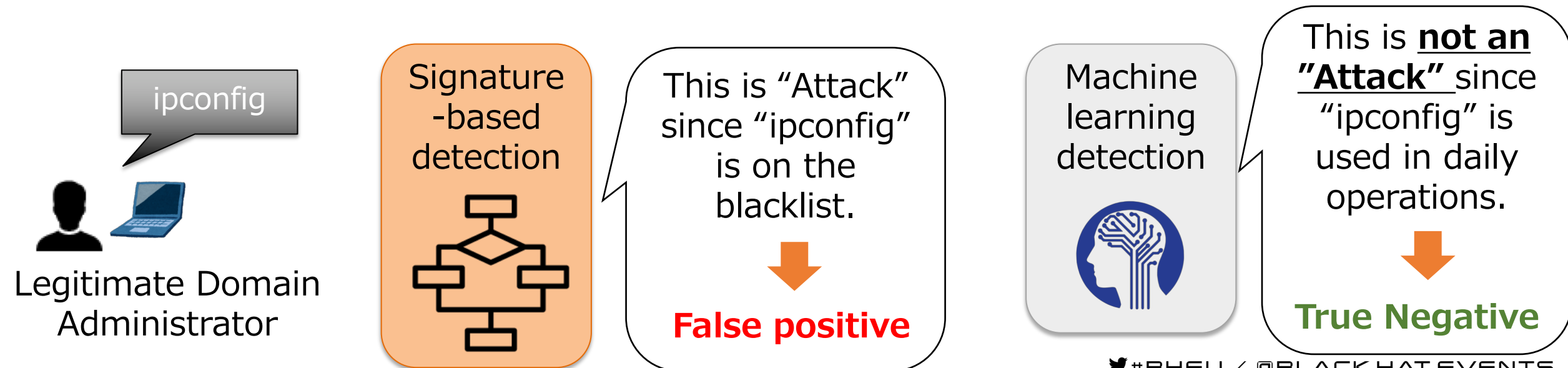
Summary of the proposed method

- We've implemented a real-time detection method to detect attack activities that abuse Domain Administrator privileges such as the use of Golden Tickets
- It analyzes Event Logs with **signature-based and machine learning detection** to yield high detection rate
- If attackers' activities are detected, real-time alerts are raised

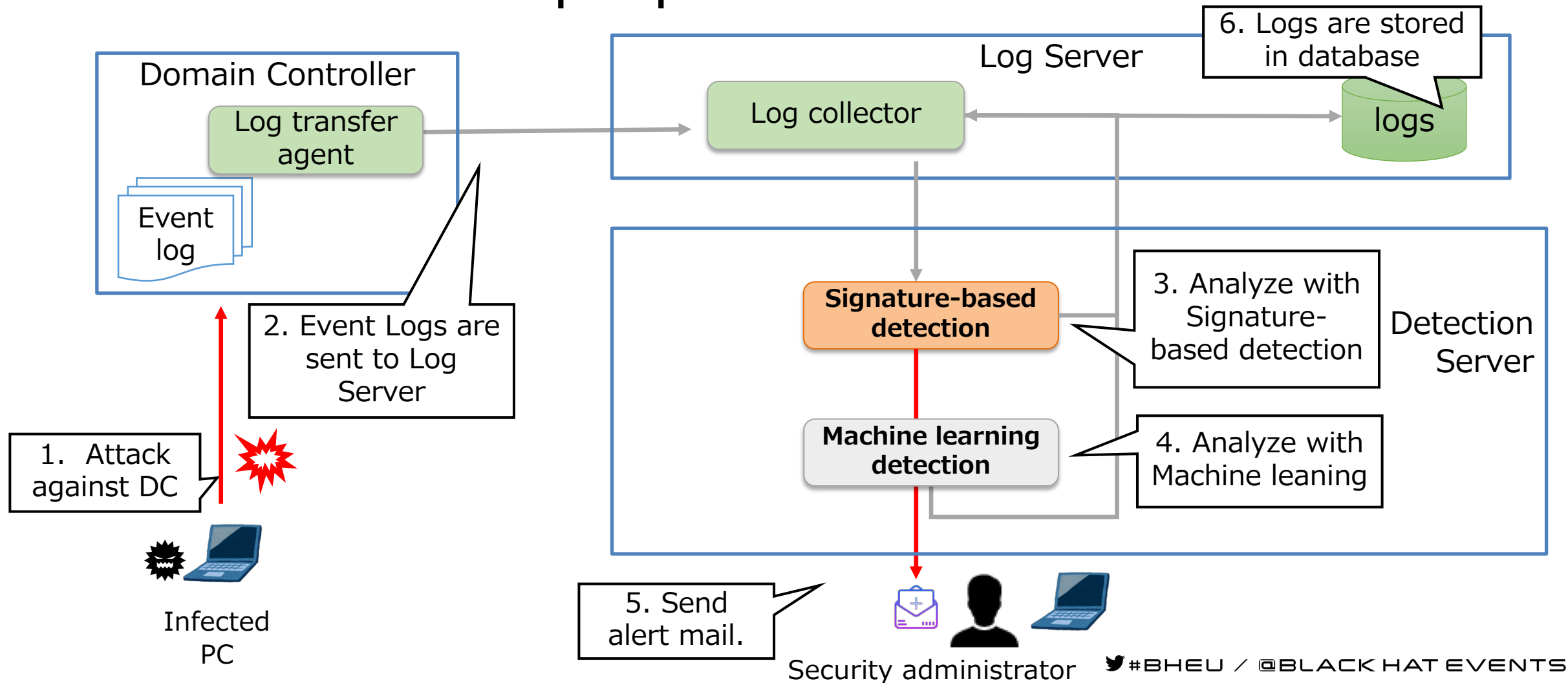
Methods	Advantages	Disadvantages
Signature-based detection	It yields high recall rate.	A lot of false positive can occur depending on the daily operations.
Machine learning detection	It can find unusual activities compared with daily operations.	False negative can occur in some situations.

Problems of the signature-based detection

- For detection of suspicious commands, a lot of false positives can occur when the legitimate Domain Administrator uses the commands included in the blacklist for daily operations
- To solve the problem, we re-analyze the results of signature-based detection using machine learning



Structure of the proposed method



Input data

- Input data is the **Domain Controller's Event Logs**
- Focus on detecting **attacks against the Domain Controller**

Event ID	Description	The point for detection
4672	Special privileges assigned to a new login	Information of accounts that use administrative privileges are recorded.
4674	An operation was attempted on a privileged object	Specific commands and process executed with administrative privilege are recorded.
4688	A new process has been created	All processes information including attack commands are recorded.
4768	A Kerberos authentication ticket (TGT) was requested	When a Golden Ticket is used, this event is not recorded.
4769	A Kerberos service ticket was requested	When a service is accessed using a TGT including the Golden Ticket, this event is recorded.
5140	A network share object was accessed	This event is recorded when a file sharing service is accessed.

Input data

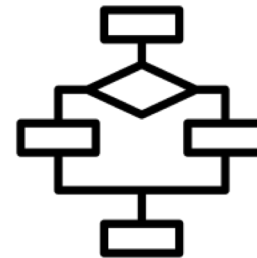
- We extract the following items from Event Logs, and use them for input

Event ID	Account name	IP address	Service name	Process name	Object name	Shared name
4672	○	—	—	—	—	—
4674	○	※	—	○	○	—
4688	○	※	—	○	—	—
4768	○	○	○	—	—	—
4769	○	○	○	—	—	—
5140	○	○	—	—	—	○

※Event ID 4674 and 4688 have no information of IP address. The method identifies IP address from Event ID 4769 recorded just before Event 4674/4688 for each accounts





Proposed method

-Signature-based detection-



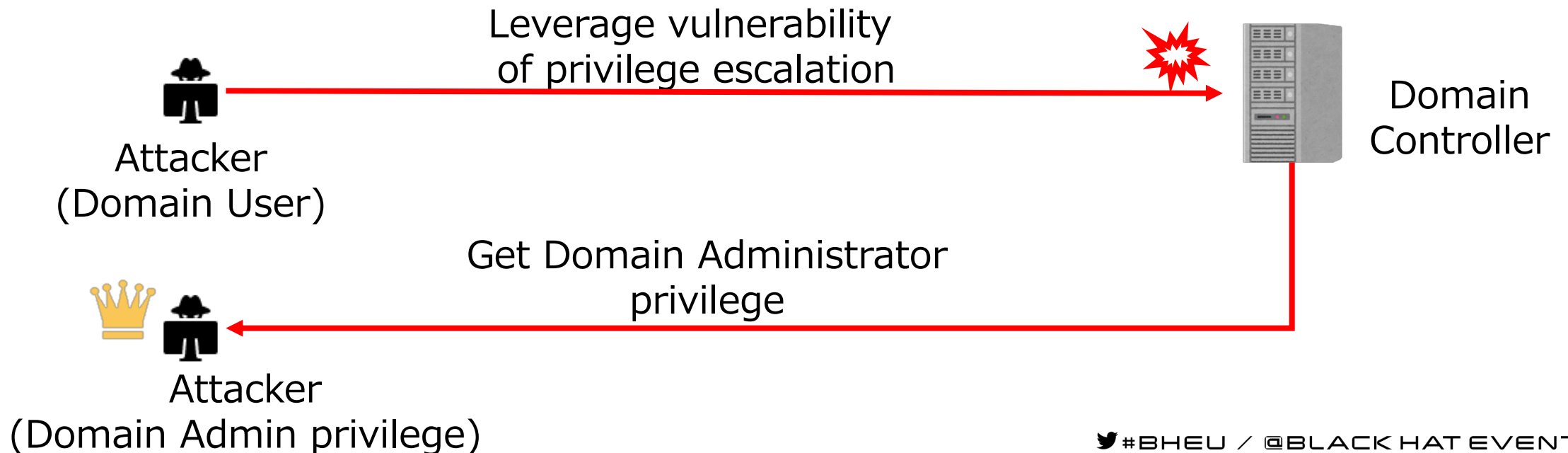
Signatures for detection

- We pick up several useful existing methods, and organize specific detection signatures

	Signature	Icon
A	Unexpected use of administrative privilege	
B	Execution of CLI tools that attackers tend to use	
C	Use of administrative shared resources	
D	Service Ticket requests made without a prior TGT request	

Signature A) Unexpected administrative privilege use

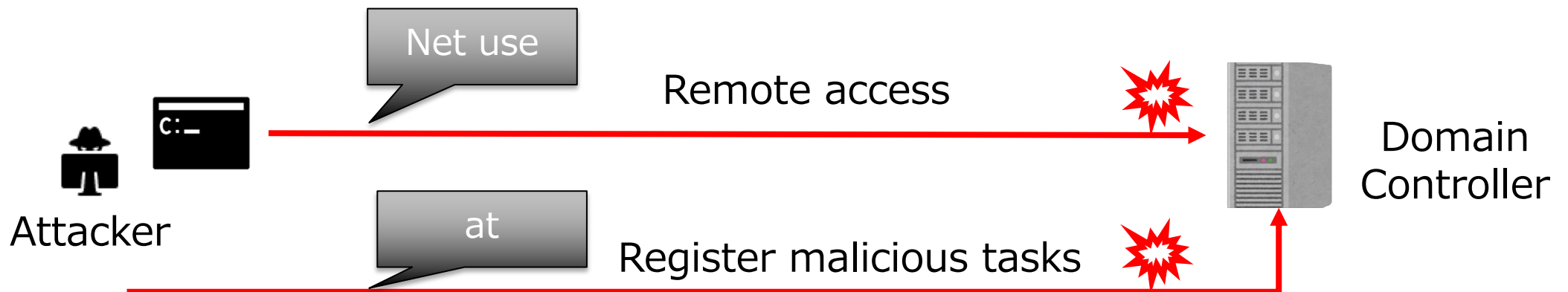
- Useful for detecting privilege escalation such as the use of vulnerability MS14-068 (CVE-2014-6324)
- Detection method: Compare accounts recorded in Event ID:4672 with an administrator account list in the operational environment



Signature B) Execution of tools attackers tend to use



- Useful for detecting activities such as remote access or task creation
- Detection method: Compare process information recorded in Event ID:4674 and 4688 with commands in the black list
- Pre-process: Add IP address information to Event ID 4674 and 4688
 - Extract IP address information from Event ID 4769 (service ticket request) recorded just before Event ID 4674, 4688





Signature B) Execution of tools attackers tend to use



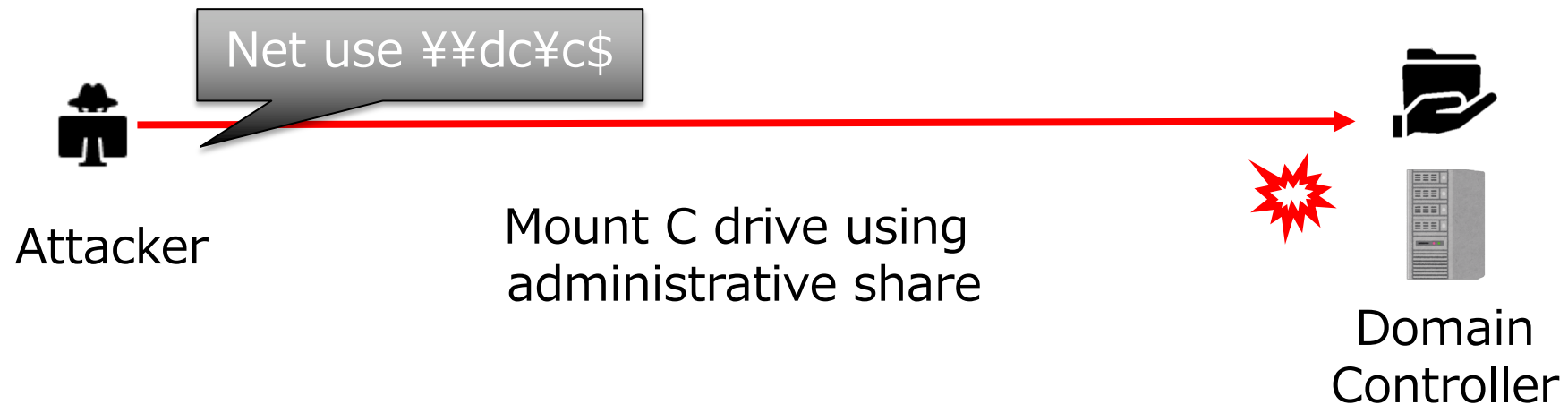
- We register the following commands into the blacklist, since they tend to be used by attackers

Command	
tasklist.exe	type
ver	at.exe
ipconfig.exe	reg.exe
systeminfo.exe	wmic.exe
net.exe	wusa.exe
netstat.exe	netsh.exe
whoami.exe	sc.exe
qprocess.exe	rundll32.exe
query.exe	schtasks.exe
dir	ping.exe

Reference: <https://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html>

Signature C) Use of administrative shared resource

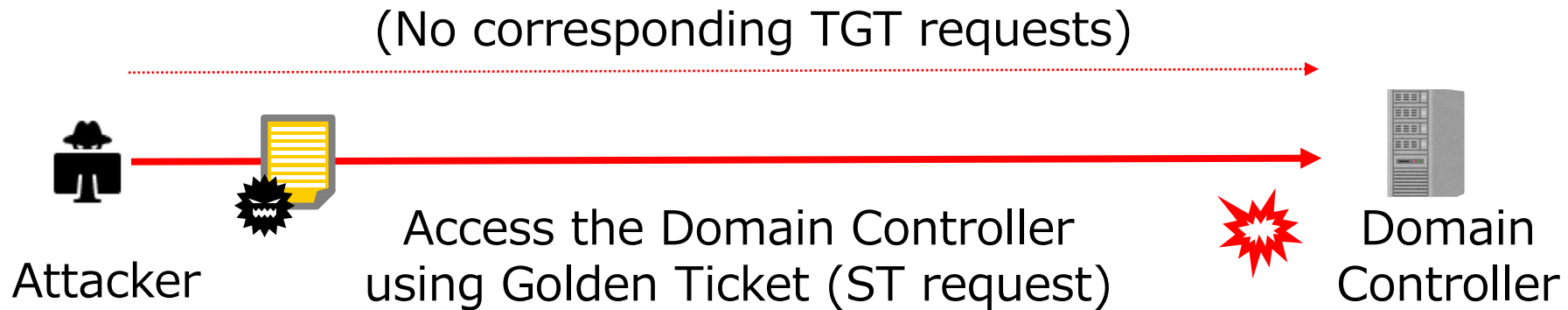
- Useful for detecting activities such as placing attack tools or stealing information
- Detection method: Extract administrative shared resources such as "¥c\$" recorded in Event ID:5140



Signature D) ST requests without a prior TGT request

- Useful for detecting use of the Golden Ticket
- Detection method: Extract Event ID:4768(TGT request) and 4679(ST request), and sort by account and computer

Find Event ID 4769 without corresponding 4768

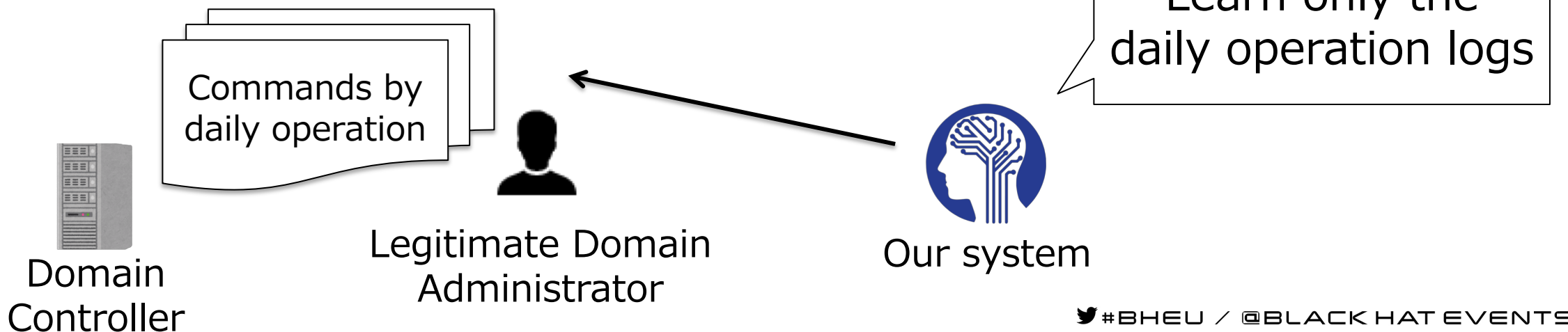


Proposed method -Machine Learning -



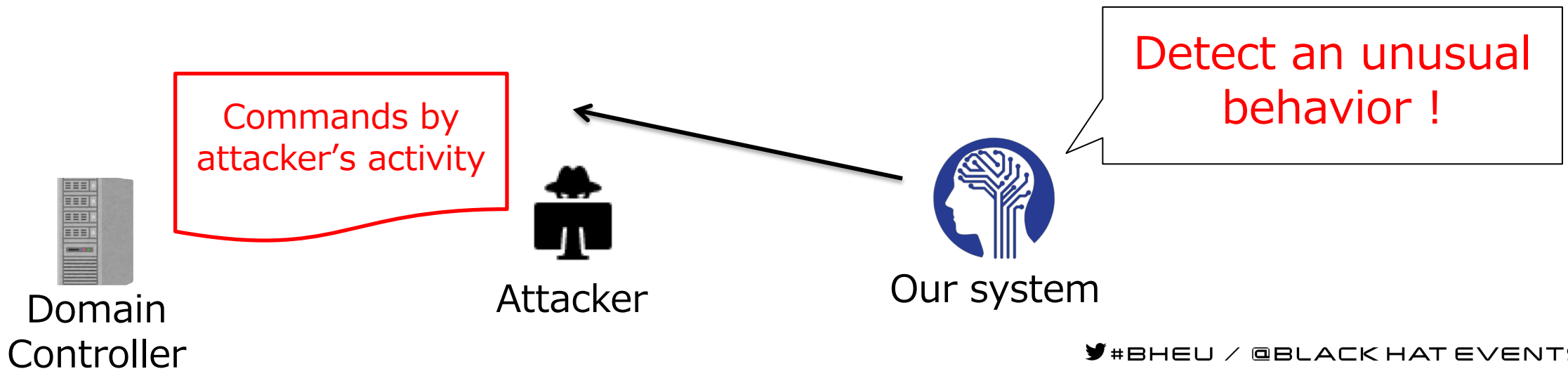
Why machine learning?

- Comparing logs with daily operations (commands, account, etc.) can reduce False positive
- It's difficult to add daily operations to the white list manually
- Our proposal is learning the daily operations using **unsupervised machine learning**



Why machine learning?

- Comparing logs with daily operations (commands, account, etc.) can reduce False positive
- It's difficult to add daily operations to the white list manually
- Our proposal is learning the daily operations using **unsupervised machine learning**



Overview of detection with machine learning

- Learn Event Logs related to processes with “**unsupervised learning**” in order to detect unusual command execution
- The dataset should be Event Logs **only of the normal state** (should not contain logs of an attack)

Event ID	Summary	Characteristic of the event
4688	A new process has been created	All executed commands and process are recorded.
4674	An operation was attempted on a privileged object	Specific commands and process executed with administrative privilege are recorded.

Pre-process

- Ignore some data commonly included in every log regardless of environment (not a feature for detection)
 - lsass.exe
 - services.exe
- Encode dataset using One-Hot encoding

Machine learning algorithm

- Learn with **One-class SVM**
- One-class SVM is an unsupervised algorithm that learns a decision function for novelty detection with only one label
- The following hyper parameters are adjustable. We use grid search to determine the best hyper parameter
 - nu : Specifies the proportion of outliers expected in the dataset
 - gamma: Controls the influence of individual training samples
 - Example: `clf = svm.OneClassSVM(nu=0.01, kernel="rbf", gamma=0.01)`

Evaluation metrics

- We use the following metrics to evaluate detection quality.
 - **Precision:** The ratio of correctly predicted positive observations to the total predicted as a positive class.
$$\text{Precision} = TP / (TP + FP)$$
 - **Recall:** The ratio of correctly predicted positive observations to the all observations in actual positive class.
$$\text{Recall} = TP / (TP + FN)$$

Detection rate

- Machine learning reduces False positive

	Signature-based detection only	Signature-based detection + Machine learning detection
True Positive	78	78
True Negative	112,255	112,266
False positive	17	6
False negative	5	5
Recall(%)	93.98	<u>93.98</u>
Precision(%)	82.11	<u>92.86</u>

N=112355

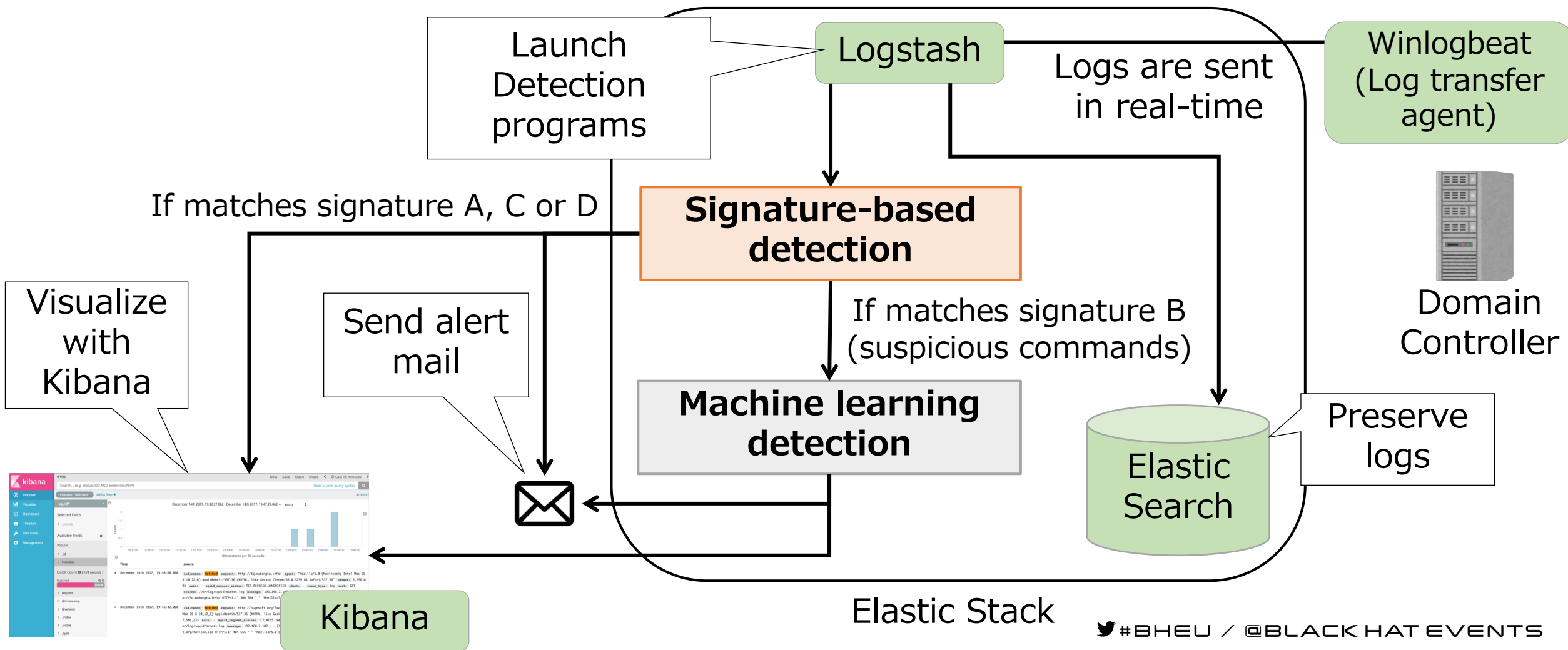


Real-time alert

Real-time detection using Elastic Stack

- We implement the proposed method using Elastic Stack
 - Preserve Windows Event Logs
 - Detect attacks in a timely-manner
 - Send alerts when attacks are detected

Implementation using Elastic Stack





Demonstration

Demonstration scenario

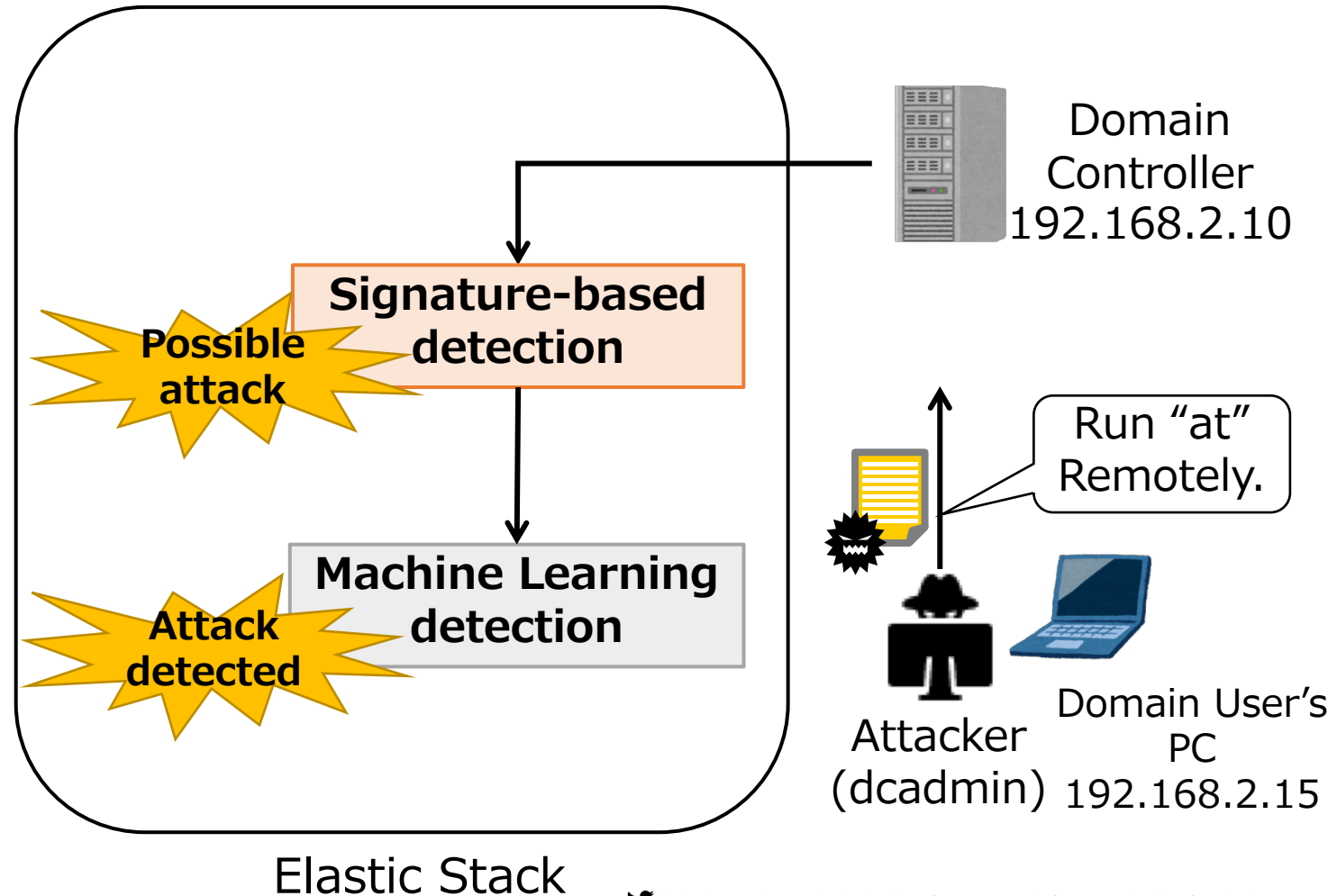
- The preconditions of the scenario are:
 - Legitimate Domain Administrator (dcadmin) accesses the Domain Controller:
 - Remote access to DC from Domain User's PC (192.168.2.15)
 - Legitimate Domain Administrator uses "ipconfig" and "ping" in daily operations
 - Legitimate Domain Administrator does not use "at" command in daily operations

Demonstration scenario

- The preconditions of the scenario are:
 - Attackers have already compromised the target network
 - Attackers have compromised a legitimate Domain Administrator account (dcadmin) and his/her computer (192.168.2.15)
 - Attackers have created a Golden Ticket for the account "dcadmin"

Demonstration scenario

1. The attacker accesses the DC using remote access tool "PsExec" with a Golden Ticket
2. Signature-based detection detects attack since "at" command is on the blacklist (matches signature B)
3. Machine Learning also detects attack since "at" command is not used in daily operations
4. Alert mails are sent to the security operators



Considerations of False detections

- A False negative detection can occur if all the following conditions are satisfied
 - Attackers use the same commands that legitimate domain administrators use in their daily operations
 - Attackers compromise legitimate domain administrator accounts and their computer
 - Attackers use windows commands which are not in the blacklist
- A False positive detection occurs in the following condition
 - The commands that are not frequently used in daily operations are used



Conclusion

Conclusion

- The abuse of a Domain Administrator means the AD is under the full control of the attacker, and thus requires immediate action
- Attack detection is difficult if legitimate administrator accounts are abused such as the case with Golden Ticket attacks
- Our method can detect attacks in timely manner, and yields a high detection rate even if legitimate accounts or built-in commands are leveraged
- For future works, we are planning to analyze Event Logs of client computers for further investigation



We published the source code of our tool.

<https://github.com/sisoc-tokyo/Real-timeDetectionAD>

Thank you for your attention!

coe@sisoc.org