



# HAWKEYE

HUNTING CYBER ADVERSARIES

## **HawkEye AI** *powered by* DTS Solution

Hunting Cyber Adversaries

# Table of Content

Machine Learning for Enhanced Threat Detection in SOC	3
Outlier Threshold	4
User Behaviour Analysis	5
<hr/>	
Login Geo Anomaly Detection	6
RDP Login Anomaly Detection	7
Traffic to an Anomalous Service	8
Traffic to an Anomalous Domain	9
Traffic using Anomalous Header	10
Anomalous Logon Process	11
Anomalous Logon Type	12
Anomalous Operation Office 365	13
Anomalous Admin Operations Azure AD	14
Anomalous User Operations Azure AD	15
Anomalous Application Usage	16
Anomalous Operation by User in Azure	17
Anomalous Operation by User in Azure	18
<hr/>	
DNS Based Threat Detection	19
DGA detection	20

# Machine Learning and AI for Enhanced Cyber Threat Detection

HAWKEYE Managed CSOC and XDR powered by DTS Solution helps you stay ahead of the cyber threat and adversary landscape.

The overarching goal of our machine learning initiatives in the Security Operations Center (SOC) context is to enhance the SOC's capabilities in detecting, analyzing, and responding to cybersecurity threats more efficiently and accurately.

## HawkEye AI - Goals



**Improve Threat Detection**



**Reduce False Positives**



**Enhance Prediction Capabilities**



**Streamline SOC Operations**



**Adapt to Evolving Threats**

# Outlier Threshold

**HAWKEYE AI and Machine-Learning models are trained to discern the normal operational baselines for system interactions and user behaviors.**

These baselines encompass a wide array of metrics, such as login frequencies, file access patterns, and network traffic norms. By applying statistical methods, the models develop an understanding of what constitutes typical behavior within these metrics. The outlier threshold is then established around this norm, often set at a point that captures the desired balance between sensitivity and specificity.

When user behavior crosses this threshold, an alert is generated, signifying a possible security event. The precision of this threshold is crucial: too sensitive, and we risk overwhelming our analysts with false positives; too lax, and genuine threats may slip through unnoticed. Therefore, we implement an iterative approach, where the threshold is regularly adjusted to account for evolving patterns and to maintain an optimal level of alerting.

In practice, this means our machine learning algorithms are not only identifying outliers but also learning from what subsequent investigations reveal about these outliers, be they false alarms or actual compromises.

This learning feeds back into the model, making our thresholding more intelligent and responsive to the ever-changing landscape of cyber threats.

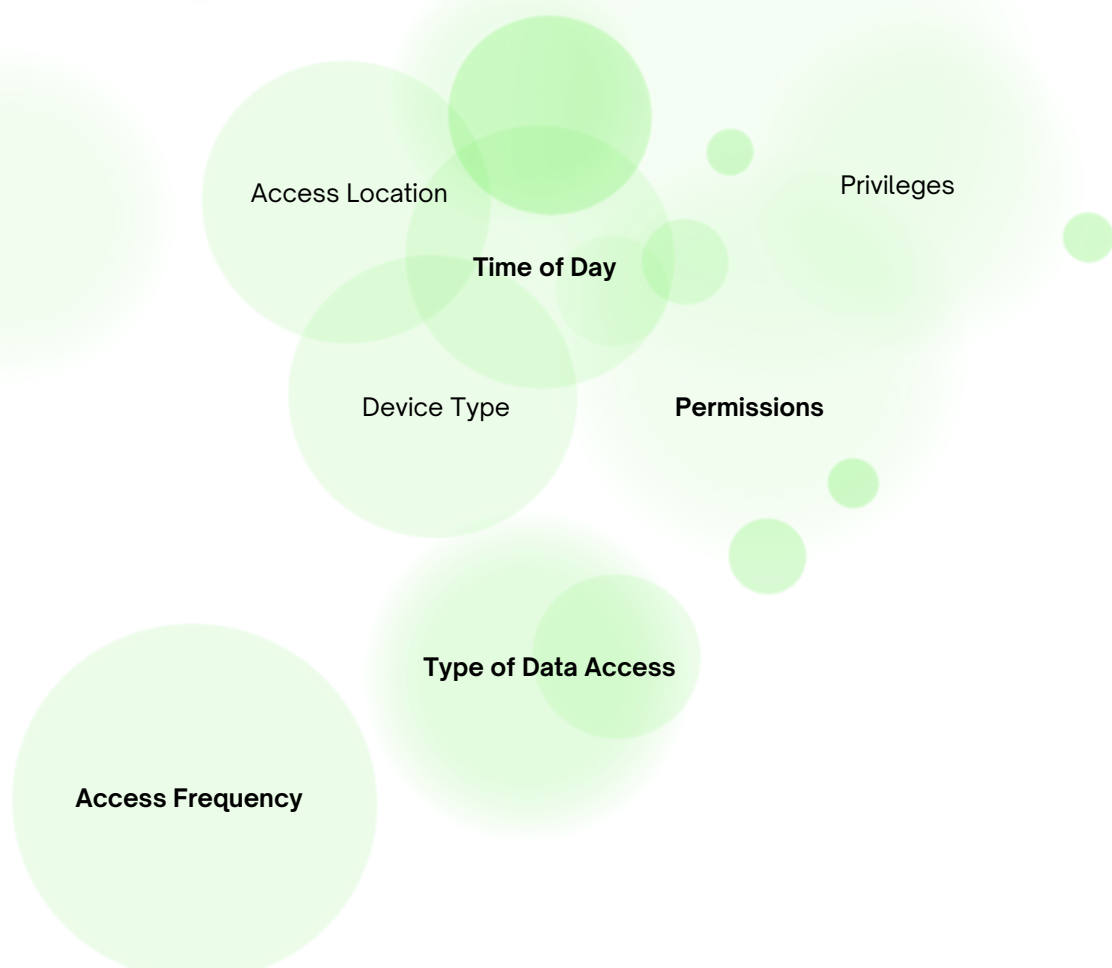
Thus, the outlier threshold is more than a mere demarcation—it's a dynamic tool that adapts to our unique security environment, enhancing our SOC's ability to safeguard our digital ecosystem effectively.

# USER BEHAVIOUR ANALYSIS

User behavior analysis via machine learning in SOCs entails creating detailed profiles of typical user activity and employing these profiles to detect anomalous actions that could indicate security breaches.

Machine learning algorithms analyze a wealth of data points, like the timing, location, device type, and frequency of user activities, along with access patterns to critical files and systems.

Deviations from established patterns are flagged for further investigation, enabling SOC teams to proactively address potential security incidents. This continuous and automated analysis facilitates a dynamic defense mechanism, crucial for modern digital security.

A diagram consisting of several overlapping light green circles of varying sizes. Each circle contains a text label representing a factor in user behavior analysis. The labels are: 'Access Location' (top left), 'Time of Day' (center), 'Device Type' (middle left), 'Permissions' (middle right), 'Privileges' (top right), 'Type of Data Access' (bottom center), and 'Access Frequency' (bottom left).

Access Location

Privileges

Time of Day

Device Type

Permissions

Type of Data Access

Access Frequency

# Login Geo Anomaly Detection

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Initial Access (TA0001) □

### TECHNIQUES

T1078: Valid Accounts □

T1090: Connection Proxy

Monitoring for geographical irregularities in login patterns is essential in pinpointing unauthorized access attempts within an organization's network. This use case revolves around identifying logins from locations that are unusual for a specific user, which could suggest the presence of compromised credentials or an attacker trying to gain unauthorized access to the network.

## Detection Criteria:

Geo-anomaly detection in network security monitors for logins from locations atypical for a user, which could signal compromised credentials or unauthorized access. The static field User Id identifies the user, while the dynamic field Country Name records the login's origin country. By establishing a user's normal login geography, the system flags deviations, such as new country logins or unusual patterns, prompting an immediate investigation.

# RDP Login Anomaly Detection

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Credential Access (TA0006)

Discovery (TA0007)

Lateral Movement (TA0008)

### TECHNIQUES

T1078: Valid Accounts

T1021.001: Remote Services

Remote Desktop Protocol (RDP) login anomaly detection is a critical security measure that focuses on monitoring and analyzing login patterns to identify irregular activities that could suggest unauthorized access attempts or brute force attacks.

## Detection Criteria:

To effectively detect anomalies in RDP logins, it's essential to monitor specific fields in event logs. The Target Username (static) helps identify the account being accessed, while dynamic fields like Subject Username, IP address, and Computer offer insights into the nature of each login. Monitoring Subject Username detects discrepancies in access attempts, IP address flags logins from unusual or inconsistent locations, and computer tracks access to various machines within the network. Analyzing these fields helps promptly identify and respond to potential security threats related to RDP access.

# Traffic to an Anomalous Service

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Command and Control (TA0001)

### TECHNIQUES

T1043: Commonly Used Port

T1071: Standard Application Layer protocol

T1065: Uncommonly Used port

T1102: Webservice

In the SOC context, monitoring for traffic to anomalous services involves identifying unusual outbound connections that deviate from normal network behavior. This detection highlights potential communications with unauthorized or malicious external services, signalling possible system compromises or data exfiltration attempts.

## Detection Criteria:

The detection hinges on analysing the network traffic where the Source IP acts as the static field representing the initiating device within the organization's network. The Destination Port and Destination IP serve as dynamic fields and are key to identifying the nature and legitimacy of the external service being accessed.



# Traffic to an Anomalous Domain

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Command and Control (TA0011)

Initial Access (TA0001)

### TECHNIQUES

T1189: Drive-by Compromise

T1566: Phishing

T1041: Exfiltration over Command and Control

In SOC operations, identifying traffic to anomalous domains is key to detecting potential threats. This use case focuses on spotting requests to domains that do not match the organization's usual internet usage patterns, potentially indicating phishing attempts, malware communication, or data exfiltration activities.

## Detection Criteria:

The analysis is centered on web traffic passing through proxies (e.g., Zscaler), where Proxy Names serve as the static field, representing the intermediary devices or services handling the organization's web traffic. The Hostname acts as the dynamic field, essential for identifying the destination of web requests. Monitoring for requests to unusual hostnames through known proxies enables the detection of anomalous domain access, which may be related to malicious activities or compromised endpoints.

# Trafficusing Anomalous Header

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Command and Control (TA0011)

Initial Access (TA0001)

### TECHNIQUES

T1189: Drive-by Compromise

T1566: Phishing

T1041: Exfiltration over Command and Control

Traffic with anomalous headers is a critical focus for SOC teams, aimed at identifying web requests that carry unusual or suspicious HTTP header values. This activity can signal attempts to disguise malicious traffic, exploit vulnerabilities, or bypass security controls, potentially leading to compromised systems or data breaches.

## Detection Criteria:

The detection framework employs Proxy Names (e.g., Zscaler) as the static field, which identifies the network's web traffic management systems. The Header Applications act as the dynamic field, referring to the specific HTTP header fields in web requests. Monitoring for unusual or non-standard header values, especially when routed through organizational proxies, helps in pinpointing web traffic that could be attempting to conceal its true nature or origin, flagging it for further investigation.

# Anomalous Logon Process

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Credential Access (TA0006)

Persistence (TA0003)

Privilege Escalation (TA0004)

### TECHNIQUES

T1078: Valid Accounts

T1003: Credential Dumping

T1101: Security Support Provider

Monitoring for anomalous logon processes is crucial for identifying potentially malicious activities within an organization's network. This use case focuses on detecting logon attempts that involve atypical processes or methods, which could indicate the use of stolen credentials, exploitation of vulnerabilities, or an attacker's attempt to establish persistence or escalate privileges within the network.

## Detection Criteria:

The analysis is centred around the Target Username as the static field, pinpointing the account being accessed. The dynamic fields, Subject Username and Logon Process Name, are key to identifying who is attempting access and the method being used. Unusual or unrecognized logon processes, especially when they differ from the norm for a given user or system, can signal unauthorized access attempts, requiring immediate investigation.

# Anomalous Logon Type

**0.2**

Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Initial Access(TA0001)

Persistence (TA0003)

Lateral Movement (TA0008)

### TECHNIQUES

T1078: Valid Accounts

T1021: Remote Services

T1133: External remote Services

The detection of anomalous logon types is aimed at identifying logon attempts that utilize unusual or suspicious methods, which could signify malicious activities such as unauthorized access, credential misuse, or attempts to bypass normal authentication mechanisms. This monitoring is crucial for early detection of potential security breaches or insider threats.

## Detection Criteria:

This use case leverages the Target Username as the static field, focusing on the specific account that is being accessed. The dynamic fields, Subject Username and Logon Type, provide insights into the identity of the user attempting access and the method of logon being used, respectively. Anomalies in logon types, such as the use of remote access methods where they are not expected, can be indicative of compromise or malicious intent, prompting further investigation.

# Anomalous Operations O365

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Credential Access (TA0006)

Discovery (TA0007)

Persistence (TA0003)

Privilege Escalation (TA0004)

### TECHNIQUES

T1078: Valid Accounts

T1526: Cloud Service Discovery

T1578: Modify Cloud Compute Infrastructure

T1548: Abuse Elevation Control Mechanism

Detecting anomalous combinations of application usage and operations in Office 365 is crucial for identifying activities that may compromise security or indicate malicious behavior. This involves spotting actions that are not in alignment with typical user patterns or job functions, potentially signaling account compromise, insider threats, or targeted attacks within the cloud services environment.

## Detection Criteria:

The detection mechanism focuses on **Office\_365 User Id** as the static field, pinpointing the user involved in the activity. The dynamic fields, **Office\_365 Application**, and **Office\_365 Operation** are instrumental in identifying not only the applications being accessed but also the specific operations being performed. Anomalies are detected when there is a divergence from the norm in the combination of applications and operations being used, such as accessing sensitive applications with operations that the user does not normally perform, which could indicate unauthorized access or misuse.

# Anomalous Admin Operations Azure AD

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Credential Access(TA0006)

Defense Evasion(TA0005)

Persistence (TA0003)

Privilege Escalation (TA0004)

### TECHNIQUES

T1578: Modify Cloud Compute Infrastructure

T1548: Abuse Elevation Control Mechanism

T1543: Create or Modify System Process

This use case targets the detection of unusual or unauthorized operations performed in Azure Active Directory (Azure AD) by a user, which could signal potential security incidents such as account compromises, privilege escalation attempts, or unauthorized modifications within the Azure environment. It's crucial for maintaining the integrity and security of Azure AD services and sensitive organizational resources.

## Detection Criteria:

The analysis leverages Office\_365 User Id as the static field to identify the user account executing operations within Azure AD. The dynamic field, Office\_365 Operation, is essential for detailing the specific actions taken by the user. Anomalies are identified when operations performed by a user deviate significantly from their normal behavior patterns or when sensitive operations are executed that are not typical for the user's role, suggesting possible malicious activity or policy violations.

# Anomalous User Operations Azure AD

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□TACTICS

Credential Access(TA0006)

Defense Evasion(TA0005)

Privilege Escalation (TA0004)

### TECHNIQUES

T1078: Valid Accounts

T1578: Modify Cloud Compute Infrastructure

T1548: Abuse Elevation Control Mechanism

This use case involves the detection of anomalous or unauthorized user activities based on operations performed within Azure Active Directory (Azure AD). It aims to identify instances where operations typically not associated with a user's normal role or behavior patterns are executed, potentially indicating compromised accounts, privilege abuse, or insider threats within the Azure environment.

## Detection Criteria:

The detection strategy uses Office\_365 Operation as the static field, focusing on the specific types of operations being performed within Azure AD. The dynamic field, Office\_365 User Id is critical for identifying which user is operating. Anomalies are flagged when operations that are unusual for a given user's typical activity patterns are detected, such as a non-administrative user attempting admin-level operations, which could suggest unauthorized access or an attempt to escalate privileges improperly.

# Anomalous Application Usage

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□ TACTICS

Execution (TA0002)

Discovery (TA0007)

Persistence (TA0003)

Privilege Escalation (TA0004)

### TECHNIQUES

T1518: Software Discovery

T1059: Command and Scripting Interpreter

T1204: User Execution

Anomalous application usage monitoring is designed to identify unexpected or suspicious use of software applications within an organization's network. This can point to various security issues, such as compromised accounts, insider threats, or malware activity, especially when the application usage deviates from the user's normal behavior patterns or job requirements.

## Detection Criteria:

The framework for detection incorporates **Source IP** as the static field, which identifies the originating IP address of the application usage within the network. The dynamic field, **Application Name**, is crucial for determining the specific application being accessed or used. Anomalies in application usage are flagged when there is a significant deviation from established patterns, such as the use of high-risk applications, applications not typically used within the user's role, or applications being accessed at unusual times, indicating potential security concerns.



# Anomalous Operation by User in Azure

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□TACTICS

Credential Access(TA0006)

Discovery (TA0007)

Impact (TA0040)

Privilege Escalation (TA0004)

### TECHNIQUES

T1078: Valid Accounts

T1530: Data from Cloud Storage Object

T1578: Modify Cloud Compute Infrastructure

This use case zeroes in on detecting irregular or suspicious operations conducted by users within the Azure environment. It is particularly focused on identifying actions that deviate from a user's normal activity pattern, which could be indicative of compromised credentials, attempts to exploit system vulnerabilities, or unauthorized attempts to access or modify resources.

## Detection Criteria:

The approach utilizes **Azure activity Caller** as the static field to identify the specific user (or entity) initiating the operation. The dynamic field, **Azure activity Operation Name**, is essential for detailing the exact nature of the operation being performed. Anomalies are detected when a user performs operations that are unusual for their role or historical behavior, such as accessing resources or performing administrative actions they normally do not, suggesting potential security risks that need immediate attention.

# Anomalous Operation by User in Azure

0.2



Outlier Threshold

## MITRE ATT&CK Mapping

### □□TACTICS

Credential Access(TA0006)

Privilege Escalation (TA0004)

Defense Evasion(TA0005)

### TECHNIQUES

T1078: Valid Accounts

T1548: Abuse Elevation Control Mechanism

T1578: Modify Cloud Compute Infrastructure

This use case focuses on identifying instances where the entity performing an operation within the Azure environment is unexpected or out of the ordinary for the type of operation being executed. It aims to uncover potential security issues such as compromised credentials, unauthorized access, or insider threats by monitoring for operations conducted by users who do not normally perform them.

## Detection Criteria:

The detection framework is based on **Azure activity Operation Name** as the static field, which specifies the operation being analyzed. The dynamic field, **Azure activity Caller**, identifies the user or entity executing the operation. Anomalies are flagged when operations typically restricted to certain roles or profiles are attempted by users who do not fit these profiles, indicating possible security breaches or misuse that warrants further investigation.

# DNS BASED THREAT DETECTION

DNS-based threat detection is a crucial cybersecurity mechanism focused on analyzing DNS traffic to identify potential threats and malicious activities. One specific detection mechanism within this domain is DGA (Domain Generation Algorithm) detection

DGAs are used by malware to generate a large number of domain names that serve as rendezvous points with their command and control servers. The ability to detect unusual patterns associated with these algorithmically

generated domains allows organizations to intercept and mitigate malware communications before any harm can be done. By implementing DNS-based DGA detection, organizations enhance their ability to prevent advanced persistent threats and reduce the impact of malware infections.



# DGA Detection

## MITRE ATT&CK Mapping

### □□ TACTICS

Command and Control(TA0011)

Privilege Escalation (TA0004)

Defense Evasion(TA0005)

# 98%



Accuracy

## TECHNIQUES

T1573: Encrypted Channel

T1071: Application Layer Protocol

Domain Generation algorithm (DGA) is an automation technique used by cyber attackers for a variety of attacks like Data exfiltration, command and control, and DNS tunneling and to make it harder for the company's defenses to detect them. Threat actors are always seeking a way to evade the company's defenses. The more progressive their method, the more successful they are in evading security controls that uses static methods. The business must detect such attacks at the beginning stages of the attack life cycle to reduce the impact and the cost of recovery.

## Detection Criteria:


Domain Generation Algorithms (DGA) are used by malware to generate a series of domain names that facilitate elusive communications between infected clients and command and control (C&C) servers. By dynamically producing a list of domains, DGAs allow malware operations to swiftly shift to a new domain if the current one is blocked, thereby bypassing traditional security measures such as domain blacklisting.


The detection challenge is heightened by DGAs that employ dictionary-based methods to create domain names; these DGAs concatenate legitimate-sounding words in various combinations, making the domains appear benign and significantly harder to identify as malicious. To enhance detection capabilities, deep learning neural networks are also employed, leveraging their ability to learn complex patterns and improve the identification of such sophisticated evasion techniques. This advanced approach allows for more effective detection of DGAs, even when they generate domains that closely mimic legitimate ones.



**HAWKEYE**  
HUNTING CYBER ADVERSARIES

---

 [www.hawk-eye.io](http://www.hawk-eye.io)

 +971 4 338 3365

 [hawkeye@dts-solution.com](mailto:hawkeye@dts-solution.com)

---