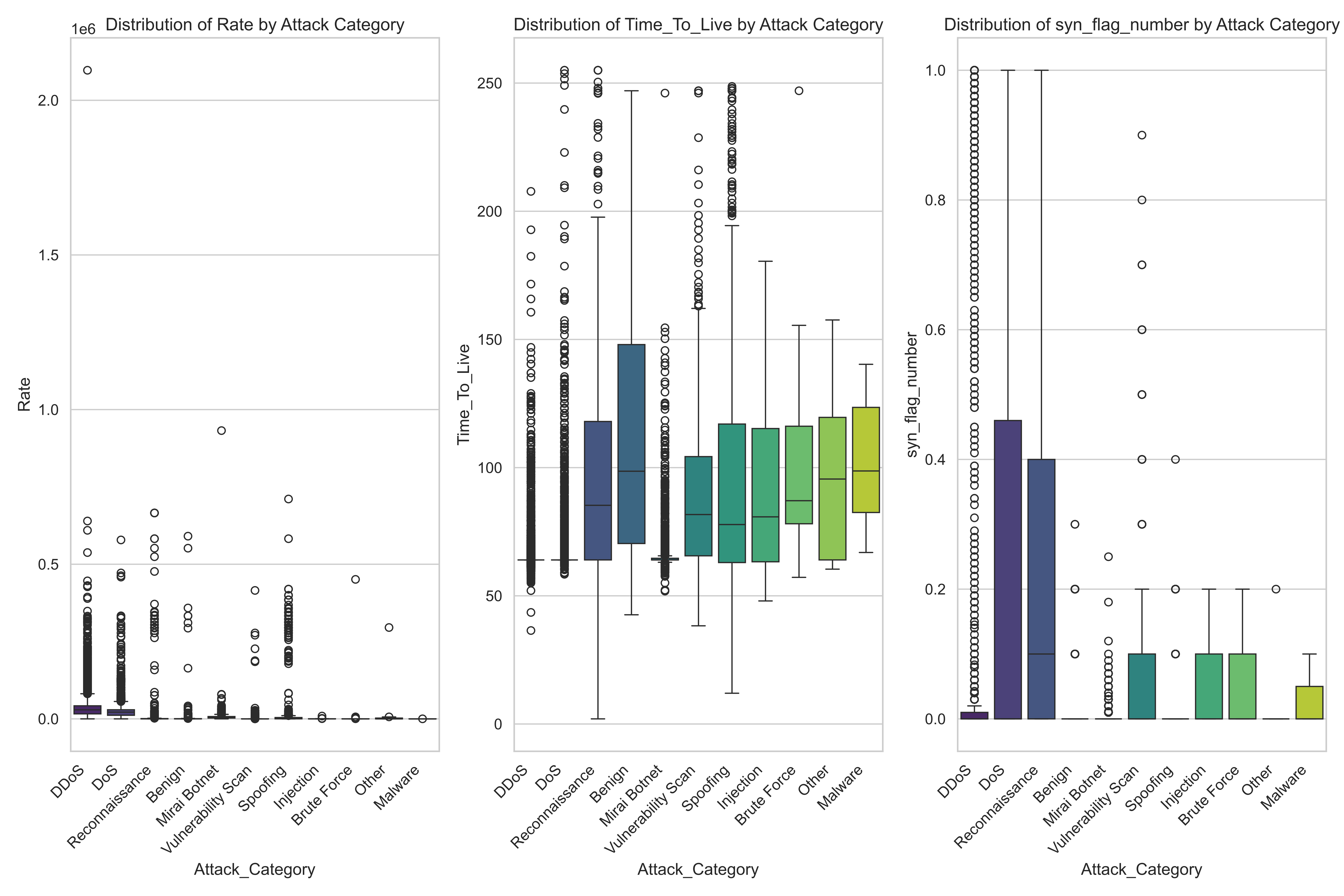
IoT Security Threat Detection for SMEs:

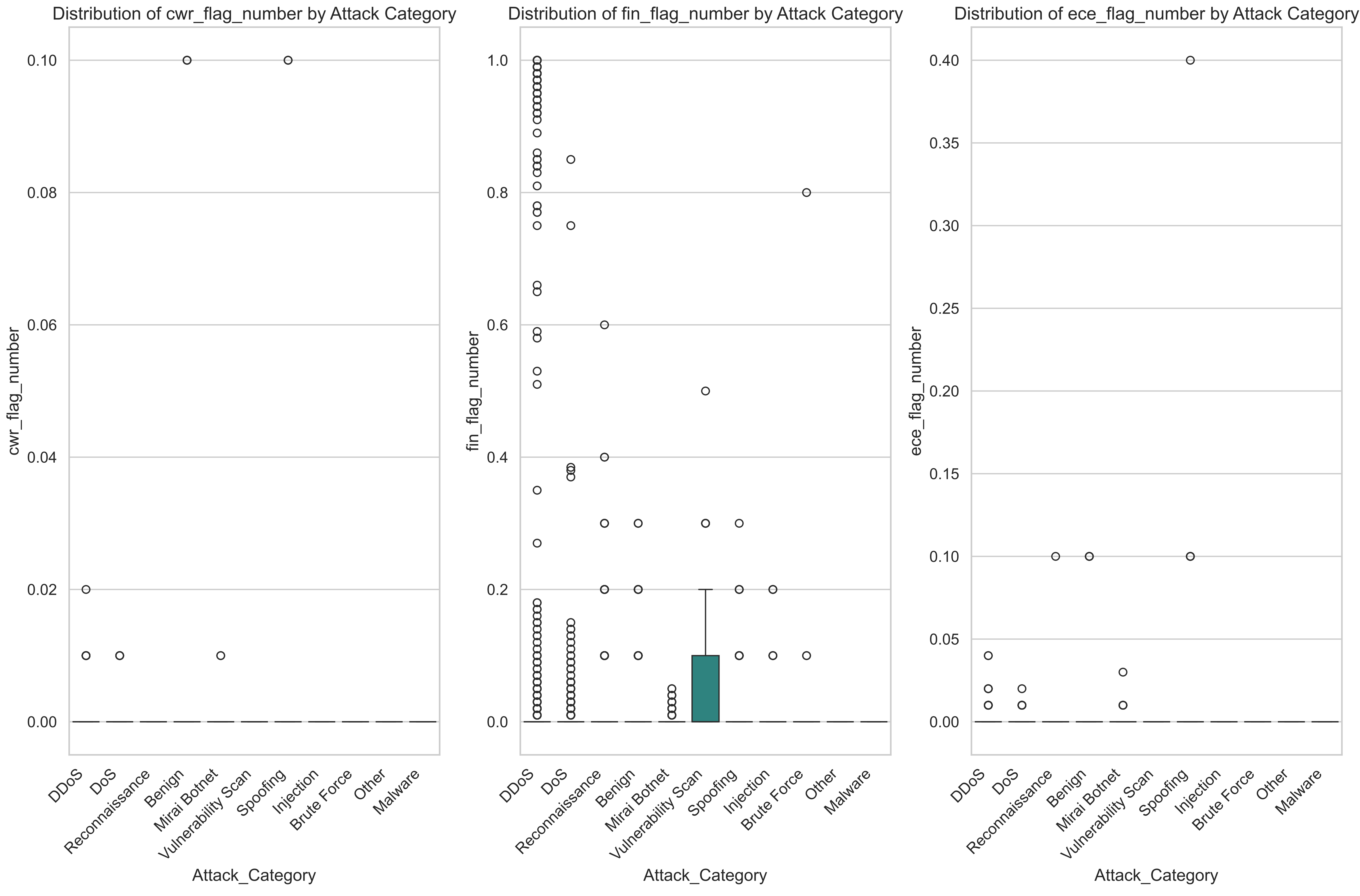
A Machine Learning Approach Using CIC-IoT Dataset

STAGE 3, STEP 2: CORRELATION ANALYSIS

This report analyzes relationships between packet features and attack types, protocol correlations with specific attacks, feature importance for attack categories, and device-specific vulnerability patterns.


Distribution of Rate by Attack Category
1e6
Rate
Distribution of Time_To_Live by Attack Category
Time_To_Live
Distribution of syn_flag_number by Attack Category
syn_flag_number
DDoS
DoS
Reconnaissance
Benign
Mirai Botnet
Vulnerability Scan
Spoofing
Injection
Brute Force
Other
Malware
Attack_Category

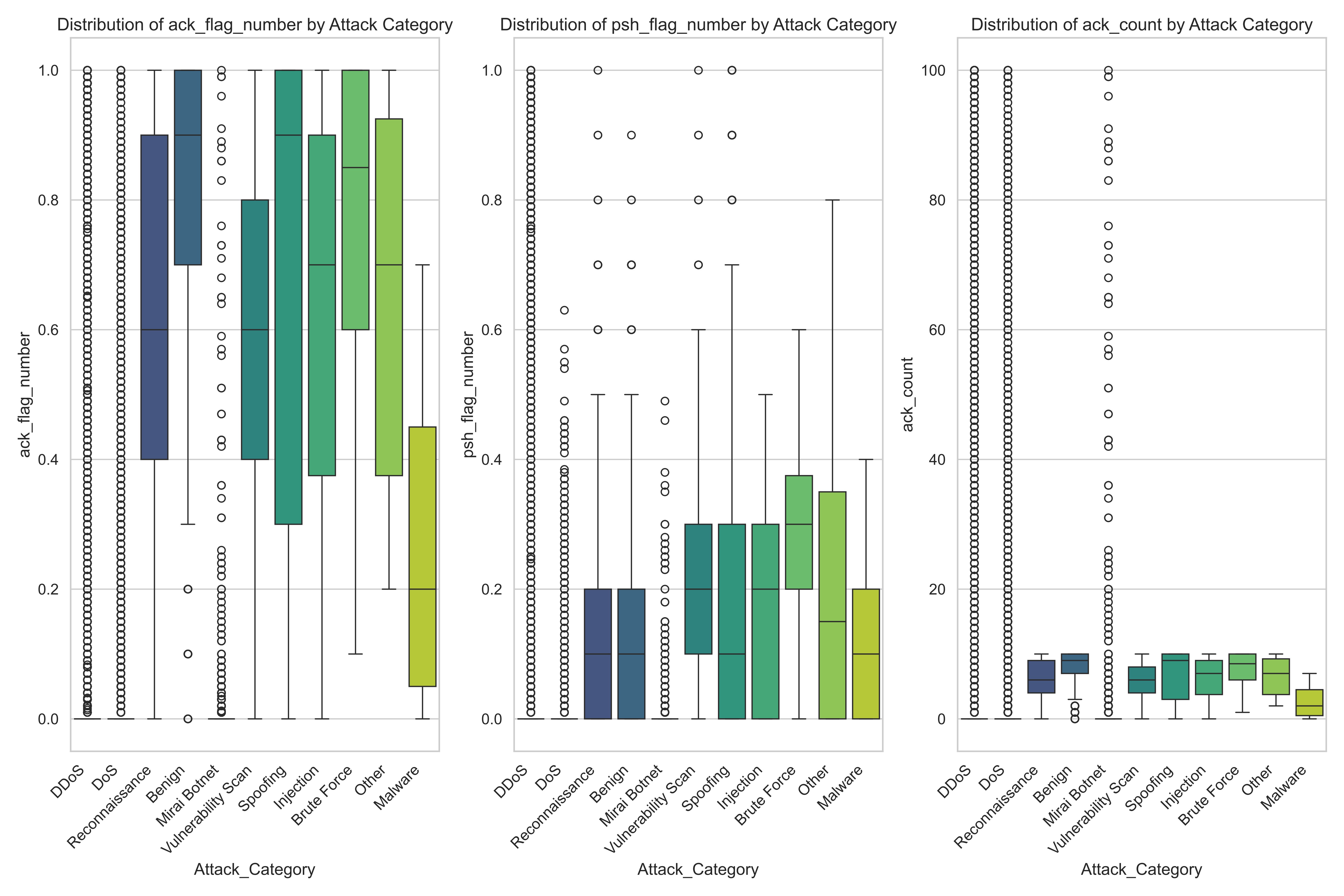
These boxplots show the distribution of Rate, Time_To_Live, syn_flag_number across different attack categories.
Each box shows the median (center line), interquartile range (box boundaries), and outliers (points) for a specific feature within each attack type. The visualizations reveal distinctive patterns in how different attack categories affect network traffic characteristics. For example, DDoS and DoS attacks typically show
extreme values in rate-related features, while reconnaissance attacks display distinctive patterns in flag counts and packet timing. These distributions provide critical insights for SMEs attempting to distinguish normal from malicious traffic. The significant differences in feature distributions between attack categories
demonstrate why targeted detection strategies are more effective than generic approaches. For resource-constrained
SMEs, understanding these distinct patterns can help focus monitoring efforts on the most relevant features for
their specific threat environment.



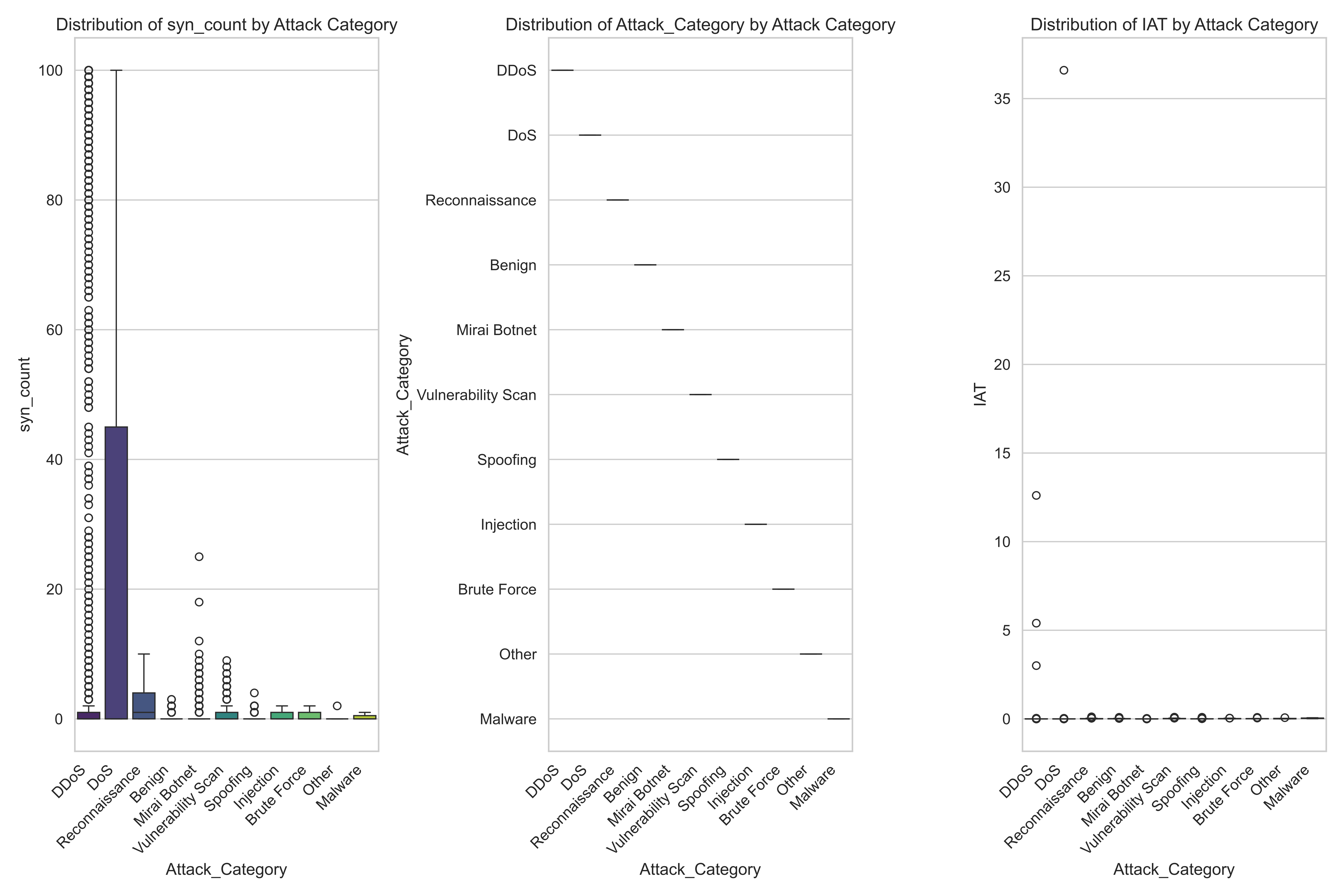
Distribution of cwr_flag_number by Attack Category
Distribution of fin_flag_number by Attack Category
Distribution of ece_flag_number by Attack Category
cwr_flag_number
fin_flag_number
ece_flag_number
0.00
0.02
0.04
0.06
0.08
0.10
0.0
0.2
0.4
0.6
0.8
1.0
0.05
0.15
0.20
0.25
0.30
0.35
0.40
DDoS
DoS
Reconnaissance
Benign
Mirai Botnet
Vulnerability Scan
Spoofing
Injection
Brute Force
Other
Malware
Attack_Category

These boxplots show the distribution of cwr_flag_number, fin_flag_number, ece_flag_number across different attack categories.

Each box shows the median (center line), interquartile range (box boundaries), and outliers (points) for a specific feature within each attack type. The visualizations reveal distinctive patterns in how different attack categories affect network traffic characteristics. For example, DDoS and DoS attacks typically show extreme values in rate-related features, while reconnaissance attacks display distinctive patterns in flag counts and packet timing. These distributions provide critical insights for SMEs attempting to distinguish normal from malicious traffic. The significant differences in feature distributions between attack categories demonstrate why targeted detection strategies are more effective than generic approaches. For resource-constrained SMEs, understanding these distinct patterns can help focus monitoring efforts on the most relevant features for their specific threat environment.

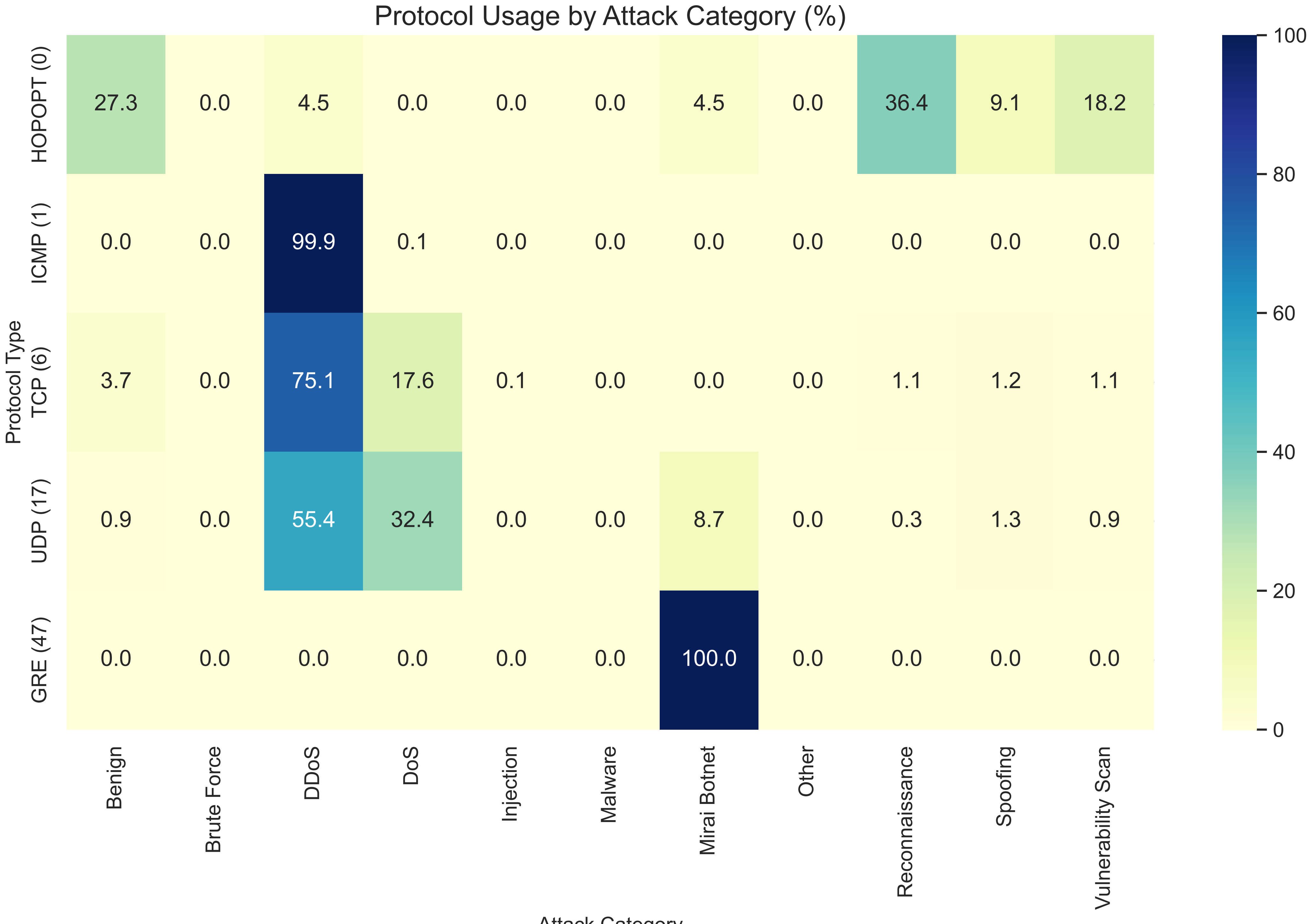

Distribution of ack_flag_number by Attack Category
Distribution of psh_flag_number by Attack Category
Distribution of ack_count by Attack Category
ack_flag_number
psh_flag_number
ack_count
1.0
0.8
0.6
0.4
0.2
0.0
100
80
60
40
20
0
DDoS
DoS
Reconnaissance
Benign
Mirai Botnet
Vulnerability Scan
Spoofing
Injection
Brute Force
Other
Malware
Attack_Category

These boxplots show the distribution of ack_flag_number, psh_flag_number, ack_count across different attack categories.
Each box shows the median (center line), interquartile range (box boundaries), and outliers (points) for a specific feature within each attack type. The visualizations reveal distinctive patterns in how different attack categories affect network traffic characteristics. For example, DDoS and DoS attacks typically show
extreme values in rate-related features, while reconnaissance attacks display distinctive patterns in flag counts and packet timing. These distributions provide critical insights for SMEs attempting to distinguish normal from malicious traffic. The significant differences in feature distributions between attack categories
demonstrate why targeted detection strategies are more effective than generic approaches. For resource-constrained
SMEs, understanding these distinct patterns can help focus monitoring efforts on the most relevant features for
their specific threat environment.



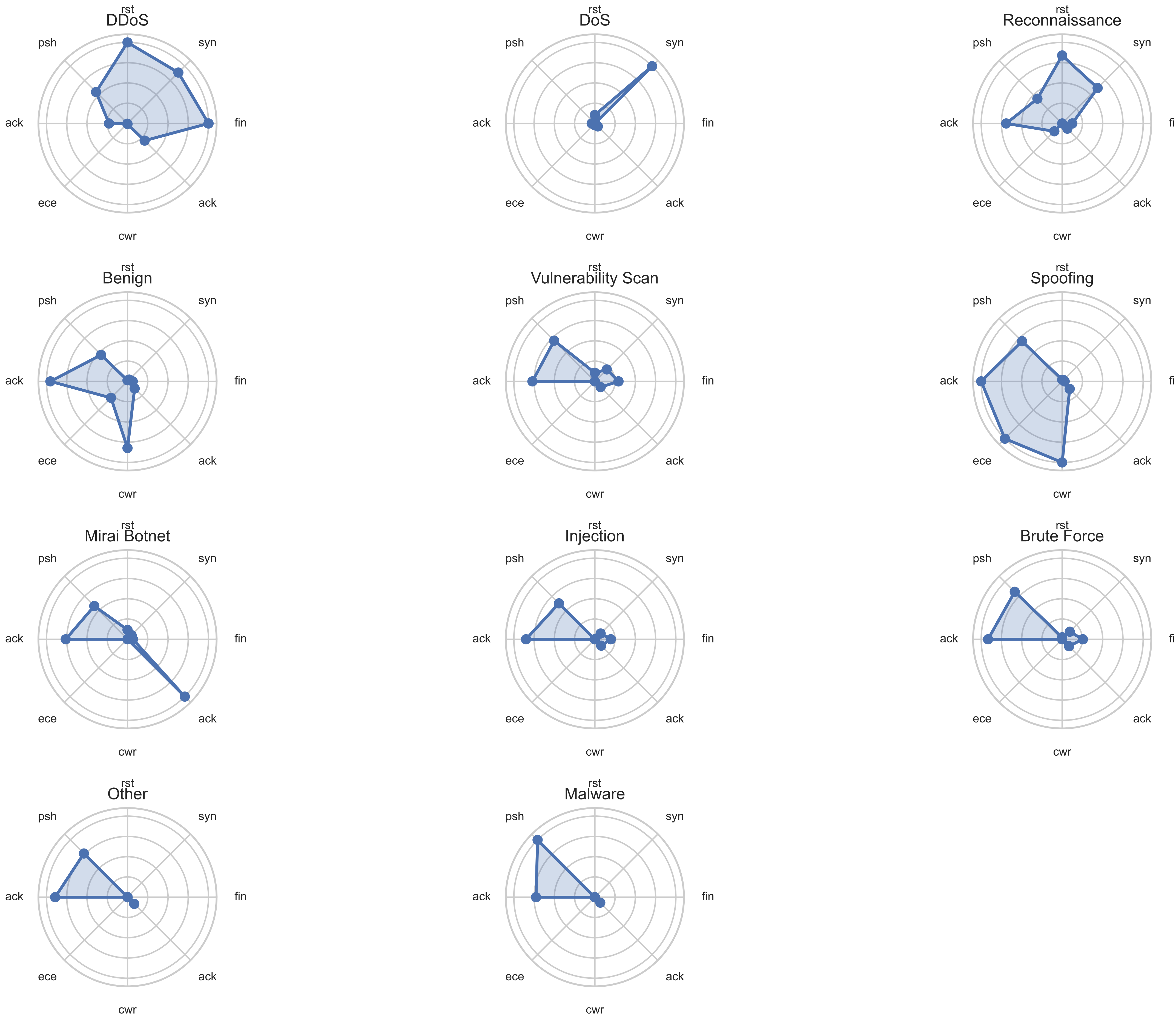
Distribution of syn_count by Attack Category
syn_count
0
20
40
60
80
100
DDoS
DoS
Reconnaissance
Benign
Mirai Botnet
Vulnerability Scan
Spoofing
Injection
Brute Force
Other
Malware
Attack_Category
Distribution of Attack_Category by Attack Category
Attack_Category
Attack_Category
Distribution of IAT by Attack Category
IAT
0
5
10
15
20
25
30
35
Attack_Category

These boxplots show the distribution of syn_count, Attack_Category, IAT across different attack categories.
Each box shows the median (center line), interquartile range (box boundaries), and outliers (points) for a specific feature within each attack type. The visualizations reveal distinctive patterns in how different attack categories affect network traffic characteristics. For example, DDoS and DoS attacks typically show
extreme values in rate-related features, while reconnaissance attacks display distinctive patterns in flag counts and packet timing. These distributions provide critical insights for SMEs attempting to distinguish normal from malicious traffic. The significant differences in feature distributions between attack categories
demonstrate why targeted detection strategies are more effective than generic approaches. For resource-constrained
SMEs, understanding these distinct patterns can help focus monitoring efforts on the most relevant features for
their specific threat environment.

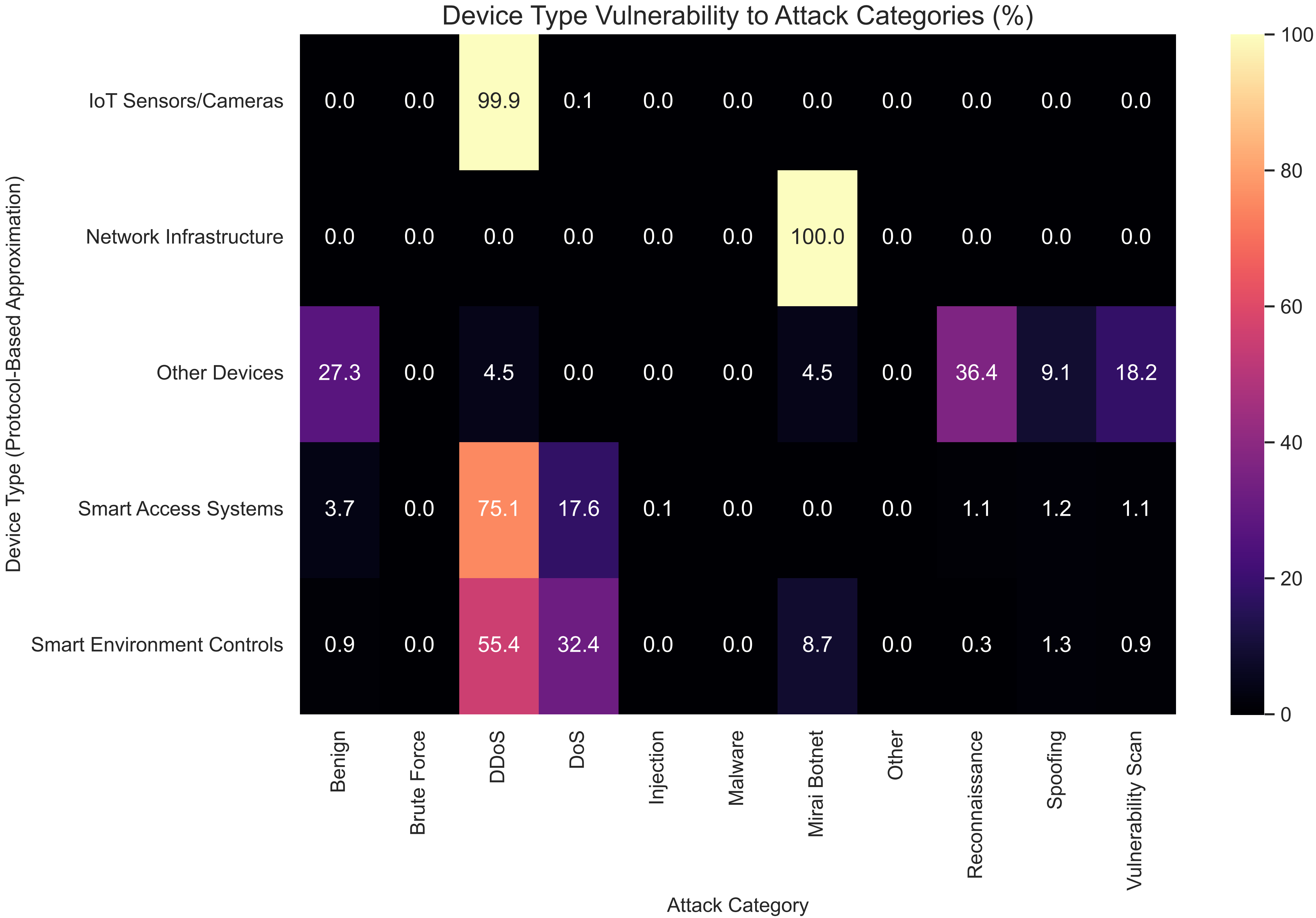


Protocol Usage by Attack Category (%)
Protocol Type
HOPOPT (0)
ICMP (1)
TCP (6)
UDP (17)
GRE (47)
Attack Category
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan
27.3 0.0 4.5 0.0 0.0 0.0 4.5 0.0 36.4 9.1 18.2
0.0 0.0 99.9 0.1 0.0 0.0 0.0 0.0 0.0 0.0 0.0
3.7 0.0 75.1 17.6 0.1 0.0 0.0 0.0 1.1 1.2 1.1
0.9 0.0 55.4 32.4 0.0 0.0 8.7 0.0 0.3 1.3 0.9
0.0 0.0 0.0 0.0 0.0 0.0 100.0 0.0 0.0 0.0 0.0
100
80
60
40
20
0

This heatmap illustrates the relationship between network protocols and attack categories, showing what percentage of traffic for each protocol belongs to different attack types. The color intensity and annotation values represent the percentage distribution. This visualization reveals clear protocol preferences for certain attack types - for example, DDoS attacks heavily utilize ICMP (protocol 1), while reconnaissance activities predominantly use TCP (protocol 6). For SMEs implementing security monitoring, this analysis provides crucial guidance on which protocols to monitor for specific threat types. It also demonstrates why protocol-specific security controls are important - a one-size-fits-all approach would miss the protocol-specific patterns that distinguish different attack categories. By understanding these relationships, SMEs can implement more targeted protocol filtering and monitoring rules, optimizing their security resources for their specific threat landscape.

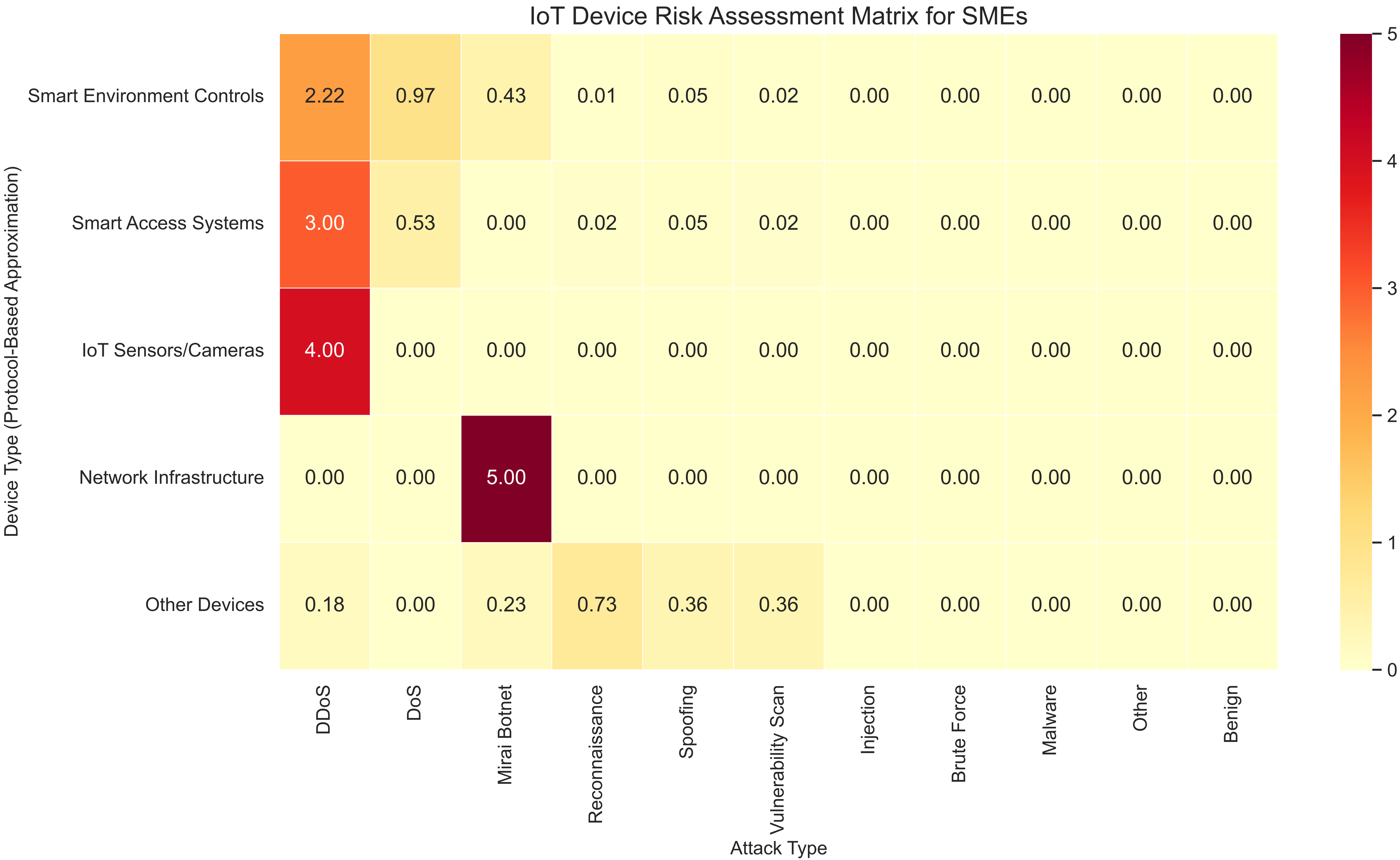

DDoS
DoS
Reconnaissance
Benign
Vulnerability Scan
Spoofing
Mirai Botnet
Injection
Brute Force
Other
Malware
rst
syn
fin
ack
cwr
ece
ack
psh

These radar charts display the normalized TCP flag usage patterns for different attack categories, highlighting the distinctive "fingerprints" of various attacks at the protocol level. Each chart shows how a specific attack category utilizes different TCP flags relative to other categories. For example, reconnaissance attacks typically show higher RST flag usage, while DDoS attacks may show elevated SYN flags in SYN flood scenarios. These visualizations reveal how attackers manipulate protocol mechanics to achieve their goals, creating identifiable signatures that can be used for detection. For SMEs implementing network security monitoring, these protocol-specific patterns provide valuable detection rules that can be implemented in firewalls or intrusion detection systems. Understanding these patterns also helps security teams distinguish between normal protocol behavior and potentially malicious activity, improving detection accuracy while reducing false positives.


Device Type Vulnerability to Attack Categories (%)
Device Type (Protocol-Based Approximation)
IoT Sensors/Cameras
Network Infrastructure
Other Devices
Smart Access Systems
Smart Environment Controls
Attack Category
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan
0.0 0.0 99.9 0.1 0.0 0.0 0.0 0.0 0.0 0.0 0.0
0.0 0.0 0.0 0.0 0.0 0.0 100.0 0.0 0.0 0.0 0.0
27.3 0.0 4.5 0.0 0.0 0.0 4.5 0.0 36.4 9.1 18.2
3.7 0.0 75.1 17.6 0.1 0.0 0.0 0.0 1.1 1.2 1.1
0.9 0.0 55.4 32.4 0.0 0.0 8.7 0.0 0.3 1.3 0.9
0
20
40
60
80
100

This heatmap shows the vulnerability patterns of different device types to various attack categories, based on protocol usage as a proxy for device classification. The percentages and color intensity indicate what proportion of traffic for each device type is associated with different attack categories. For example, IoT sensors and cameras (approximated by ICMP-heavy devices) show higher vulnerability to DDoS attacks, while smart access systems (TCP-based devices) are more targeted by reconnaissance attacks. This analysis helps SMEs understand which devices in their environment are most vulnerable to specific threats, enabling more targeted security controls. For resource-constrained organizations, this information is valuable for prioritizing security investments and monitoring attention to the most vulnerable systems. The visualization also highlights that different IoT device types have distinctly different risk profiles, emphasizing the need for device-specific security approaches

rather than uniform controls across all IoT systems.


IoT Device Risk Assessment Matrix for SMEs
Device Type (Protocol-Based Approximation)
Smart Environment Controls
Smart Access Systems
IoT Sensors/Cameras
Network Infrastructure
Other Devices
2.22
0.97
0.43
0.01
0.05
0.02
0.00
3.00
0.53
0.02
4.00
5.00
0.18
0.23
0.73
0.36
DDoS
DoS
Mirai Botnet
Reconnaissance
Spoofing
Vulnerability Scan
Injection
Brute Force
Malware
Other
Benign
Attack Type
0
1
2
3
4
5

This risk assessment matrix provides a comprehensive view of IoT device vulnerabilities in SME environments, combining attack frequency and severity to calculate risk scores. The color intensity and numerical values represent the relative risk level, with darker colors indicating higher risk. This visualization reveals which device types are most vulnerable to specific high-impact attacks, helping SMEs prioritize their security efforts. For example, network infrastructure devices may show elevated risk for DDoS attacks, while smart access systems might display higher vulnerability to spoofing or brute force attempts. For SME decision-makers, this matrix translates complex security data into actionable insights, enabling informed security investment decisions. The matrix can guide resource allocation, helping organizations focus their limited security resources on protecting the most vulnerable devices against their highest-risk threats, rather than attempting to implement comprehensive security across all systems simultaneously.