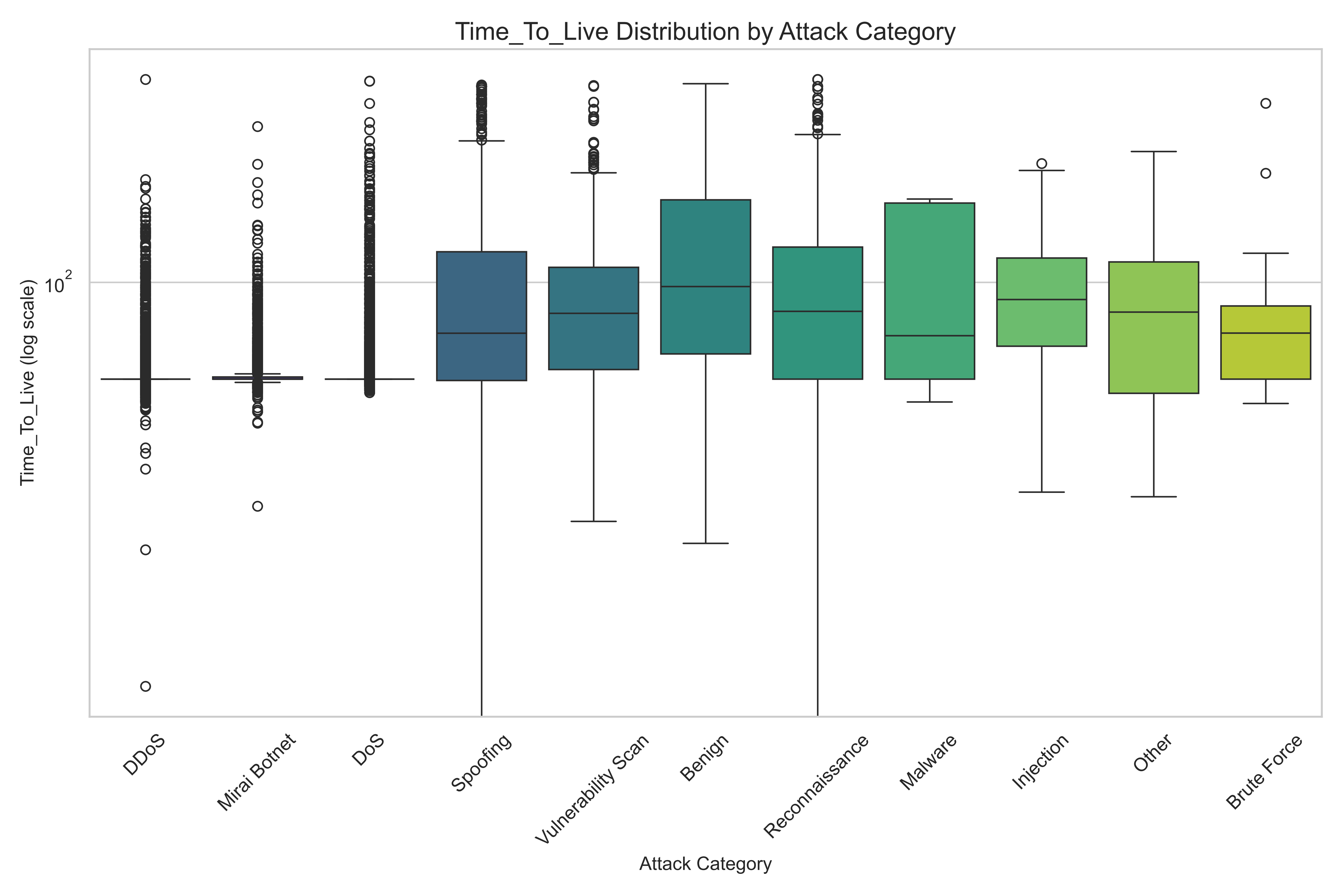
IoT Security Threat Detection for SMEs:

A Machine Learning Approach Using CIC-IoT Dataset

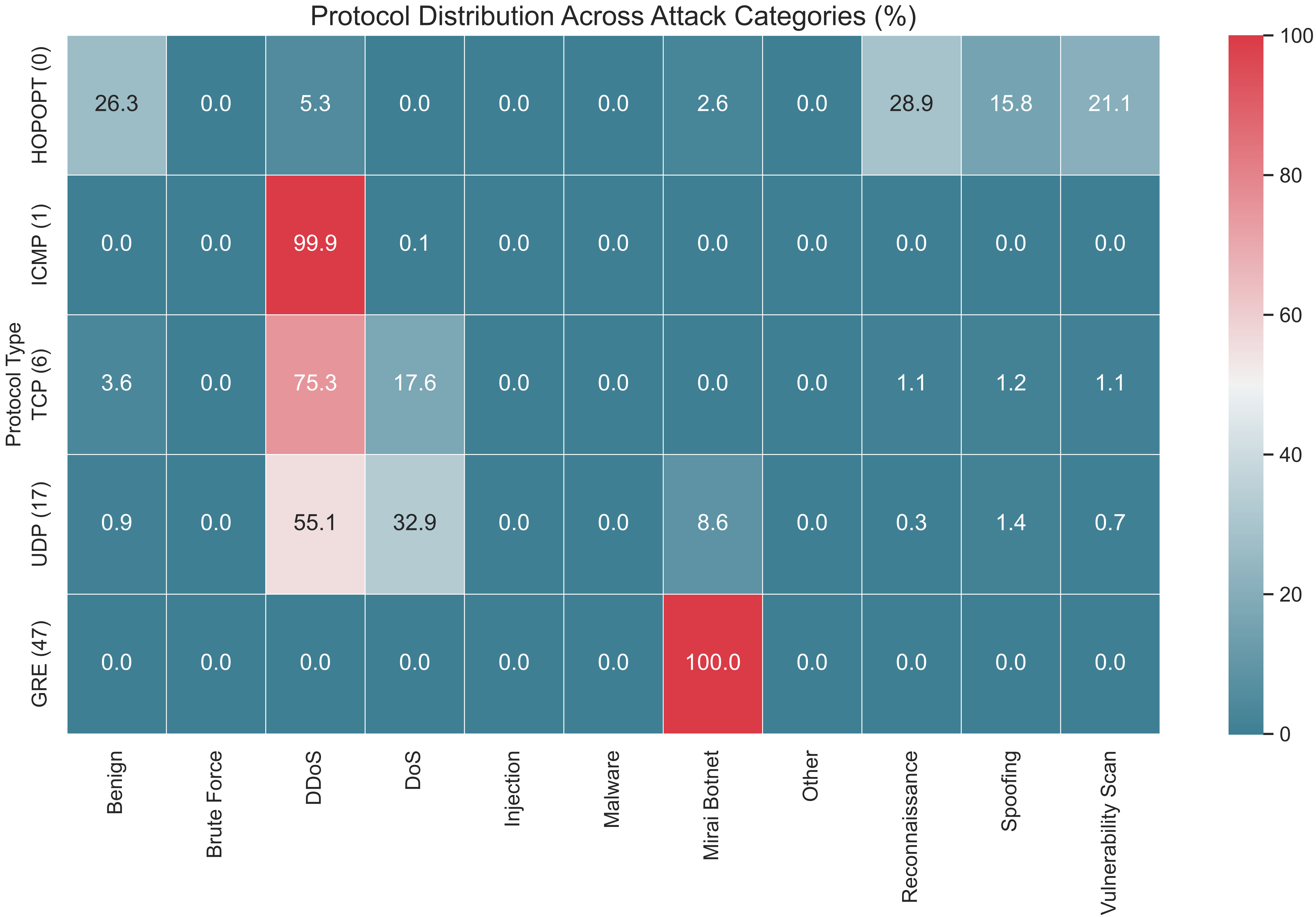
STAGE 1, STEP 3: CRITICAL METRICS IDENTIFICATION

This report identifies and analyzes key network metrics for IoT security threat detection, focusing on both primary indicators and secondary validation metrics that are most relevant for SME environments.



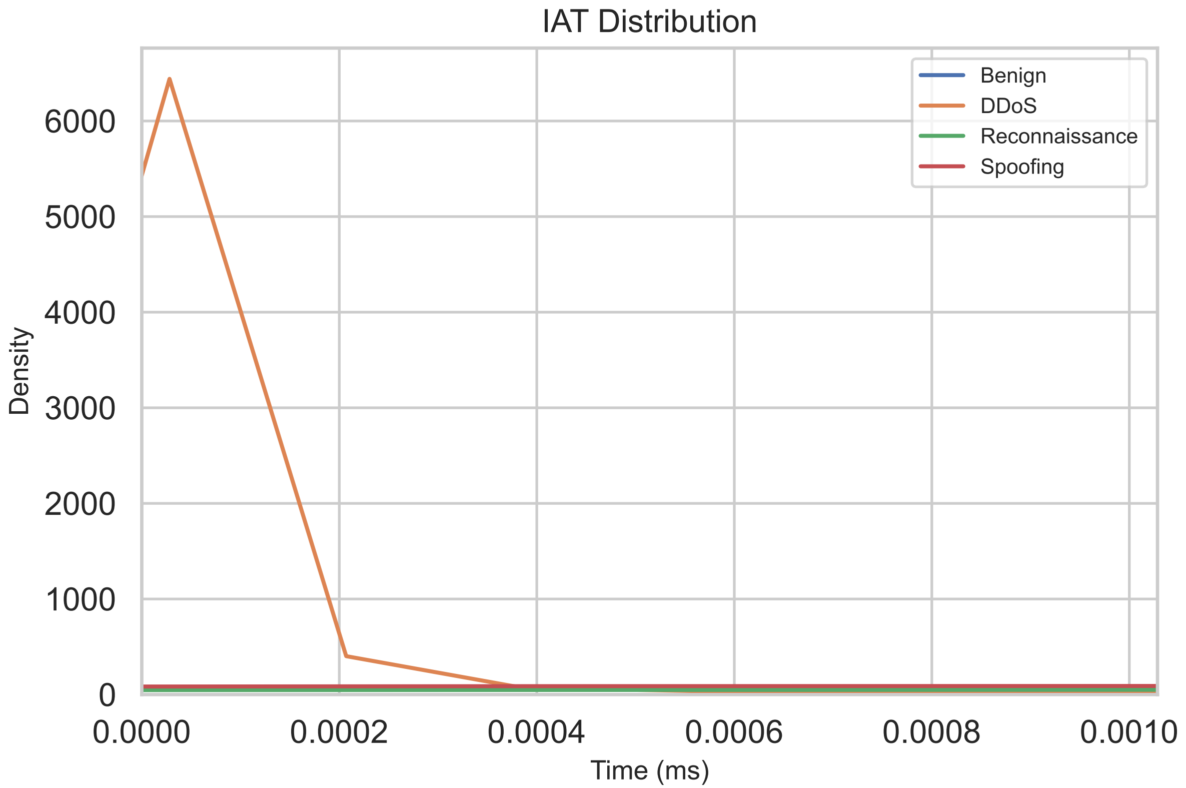
Time_To_Live Distribution by Attack Category
Time_To_Live (log scale)
10^2
DDoS
Mirai Botnet
DoS
Spoofing
Vulnerability Scan
Benign
Reconnaissance
Malware
Injection
Other
Brute Force
Attack Category

This boxplot illustrates the distribution of Time_To_Live across different attack categories in IoT network traffic.
Flow duration is a critical primary indicator as it captures how long network connections persist, which varies
significantly between normal and malicious traffic. The logarithmic scale accommodates the wide range of durations
observed. As shown, DDoS and DoS attacks typically exhibit shorter flow durations due to their rapid connection
establishment and termination patterns, while reconnaissance activities often show longer durations as they probe
systems methodically. For SMEs with limited security resources, monitoring flow duration provides an efficient
method to identify potential threats, as significant deviations from baseline patterns often indicate suspicious
activity. This metric is particularly valuable because it requires minimal computational resources to track,
making it suitable for resource-constrained IoT environments common in smaller businesses.

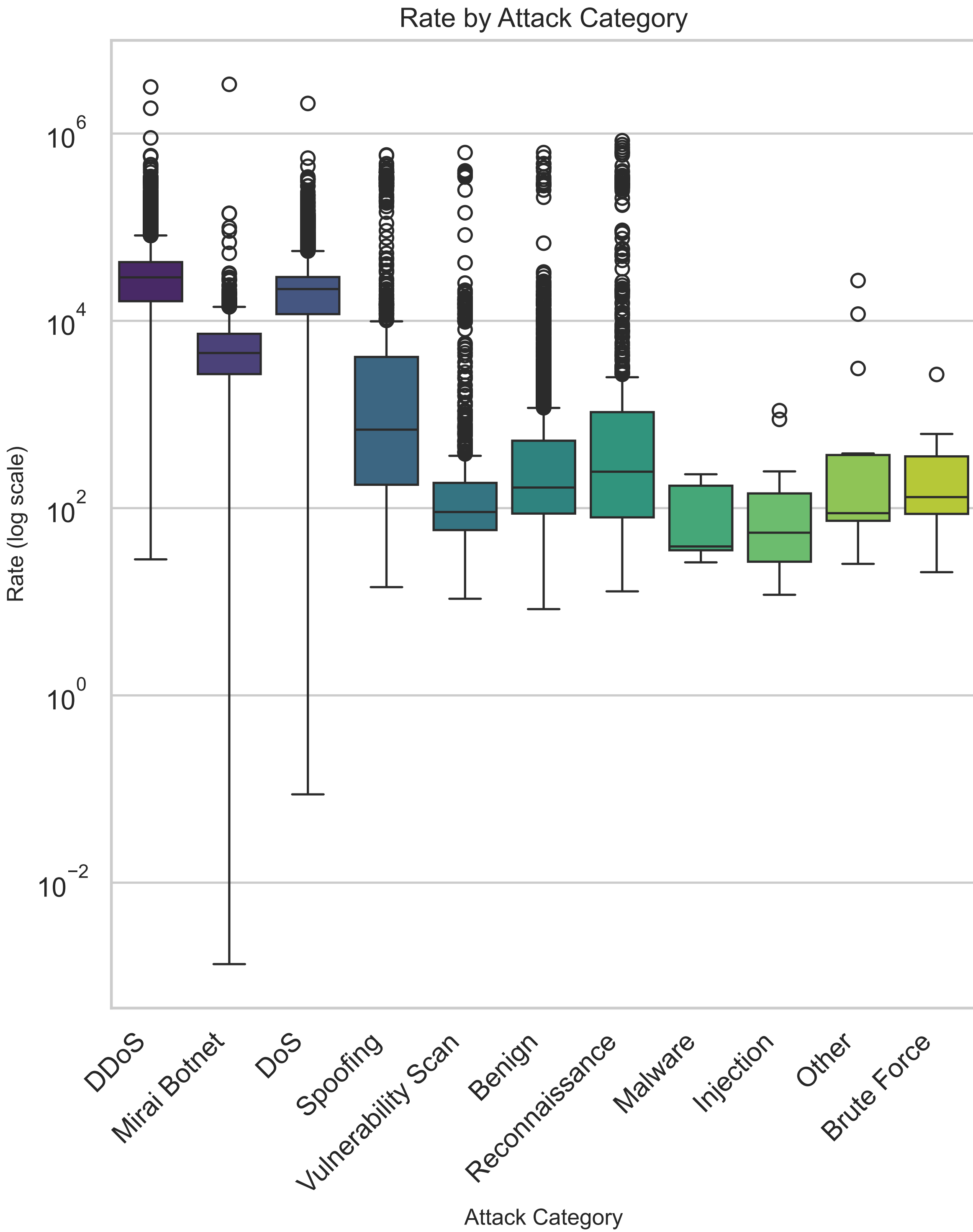

Protocol Distribution Across Attack Categories (%)
Protocol Type
HOPOPT (0)
ICMP (1)
TCP (6)
UDP (17)
GRE (47)
26.3
0.0
5.3
0.0
0.0
0.0
2.6
0.0
28.9
15.8
21.1
0.0
0.0
99.9
0.1
0.0
0.0
0.0
0.0
0.0
0.0
0.0
3.6
0.0
75.3
17.6
0.0
0.0
0.0
0.0
1.1
1.2
1.1
0.9
0.0
55.1
32.9
0.0
0.0
8.6
0.0
0.3
1.4
0.7
0.0
0.0
0.0
0.0
0.0
0.0
100.0
0.0
0.0
0.0
0.0
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan
Attack Category
100
80
60
40
20
0

This heatmap reveals the protocol distribution across different attack categories, showing what percentage of each protocol's traffic is associated with specific attack types. The color intensity represents the percentage of traffic, with annotations showing exact values. This visualization highlights how certain attacks prefer specific protocols - for example, DDoS attacks heavily utilize ICMP (protocol 1), while reconnaissance activities predominantly use TCP (protocol 6). Protocol distribution analysis is a primary indicator that helps SMEs understand which protocols may need additional monitoring in their environments.

For resource-constrained organizations, this information enables targeted protocol filtering and security controls, focusing resources where threats are most likely to manifest. By monitoring unusual shifts in protocol distribution, SMEs can detect potential attacks before they fully develop, even with limited security infrastructure.

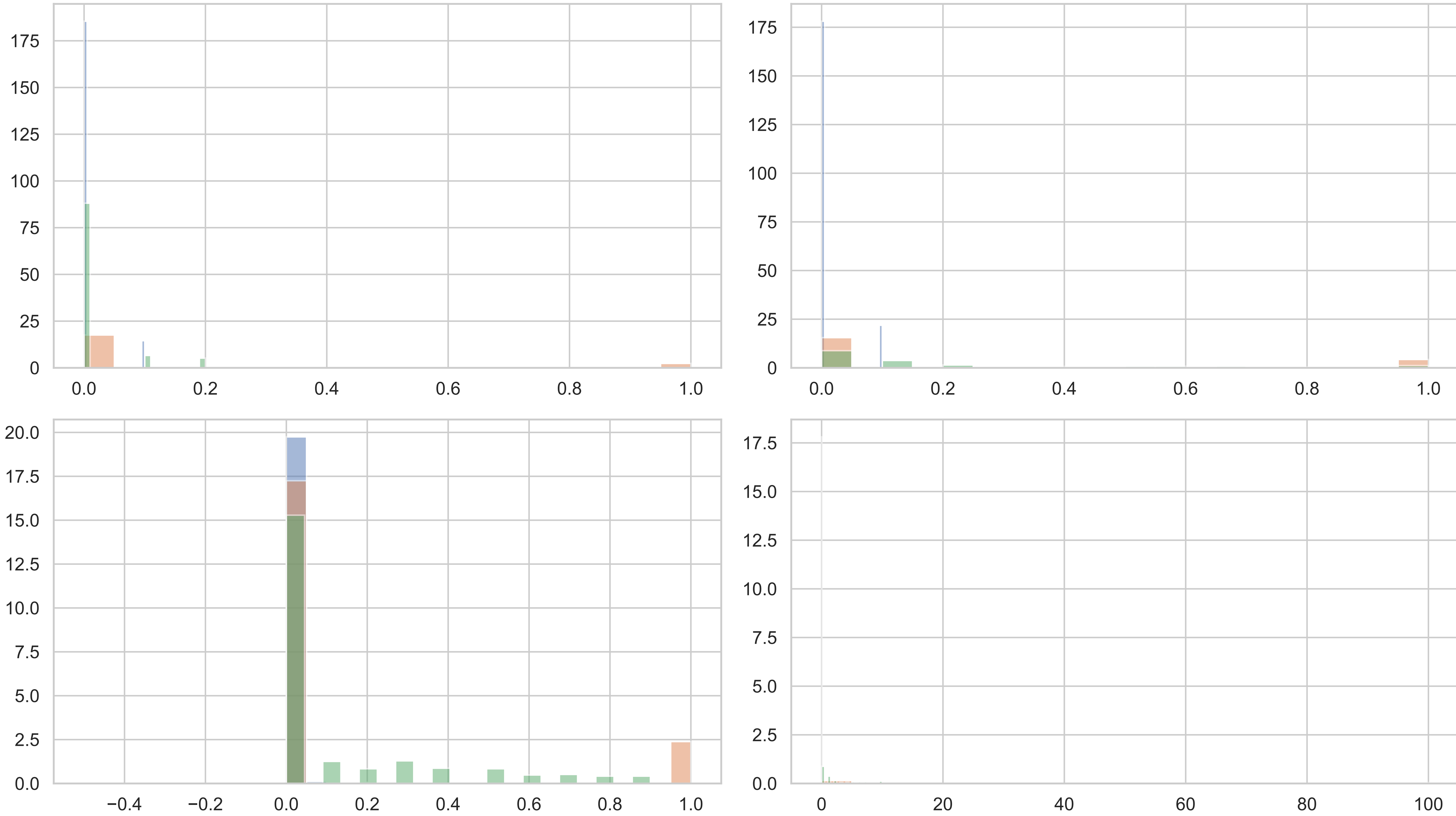

IAT Distribution
Benign
DDoS
Reconnaissance
Spoofing
Density
6000
5000
4000
3000
2000
1000
0
0.0000
0.0002
0.0004
0.0006
0.0008
0.0010
Time (ms)

These density plots show the distribution of various inter-arrival time (IAT) metrics across different attack categories. IAT measurements capture the time between consecutive packets, revealing the temporal patterns of network traffic. The plots demonstrate how different attack types exhibit characteristic timing signatures - DDoS attacks typically show a concentrated distribution with very short IATs (rapid packet transmission), while reconnaissance activities often display more dispersed patterns. Normal benign traffic generally shows a wider, more natural distribution of packet timing. For SMEs, monitoring packet timing characteristics provides a powerful method for detecting anomalous traffic patterns, even when packet contents appear legitimate. These timing-based metrics can be implemented with minimal computational overhead, making them ideal for resource-constrained environments. Changes in these distributions often serve as early warning indicators of potential security threats.

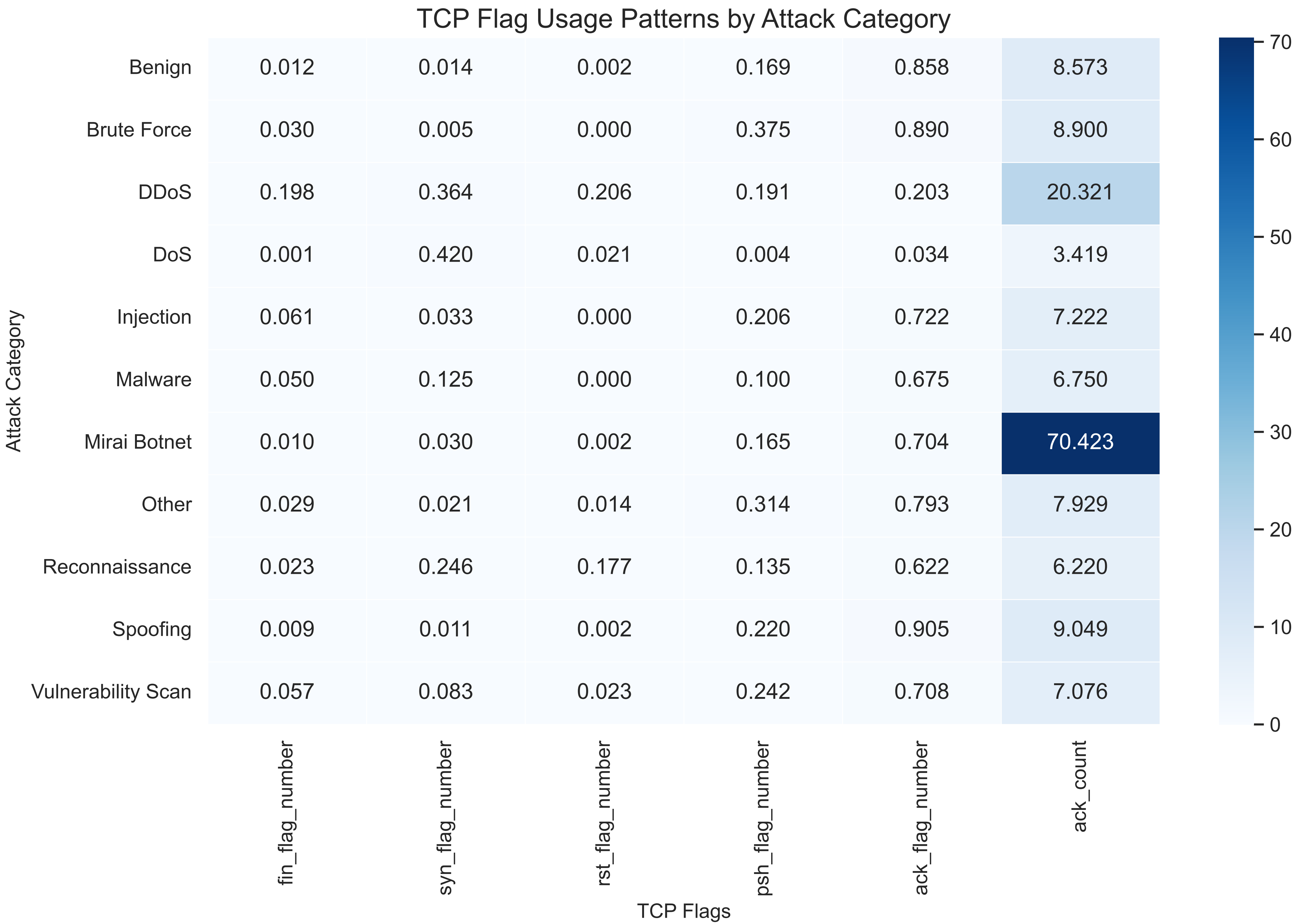


Rate by Attack Category
Rate (log scale)
10^6
10^4
10^2
10^0
10^{-2}
DDoS
Mirai Botnet
DoS
Spoofing
Vulnerability Scan
Benign
Reconnaissance
Malware
Injection
Other
Brute Force
Attack Category

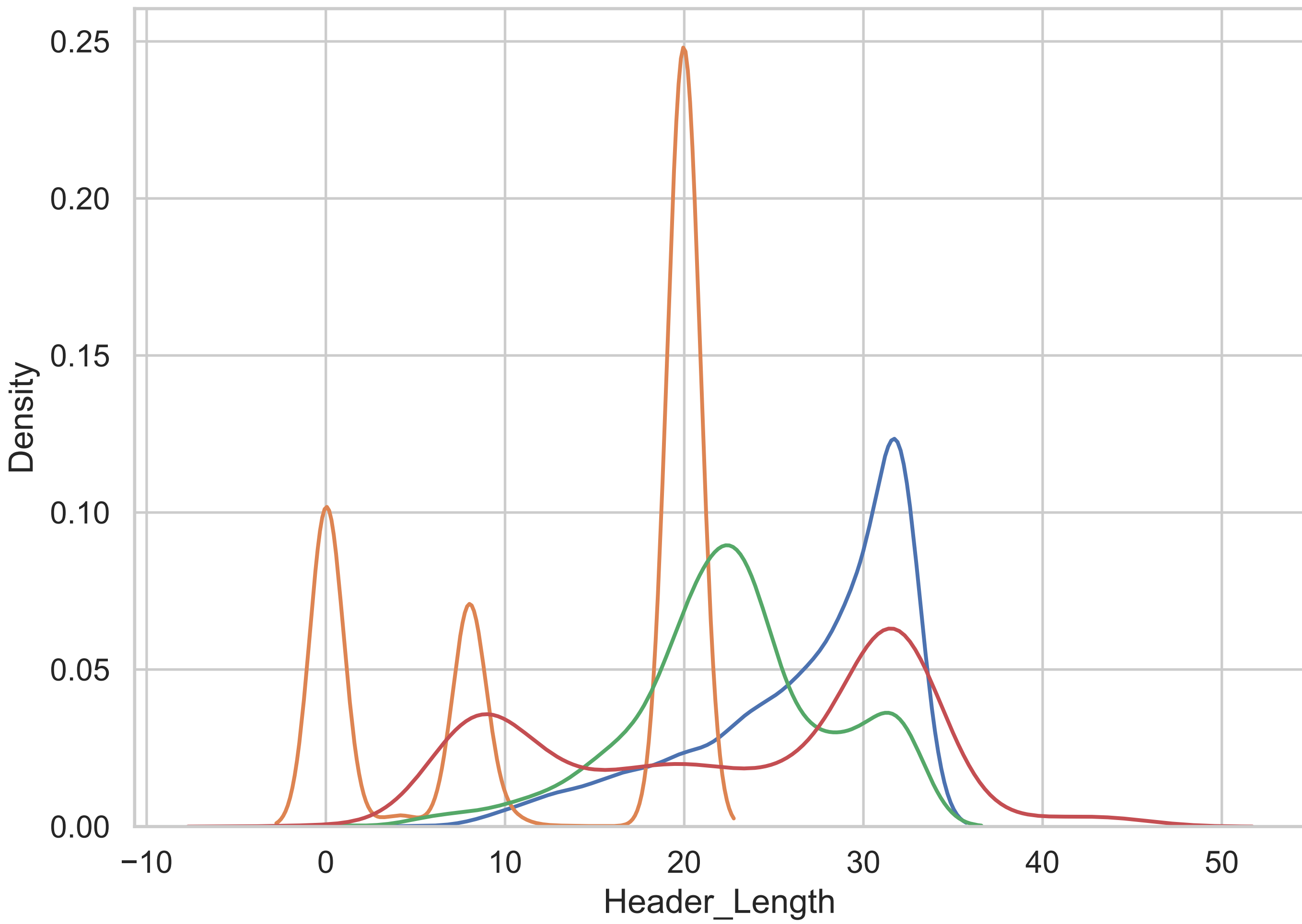
These boxplots illustrate bandwidth consumption patterns across different attack categories, displayed on a logarithmic scale to accommodate the wide range of values. Bandwidth metrics, such as Flow Bytes/s and Flow Packets/s, reveal the volume and intensity of network traffic. The visualization shows that DoS and DDoS attacks typically exhibit extremely high bandwidth consumption (visible as elevated boxes and numerous outliers), aligning with their goal of overwhelming target systems. In contrast, reconnaissance and injection attacks operate at much lower volumes to avoid detection. For SMEs, these bandwidth consumption patterns serve as critical indicators for identifying volumetric attacks that could disrupt business operations. By establishing baseline bandwidth patterns for normal operations, even small organizations can configure simple thresholds to alert on suspicious traffic volumes, providing an effective first line of defense against the most common IoT attacks.


0
25
50
75
100
125
150
175
0.0
0.2
0.4
0.6
0.8
1.0
0
25
50
75
100
125
150
175
0.0
0.2
0.4
0.6
0.8
1.0
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
−0.4
−0.2
0.0
0.2
0.4
0.6
0.8
1.0
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
0
20
40
60
80
100

These histograms demonstrate connection establishment patterns across different attack categories, focusing on TCP connection control flags and related metrics. Connection establishment patterns reveal how different attack types manipulate the TCP handshake process and connection state transitions. For example, SYN flood attacks show distinctively high SYN flag counts without corresponding completion flags, while port scanning activities in reconnaissance attacks often display elevated RST flags as closed ports respond to probes. These patterns serve as valuable secondary validation metrics that help confirm suspicious activities detected by primary indicators. For SMEs, analyzing these connection patterns provides depth to threat detection capabilities, reducing false positives by requiring anomalies in both primary indicators and these validation metrics before triggering alerts. This layered approach is particularly important for smaller organizations where false alarms can quickly overwhelm limited security resources.

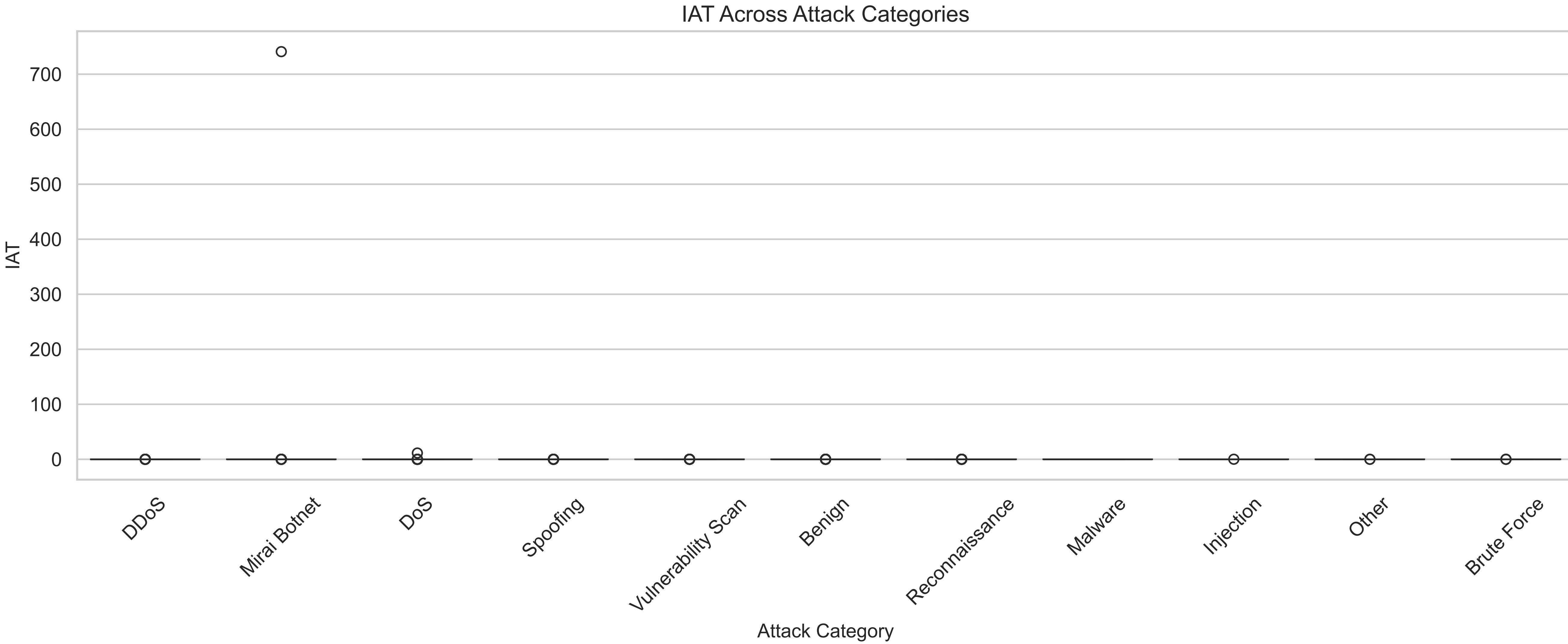

TCP Flag Usage Patterns by Attack Category
Attack Category
TCP Flags
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan
fin_flag_number
syn_flag_number
rst_flag_number
psh_flag_number
ack_flag_number
ack_count
0.012 0.014 0.002 0.169 0.858 8.573
0.030 0.005 0.000 0.375 0.890 8.900
0.198 0.364 0.206 0.191 0.203 20.321
0.001 0.420 0.021 0.004 0.034 3.419
0.061 0.033 0.000 0.206 0.722 7.222
0.050 0.125 0.000 0.100 0.675 6.750
0.010 0.030 0.002 0.165 0.704 70.423
0.029 0.021 0.014 0.314 0.793 7.929
0.023 0.246 0.177 0.135 0.622 6.220
0.009 0.011 0.002 0.220 0.905 9.049
0.057 0.083 0.023 0.242 0.708 7.076
0
10
20
30
40
50
60
70

This heatmap illustrates TCP flag usage patterns across different attack categories, with color intensity and numerical values indicating the average flag counts per flow. TCP flags are crucial security indicators because they reveal how attackers manipulate protocol mechanics to achieve their objectives. The visualization shows distinctive flag patterns for different attack types - for example, the elevated SYN counts in DDoS attacks indicate SYN flooding techniques, while the unique combinations of flags in reconnaissance attacks reveal their probing methodologies. For SMEs implementing network security monitoring, these flag patterns provide precise signatures that can be translated into detection rules with minimal false positives. By monitoring for these specific flag combinations, even organizations with limited security resources can implement targeted detection mechanisms for the most common attack types, maximizing the effectiveness of their security controls while minimizing implementation complexity.



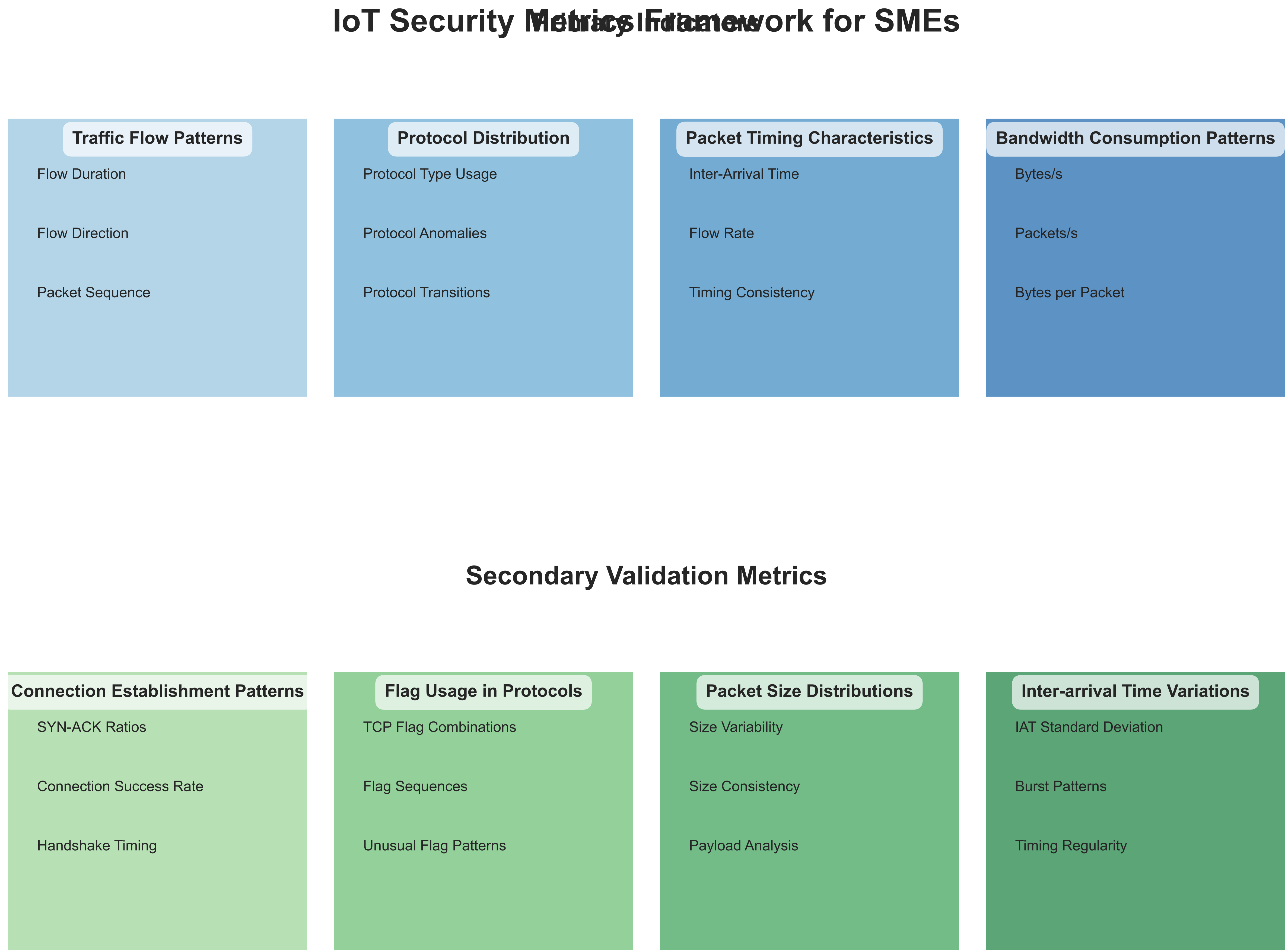
0.25
0.20
0.15
0.10
0.05
0.00
Density
−10
0
10
20
30
40
50
Header_Length

These density plots reveal packet size distributions across different attack categories for various packet length metrics. Packet size distributions serve as valuable secondary validation metrics because they capture the payload characteristics of different attack types. As shown in the visualization, DDoS attacks often display distinctive size patterns, frequently using either very small packets to maximize connection overhead or specifically crafted packet sizes to amplify the attack. Reconnaissance activities typically show different distributions focused on small probe packets, while data exfiltration attacks may exhibit unusual large packet sizes. For SMEs, monitoring packet size distributions provides a complementary detection approach that works effectively alongside timing and protocol metrics. This metric helps identify attacks that might maintain normal timing patterns but use unusual packet sizes to achieve their objectives. These distributions can be monitored with minimal processing overhead, making them suitable for resource-constrained environments.

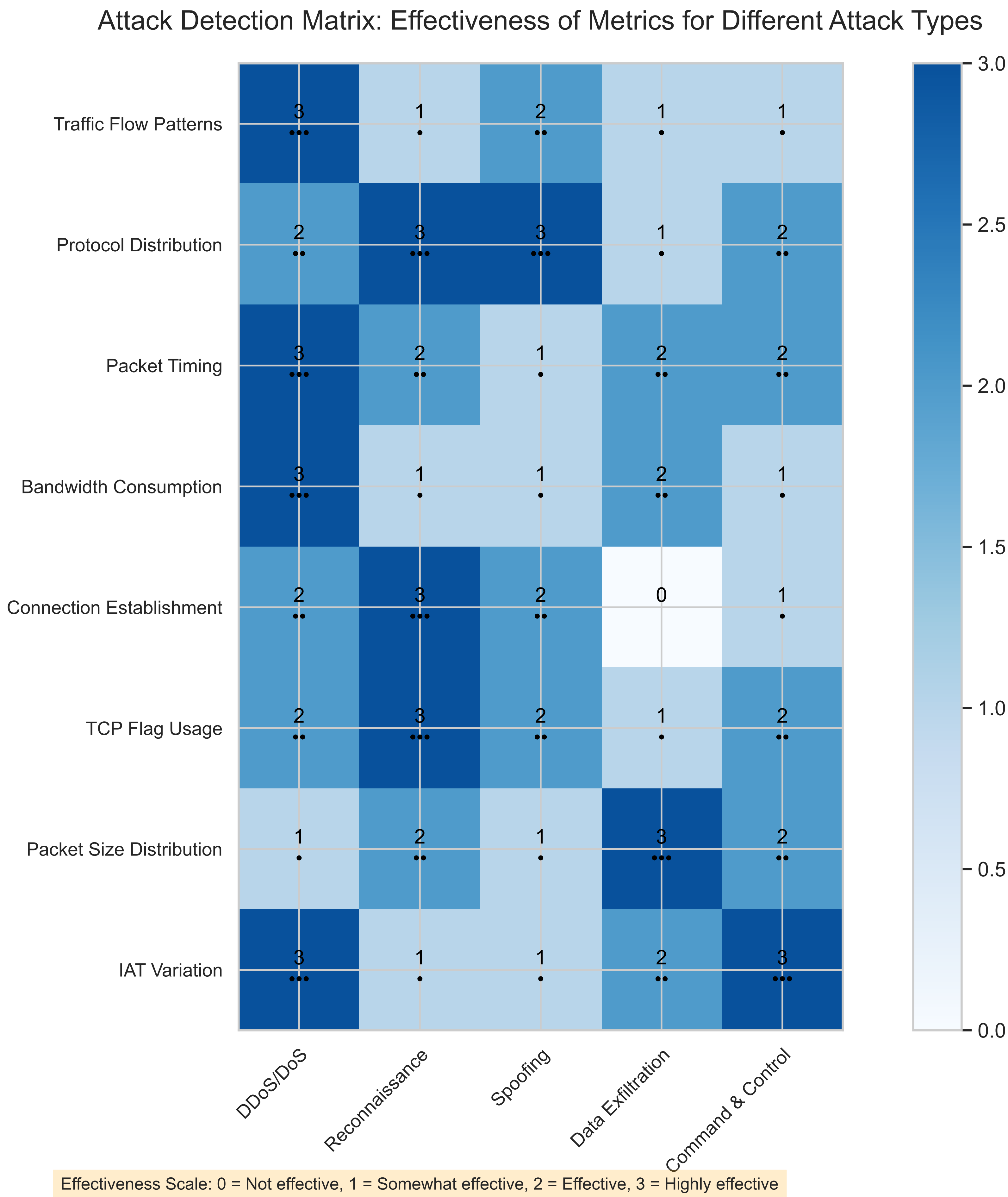

IAT Across Attack Categories
IAT
700
600
500
400
300
200
100
0
DDoS
Mirai Botnet
DoS
Spoofing
Vulnerability Scan
Benign
Reconnaissance
Malware
Injection
Other
Brute Force
Attack Category

These visualizations analyze inter-arrival time (IAT) variations across attack categories, combining boxplots and
statistical comparisons. IAT variations reveal the consistency or irregularity of packet timing, which differs significantly between normal traffic and various attack types. The main boxplot shows how the distribution of IAT
values varies across attack categories, while the bar charts compare mean, median, and standard deviation statistics.

This analysis reveals that DDoS attacks typically exhibit low IAT variation due to their consistent, automated
packet generation, while benign traffic shows natural variability reflecting human-driven usage patterns. For SMEs,
monitoring IAT variations provides a robust method for detecting automated attacks even when they attempt to mimic
normal traffic volumes. This metric helps identify sophisticated attacks that might evade simple volume-based
detection methods. IAT variation analysis complements other metrics by focusing on the regularity of traffic patterns
rather than just their volume or content, creating a more comprehensive detection approach.


IoT Security Metrics Framework for SMEs
Traffic Flow Patterns
Flow Duration
Flow Direction
Packet Sequence
Protocol Distribution
Protocol Type Usage
Protocol Anomalies
Protocol Transitions
Packet Timing Characteristics
Inter-Arrival Time
Flow Rate
Timing Consistency
Bandwidth Consumption Patterns
Bytes/s
Packets/s
Bytes per Packet
Secondary Validation Metrics
Connection Establishment Patterns
SYN-ACK Ratios
Connection Success Rate
Handshake Timing
Flag Usage in Protocols
TCP Flag Combinations
Flag Sequences
Unusual Flag Patterns
Packet Size Distributions
Size Variability
Size Consistency
Payload Analysis
Inter-arrival Time Variations
IAT Standard Deviation
Burst Patterns
Timing Regularity

This comprehensive visualization presents the IoT Security Metrics Framework developed for SME environments, organizing metrics into primary indicators and secondary validation metrics. Primary indicators represent the first line of defense, focusing on traffic flow patterns, protocol distribution, packet timing, and bandwidth consumption - metrics that can be efficiently monitored even with limited resources. Secondary validation metrics provide deeper analytical capabilities, examining connection establishment, flag usage, packet size, and inter-arrival time variations to confirm potential threats. This layered approach is specifically designed for SMEs, allowing them to implement basic monitoring using primary indicators with minimal resources, while adding secondary metrics as capabilities grow. The framework emphasizes metrics that balance detection effectiveness with implementation feasibility, acknowledging the resource constraints that smaller organizations typically face. By implementing these metrics in order of priority, SMEs can develop a progressive security monitoring capability that grows alongside their security maturity.


Attack Detection Matrix: Effectiveness of Metrics for Different Attack Types
Traffic Flow Patterns
Protocol Distribution
Packet Timing
Bandwidth Consumption
Connection Establishment
TCP Flag Usage
Packet Size Distribution
IAT Variation
DDoS/DoS
Reconnaissance
Spoofing
Data Exfiltration
Command & Control
3 1 2 1 1
2 3 3 1 2
3 2 1 2 2
3 1 1 2 1
2 3 2 0 1
2 3 2 1 2
1 2 1 3 2
3 1 1 2 3
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Effectiveness
Effectiveness Scale: 0 = Not effective, 1 = Somewhat effective, 2 = Effective, 3 = Highly effective

This Attack Detection Matrix visualizes the effectiveness of different metrics in detecting various types of IoT security threats. The color intensity and dot indicators represent effectiveness levels on a scale from 0 (not effective) to 3 (highly effective). This matrix serves as a practical guide for SMEs to focus their monitoring efforts on the most relevant metrics for their threat landscape. For example, DDoS and DoS attacks are best detected through traffic flow patterns, packet timing, and bandwidth consumption metrics, while reconnaissance activities are more effectively identified through protocol distribution, connection establishment, and TCP flag usage analysis.

For resource-constrained organizations, this prioritization is crucial - by implementing the most effective metrics for the most likely threats, SMEs can maximize security coverage while minimizing implementation complexity and resource requirements. The matrix also highlights the importance of a multi-metric approach, as no single metric provides comprehensive detection capabilities across all attack types.