## UNAUTHORIZED ACCESS

Unauthorized Access transpires when an attacker tries to infiltrate an information system without rightful authorization. Repeated failed login attempts or access from unfamiliar locations are major warning signs.

### LOG SOURCES

- **Firewall Logs:** Capture details like IP addresses, origins, and the success or failure of login attempts
- **EDR Logs (Endpoint Detection and Response):** Showcase local activities on devices like successful logins and other suspect activities, for instance, unusual file interactions

### CHALLENGES

- Multiple failed logins suggest potential unauthorized access
- Logins originating from unfamiliar geographical locations

### BITLYFT AIR® SOLUTIONS

- Real-time detection and flagging of suspect activities
- Automatic IP blocking upon detection of suspicious addresses
- Triggered automated recovery processes for account security enhancements
- Comprehensive post-event analysis to strengthen defenses

## MALWARE INFECTION

Malware Infections involve unauthorized software installations that can enact tasks such as data theft, file encryption, or overall system compromise.

### LOG SOURCES

- **EDR Logs:** Highlight unusual file actions or sudden software installations
- **Firewall Logs:** Identify suspicious outgoing traffic or connections to notorious malicious IPs

### CHALLENGES

- Indicators of malware activity in EDR logs
- Malware communication signals in firewall logs

### BITLYFT AIR® SOLUTIONS

- Isolate affected devices immediately to halt malware propagation
- Initiate scans to pinpoint and exterminate malware
- Restore systems from untainted backups and revise security protocols

## INSIDER THREAT

Insider Threats are malicious or negligent actions by those within the organization, leading to unauthorized data access, theft, or system damage.

### LOG SOURCES

- **EDR Logs:** Mark frequent file access or significant data transfers
- **Email Logs:** Highlight suspicious emailing patterns, perhaps revealing data leakage or competitor correspondence

### CHALLENGES

- Suspect data interactions or transfers noted in EDR and Email logs
- Probable insider threat activity indications

### BITLYFT AIR® SOLUTIONS

- Suspend implicated user accounts and signal the internal security team
- Initiate a comprehensive internal security audit
- Engage legal bodies or even law enforcement based on the severity

## DATA EXFILTRATION

Data Exfiltration is the unauthorized copying or transferring of data, often a well-coordinated move to extract vital data such as customer details or intellectual properties.

### LOG SOURCES

- **Firewall Logs:** Track abnormal data transfers or connections to external IPs
- **EDR Logs:** Record abnormal file interactions or data movements

### CHALLENGES

- Suggestive data transfers to external IPs
- Indications of data theft in progress

### BITLYFT AIR® SOLUTIONS

- Block questionable external IP addresses instantly
- Isolate impacted devices and initiate security reviews
- Execute internal audits to appraise and avert potential future exfiltration attempts

## RANSOMWARE ATTACKS

Ransomware Attacks lock or encrypt files on a device, asking for a ransom (often in cryptocurrency) for the key to unlock them. Swift detection is vital to curtail the damage.

### LOG SOURCES

- **EDR Logs:** Recognize file changes, encryption, or odd processes indicating ransomware
- **Email Logs:** Identify probable ransomware entry points, like phishing emails with harmful attachments

### CHALLENGES

- Signs of ransomware in EDR logs
- Employee receipt and interaction with suspicious emails

### BITLYFT AIR® SOLUTIONS

- Quarantine affected devices to prevent ransomware spread
- Instant notification to internal security teams and considering external response team activation
- Systems restoration from clean backups where viable

## REAL PROBLEMS. REAL SOLUTIONS.

Want to see more examples of BitLyft AIR® in action?
Scan the QR code to access our library of case studies.

BitLyft Cybersecurity