When it comes to securing your environment, it’s important to know where the danger lies.

**Learn your terrain**

Common threat hunting scenarios:

- **Authentication**: Represents the identity aspect of an attack.
- **Backdoors**: Are intended or malicious ways that an attacker can gain access.
- **Communication**: Provides information about what attackers are doing.

**Authentication**

- **Password spraying**
- **Password reuse**
- **Misconfigured accounts**

**Backdoors**

- **Web shells**
- **Shadow accounts**

**Communication**

- **IP addresses**
- **Proxies**

**Proactive threat hunting**

- **Identify other systems the attacker may have infected**
- **Understand the signs of potential danger in your environment**
- **Get details on Microsoft Defender Experts for cloud and on-premises systems**

**Be Proactive**

- **Leverage highly skilled security experts**
- **Know the ABCs**
- **Apply the ABCs**

**Get started with threat hunting**

- **Click here** to read our full "Threat Hunting Survival Guide" eBook.
- **Read how Microsoft Defender Experts for cloud and on-premises systems help you**

**Build your own threat hunting program**

- **Bring together the right people**
- **Give them the right tools**
- **Provide them with the right training**

**Leverage highly skilled security experts**

- **Microsoft Security Experts**
- **Proactive threat hunting can help you address sophisticated modern threats more effectively.**

**Human-operated attacks**

- **Human-operated attacks occur when attackers interact with the backdoor.**
  - **Identify how the attacker controlled the source and every element they're connected to.**
  - **Infiltrate a system and escalate their scale of attack to varying degrees based on what they find in your environment.**

**Commodity vs human-operated**

- **Commodity attacks**
  - **Use reconnaissance techniques to potentially compromise applications and systems.**
  - **Use reconnaissance techniques to potentially compromise applications and systems.**
- **Human-operated attacks**
  - **Use reconnaissance techniques to potentially compromise applications and systems.**
  - **Use reconnaissance techniques to potentially compromise applications and systems.**

**Be focused on numbers of potential targets**

- **Remote access**
- **Misconfigurations**
- **Shared credentials**

**Source: Understanding identity theft protection and Cyber Signals: A Comprehensive Guide to Identity-Based Attacks**

- **Identity attacks by CISOs report an increase in phishing campaigns and identity fraud.**
- **4.9 billion attacker-driven sign-ins in one month alone.**

**Ransomware attacks**

- **Use reconnaissance techniques to potentially compromise applications and systems.**
- **Take action.**
- **Learn more about protecting your organization from ransomware.**

**Incident response playbooks**

- **Explore Microsoft’s security research and threat intelligence efforts.**
- **Check out our quarterly cyberthreat intelligence brief called Cyber Signals.**
- **Learn more about human operated threats.**

**EXAMPLES OF COMMUNICATION ELEMENTS**

- **E-mail**
- **Remote access**
- **Shadow accounts**

**EXAMPLES OF BACKDOOR ELEMENTS**

- **Web shells**
- **Shadow accounts**
- **Remote access**

**Required**

- **Expertise, judgement, creativity**

**optional**

- **Expertise, judgement, creativity**

**Leveraged by Microsoft Security Experts**

- **Microsoft Security Experts**
- **Microsoft Security Experts**
- **Microsoft Security Experts**