FORWARD DEFENSE

# Threat Hunting

## *SEARCH AND DESTROY*

Threat Hunting Options | Threat Hunting Services | Vulnerability scanning | Honeynet deployment | File integrity checks | Configuration reviews | Account reviews

# Threat Hunting

## The enemy may be among you…so search and destroy.

Actively looking for indicators of compromise is a necessary part of today's IT security practices. Passive defense has been insufficient for a decade. Perimeter defenses are not enough, and even layered defense-in-depth approaches fail eventually. No matter how entrenched you get, the adversary can still get in. Without actively looking for the enemy within, your network can quickly become hostile.


# Threat Hunting Options

Forward Defense offers a variety of threat hunting options. We can help you design a permanent system utilizing best-of-breed technical products, based in repeatable processes, and backed by real-world training for your team to develop an internal squad of highly trained cyber warriors who can patrol your network on an ongoing basis. Alternatively, we can send in our troops on a shorter-term basis to seek out the enemy in your midst, helping you take out the trash on a periodic basis. Whatever solution meets your needs, we can customize an offering around your risk tolerance, threat level and budget.

Threat Hunting Options | Threat Hunting Services | Vulnerability scanning | Honeynet deployment | File integrity checks | Configuration reviews | Account reviews

# How Forward Defense Works with you

Our experts bring years of real world experience in a variety of disciplines to form a hunting party with the skills needed to know where to look and what to look for. Our penetration testing experts know exactly how they would breach your network and how they would hide their tracks. Meanwhile, our cyber investigators bring years of experience in tracking cyber prey and know the techniques that are most likely to expose them. Using open source and commercial tools, combined with the experience that only comes from prowling through networks year after year, our team can identify indicators of compromise and help your team contain and remediate the issue before it continues to grow.

**Threat Hunting services from Forward Defense.**
**Take back your network**

**Hacks happen.**
**Don't pretend it won't happen to you.**
**Don't pretend it hasn't already.**


Our service takes a multidisciplinary approach to the problem to leave no stone unturned, including:

## Network security monitoring

Using your existing tools, commercial products, or open source solutions our team will monitor your network for anomalies that suggest that an intruder may be present.

## Host based detection

Using commercial or open source agents our experts will work with your team to deploy and monitor your network endpoints to detect the presence of unauthorized activity.

## RAM analysis and process reviews

Collecting volatile memory for analysis is a critical component of any threat hunt. Whether spot checking critical systems, sweeping the entire enterprise for indicators of compromise, or remotely dumping system RAM in response to detected network anomalies, volatile memory will then be analyzed for rogue processes, unauthorized connections, and similar indicators of malicious code running on the system.

## Vulnerability scanning

Active defense requires that existing holes be identified and explored for evidence that others may have used them for unauthorized access. When our team detects a possible entry point, we will first examine the impacted systems to clear and hold that system rather than simply patching the vulnerability and hoping for the best.

## Log analysis

Properly configured logs can yield massive amounts of information regarding activity on the network and on individual systems. Combing through this data can be resource intensive, but combining intelligent analytics with experienced analysts allows our team to surface events of interest in a timely manner.


# Honeynet deployment

If the enemy is within, deploying a honeynet is a good way to draw him out. By configuring realistic looking target systems, coupled with enhanced monitoring and detection, our team will set the trap and wait for the adversary to take the bait.

# File integrity checks

Critical system files should be checked on an ongoing basis for signs of unauthorized tampering. Changes to core system components may indicate the presence of root kits or other malicious activity.

# Configuration reviews

Many adversaries avoid installing malicious software and instead change system configurations to reduce security, create backdoors or create vulnerabilities that they can exploit. Careful review of configuration files can detect these changes and alert you to the presence of an intruder, as well as provide opportunities to further monitor their activities.

# Account reviews

Why add malware that may be detected when you can simply upgrade access or add seemingly legitimate accounts? Many dedicated adversaries will exploit typical logon behavior, PowerShell scripts, or remote shells to fly below the radar and blend in with normal network traffic. Careful audits of user accounts and access patterns can reveal the anomalies that uncovers the enemy within.

**Threat Hunting services from Forward Defense. Take back your network.**