# Detecting a Nation-State-Level Red Team Attack with ArcSight Intelligence

**Micro Focus ArcSight Intelligence behavioral analytics shines a new light on existing endpoint data to uncover unknown threats. At a major consumer company, the powerful combination of behavioral analytics and rich endpoint data uncovered a sophisticated Red Team attack.**

Micro Focus ArcSight Intelligence behavioral analytics shines a new light on existing endpoint data to uncover difficult-to-find threats. Combined with an endpoint detection and response (EDR) platform, ArcSight Intelligence analyzes billions of events, identifies risky behaviors, and gives security teams real threat leads to follow.

## ArcSight Intelligence Uncovers a Major Enterprise's Red Team Attack

Red Teams are critical to an effective cybersecurity strategy and allow threat hunters and incident responders to put their skills to the test. Detecting this kind of attack signals that you are prepared to detect a real attack.

At a major consumer company, ArcSight Intelligence leveraged rich endpoint data—process, user and machine activity—and detected a well-executed, nation-state-level Red Team attack. Behavioral indicators of an attack quickly came to light, and ArcSight Intelligence uncovered the entire attack lifecycle and gave the company's security team the right context to respond to attack.

ArcSight Intelligence provided high-quality security leads that showed the threat hunters and incident responders the following attack characteristics:

| | |
|---|---|
| OWA Profiling | The attacker leveraged an Outlook Web Access (OWA) timing attack to uncover valid user accounts. The attack produced a sudden spike in clear-text passwords, which was detected via unusual login activity to the OWA server and logon type. |
| Remote Exploit | Remote attack tools, Mimikatz and CrackMapExec, were used against a known administrative server and detected as an unusual process that was running on the server. |
| Reconnaissance | A compromised administrator account logged in on an administrative laptop, enumerating directories on other machines to look for files with passwords. A hidden share returned the results from each machine, and the local registry hive was extracted from the admin laptop. These events signaled unusual share activity and unusual volume of processes per hour. |
| Lateral movement | The compromised account engaged in lateral movement to adjacent servers and launched more reconnaissance attacks, indicating unusual logins for the administrator accounts and unusual process use on the other machines. |
| Password Guessing | A secondary attack was underway to test for default password use. The attack used a python script to map a user drive of each username with a default password. This produced a high volume of processes and a large number of failed authentication attempts. |
| IP Address and Attack Tool | A final attack leveraged a sustained series of Windows Management Instrumentation (WMI) attacks multiple servers. It was detected by anomalous process activity on the attacked servers and unusual volume of processes on the attacking machine. ArcSight Intelligence stores raw events and identified the attack tool and IP addresses being used in the initial compromise. |