OverWatch Elite's Call Escalation Vital to Containing Attack

crowdstrike.com/blog/overwatch-elite-call-escalation-vital-to-containing-attack/

Falcon OverWatch Team

October 25, 2021

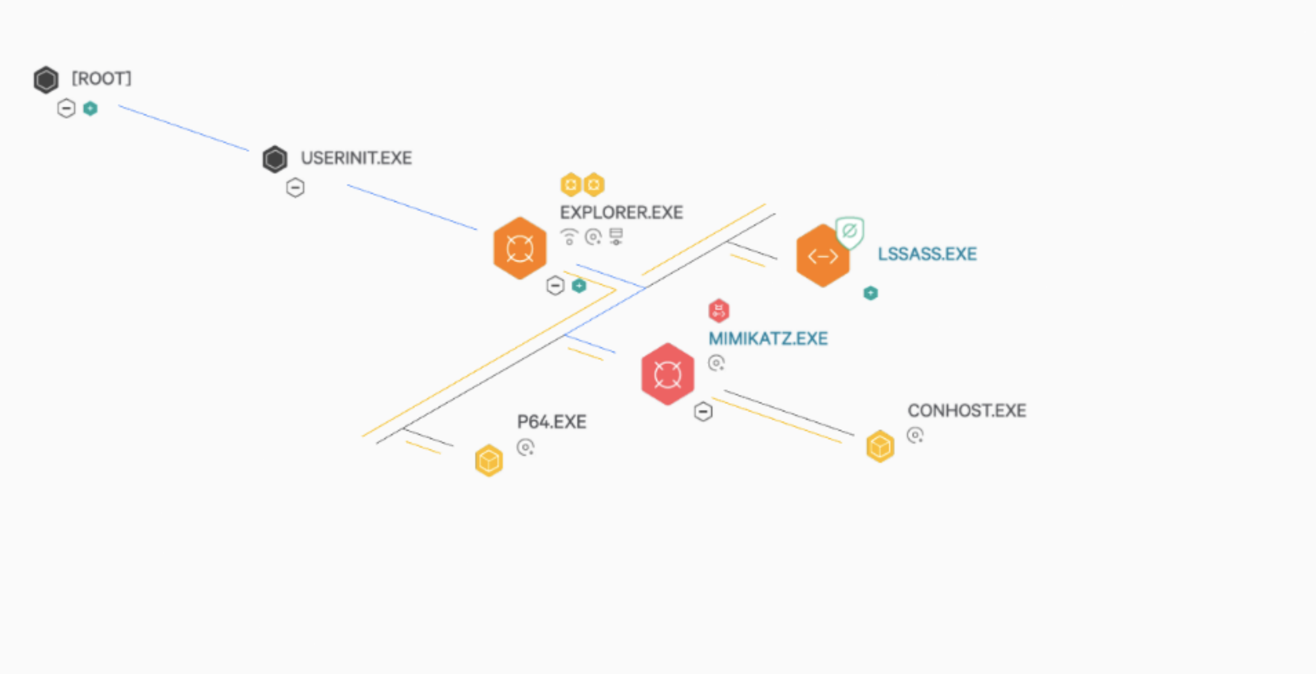
For a defender, time is critical. As CrowdStrike Falcon OverWatch™ threat hunters know firsthand, adversaries can move from initial access to lateral movement in just minutes. This blog and the real world attack scenario that it describes highlights the essential value that human security expertise adds to an organization's security defense and response capabilities beyond the limits of autonomous ML/AI alone.

Earlier this year, OverWatch threat hunters identified the early stages of an intrusion against a healthcare organization. Fortunately, this customer subscribed to the OverWatch Elite service, which includes a CrowdStrike threat hunting analyst that helps the in-house security team improve response times and drive continuous optimization. This meant an assigned threat response analyst was able to contact the organization personally to alert them of the malicious activity. This allowed the customer to contain the adversary before any significant impact resulted.

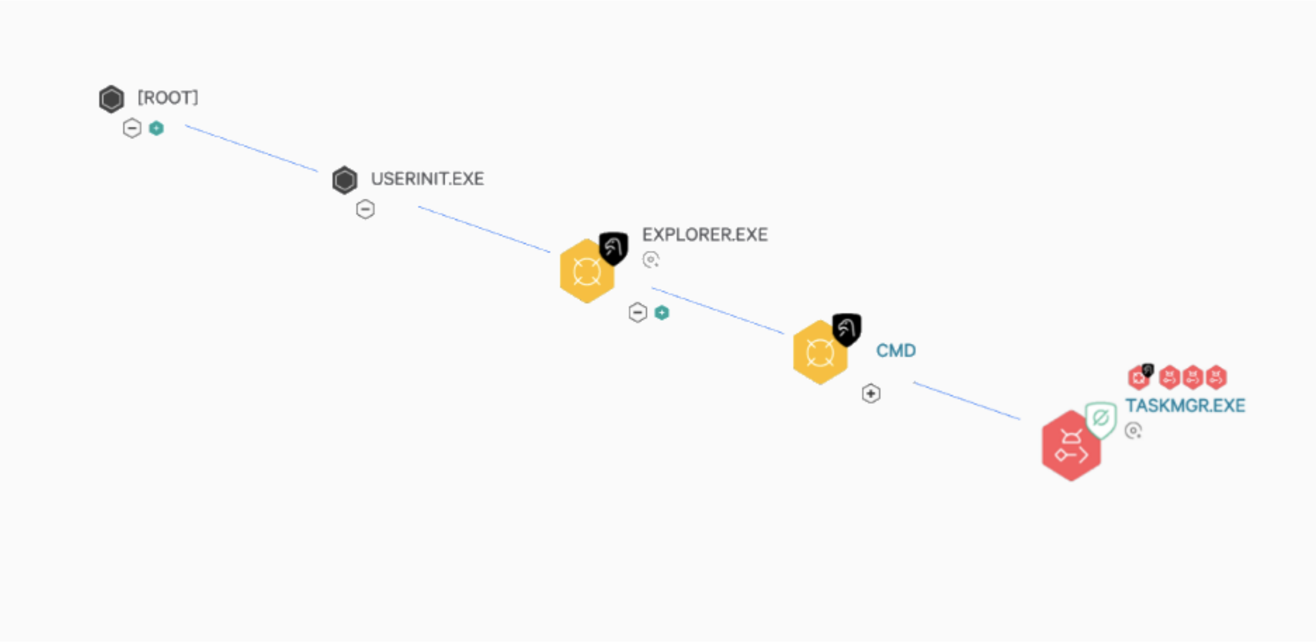
This call escalation protocol — a core offering of OverWatch Elite — can prove crucial in enabling a timely response to sophisticated hands-on-keyboard activity when every minute counts. This blog outlines the detection and response to the attempted intrusion.

Tracking and Containing an Intrusion in Real Time

OverWatch discovered an unknown adversary conducting malicious interactive activity on multiple hosts. Using a legitimate administrator account, the adversary gained access to the initial host via a Remote Desktop Protocol (RDP) session. Valid credentials are often widely available through various means and can provide an undetected path into secure networks. The adversary then wrote a series of tools to the compromised host, including PowerTool, Mimikatz, and a Meterpreter stager payload with the file name `lssass.exe`, masquerading as the legitimate Windows executable.

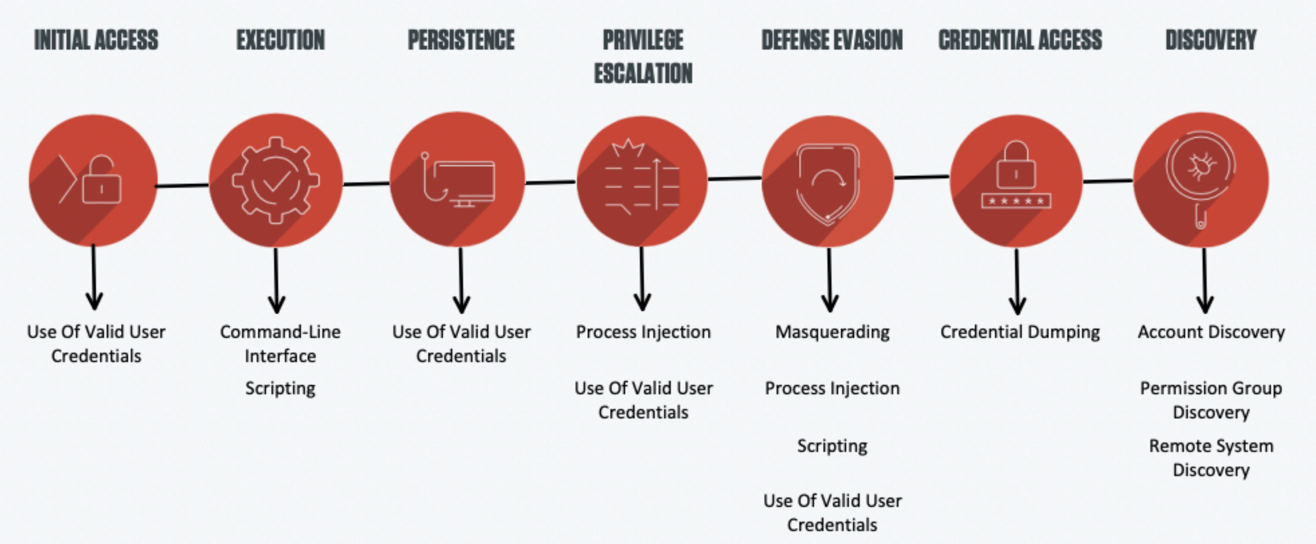


Next, the adversary executed Mimikatz in an attempt to harvest user credentials from the initial host before moving laterally to various hosts using mstsc.exe, a Windows Remote Desktop Connection tool. Using an RDP session, the adversary proceeded to log in to two additional remote hosts using yet another account, indicating that they were in possession of numerous sets of valid domain credentials. The adversary was then observed conducting host and network reconnaissance, including the enumeration of additional systems on the domain. Finally, the adversary attempted to use the Windows Task Manager to extract the contents of the LSASS process in a further attempt to harvest credentials, which was ultimately thwarted by the CrowdStrike Falcon® sensor.



The tailored guidance provided by OverWatch Elite during the customer's initial onboarding ensured that the Falcon platform was configured correctly and had appropriate prevention settings turned on, ensuring no endpoint was left unprotected.

Tactic and Technique Overview



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY
Use Of Valid User Credentials	Command-Line Interface	Use Of Valid User Credentials	Process Injection	Masquerading	Credential Dumping	Account Discovery
	Scripting		Use Of Valid User Credentials	Process Injection		Permission Group Discovery
				Scripting		Remote System Discovery
				Use Of Valid User Credentials		

An Elite Response When Every Minute Matters

As this malicious activity unfolded, OverWatch threat hunters were watching and quickly determined that this was malicious hands-on-keyboard activity. The CrowdStrike Threat Graph® database contributes to OverWatch's ability to hunt across over 1 trillion endpoint events each day, enabling threat hunters to quickly surface the most subtle of suspicious or malicious behaviors that could potentially indicate a sophisticated adversary's presence.

Upon validating that the observed activity was malicious, OverWatch triggered multiple detections to the customer's Falcon console, followed by a detailed notification that was sent via email. This notification contained a comprehensive summary of the event, including the indicators of compromise (IOCs) seen during this attack. With this actionable intelligence in hand, the organization had the critical context necessary to take immediate action and disrupt the adversary.

During working hours, customers are often available to discuss investigations, detections and intrusions with OverWatch Elite analysts. Adversaries, however, do not operate strictly within business hours. In this case, the malicious activity in question was unfolding over the weekend — a time when organizations may not be monitoring their queues or mailboxes as closely.

As a Falcon OverWatch Elite customer, this organization was provided with 60-minute call escalation. This core OverWatch Elite feature is critical to ensuring that active hands-on keyboard activity is being responded to by the customer in a timely fashion. If no one in the customer's organization confirms they are investigating the critical activity within 60 minutes of the email notification, an OverWatch Elite threat response analyst will begin calling a predetermined list of individuals at the organization until there is confirmation that someone is responding to the incident.

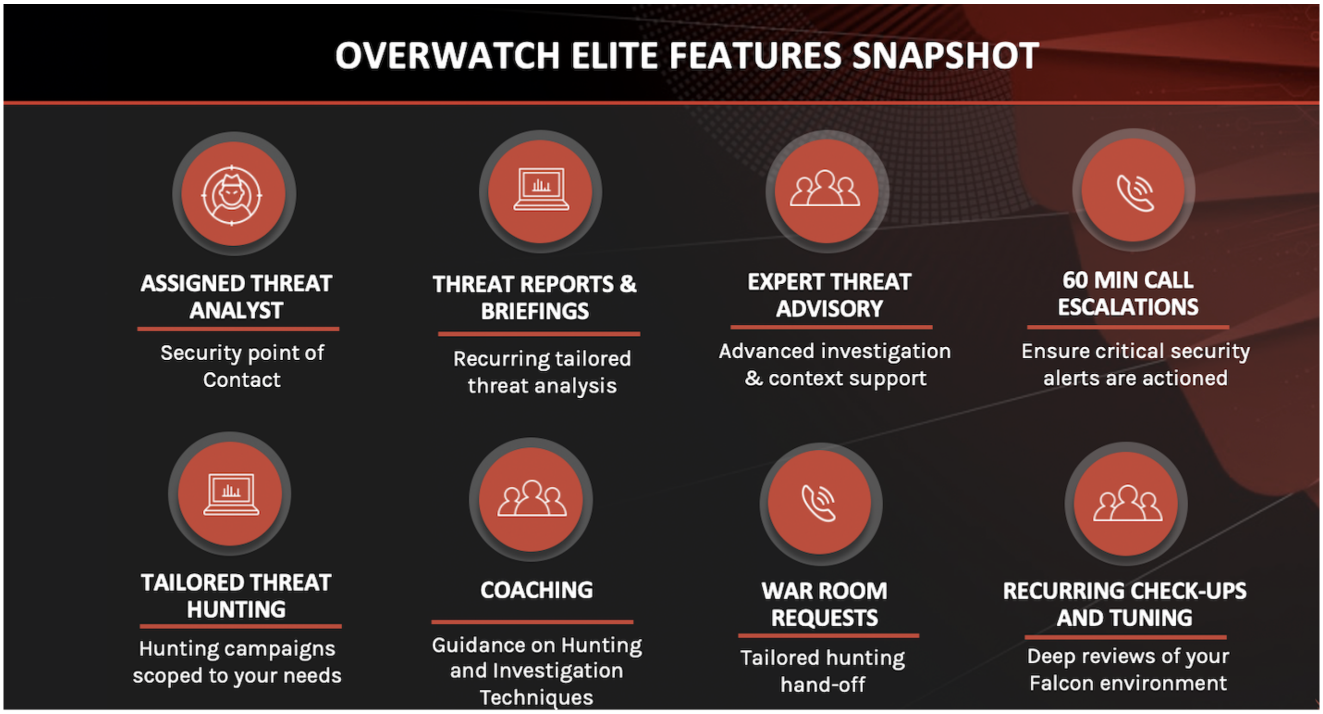
In this instance, the initial notification went unacknowledged. OverWatch Elite performed a rapid assessment of the unfolding situation and deemed rapid escalation was necessary. Once contact was secured, OverWatch Elite briefed the customer, prompting them to contain the compromised hosts before the adversary could achieve the intended objectives.

OverWatch hunts continuously and simultaneously across its customers' endpoints 24 hours a day, 365 days a year, providing near real-time notifications of potential threats to customers. It is equally crucial that defenders are ready to take action following OverWatch notifications. OverWatch Elite's call escalation protocol ensures that notifications don't get missed and defensive action can be taken quickly.

Features Unique to Falcon OverWatch Elite

OverWatch Elite's core offerings allow customers to build a personalized relationship with their assigned threat response analyst. Specific service inclusions, such as the call escalation protocol highlighted, provide OverWatch Elite customers with added peace of mind that adversary activity within their environments can be rapidly disrupted. The tailored threat hunting available to OverWatch Elite customers also allows them to develop, operationalize and tune their threat hunting program to meet the needs of their specific environment, all while giving them access to fast, closed-loop communications.

In addition to the call escalation protocol, the other unique offerings of OverWatch Elite are detailed below. For more information, please visit OverWatch Elite’s page on CrowdStrike’s website.



OVERWATCH ELITE FEATURES SNAPSHOT

ASSIGNED THREAT ANALYST
Security point of Contact

THREAT REPORTS & BRIEFINGS
Recurring tailored threat analysis

EXPERT THREAT ADVISORY
Advanced investigation & context support

60 MIN CALL ESCALATIONS
Ensure critical security alerts are actioned

TAILORED THREAT HUNTING
Hunting campaigns scoped to your needs

COACHING
Guidance on Hunting and Investigation Techniques

WAR ROOM REQUESTS
Tailored hunting hand-off

RECURRING CHECK-UPS AND TUNING
Deep reviews of your Falcon environment

Additional Resources

- *Read about the latest trends in threat hunting and more in the 2021 Threat Hunting Report.*
- *Learn more about Falcon OverWatch proactive managed threat hunting.*
- *Watch this video to see how Falcon OverWatch proactively hunts for threats in your environment.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*