Mike Pilkington

WMIC for incident response

June 4, 2010

Earlier this week, I posted about using psexec during incident response. I mentioned at the end of that post that I've been using WMIC in place of psexec and that I'd have more on that later. This post, is a follow up to the psexec post.

WMIC

Prompted by the excellent work of Ed Skoudis and his part in the Command Line Kung Fu blog, as well as a really nice webcast he did a few years ago titled Essential Windows Command-Line Kung Fu for Info Sec Pros and an Internet Storm Center article from the same year, I've come to rely on WMIC for a large number of IR tasks. It provides much of the functionality of PsExec, as well as a lot of additional functionality, and it does so without ever sending the password in the clear. Instead, authentication is performed via native Windows network authentication methods.

The WMIC tool was introduced in Windows XP Professional and has been included in every version of Windows since. Furthermore, it can be used to manage every Windows version since Window 95, although 9x and NT require the Microsoft WMI Core add-on to be installed.

Unfortunately there is not a lot of detailed documentation on WMIC. Ed has arguably produced much more and much better documentation than Microsoft, or anyone else for that matter, so the links above to Ed's resources are your best bet for digging deeper into its capabilities.

For my purposes, the following are several WMIC examples which I find very useful.

The first couple of examples are useful for enterprise forensic purposes, where the responder's goal is to deploy an agent:

For EnCase Enterprise users, here's a method to deploy the servlet (named Setup.exe, which has been copied to the remote machine via "?xcopy Setup.exe \\remote-host\c$\Windows\Temp')":

```
wmic /node:<remote-ip> /user:<username> process call create "C:\Windows\Temp\Setup.exe <-n process name> <-l
```

For FTK users, here's a method to deploy the agent (FTKAgent.exe and InvestigatorCert.crt have been copied to the remote machine via xcopy):

```
wmic /node:<remote-ip> /user:<username> process call create "C:\Windows\Temp\FTKAgent.exe –cert InvestigatorC
```

The rest of the examples are useful for incident response. Many of these were taken directly from Ed's ISC article linked above.

Examine Auto Start processes:

```
wmic /node:<remote-ip> /user:<username> startup list full
```

Find who is logged on to a computer's console:

```
wmic /node:<remote-ip> /user:<username> ComputerSystem Get UserName
```

Query local user accounts:

```
wmic /node:<remote-ip> /user:<username> useraccount list full
```

Find the path to a specific running executable and its parent process (for all, leave off ?where name='):

```
wmic /node:<remote-ip> /user:<username> process where get ExecutablePath,parentprocessid
```

Find command line invocation of a specific executable as well as the creation time for the process (for all, leave off ?where name='). Reference this Microsoft TechNet article for converting the time:

```
wmic /node:<remote-ip> /user:<username> process where get name,processid,commandline,creationdate
```

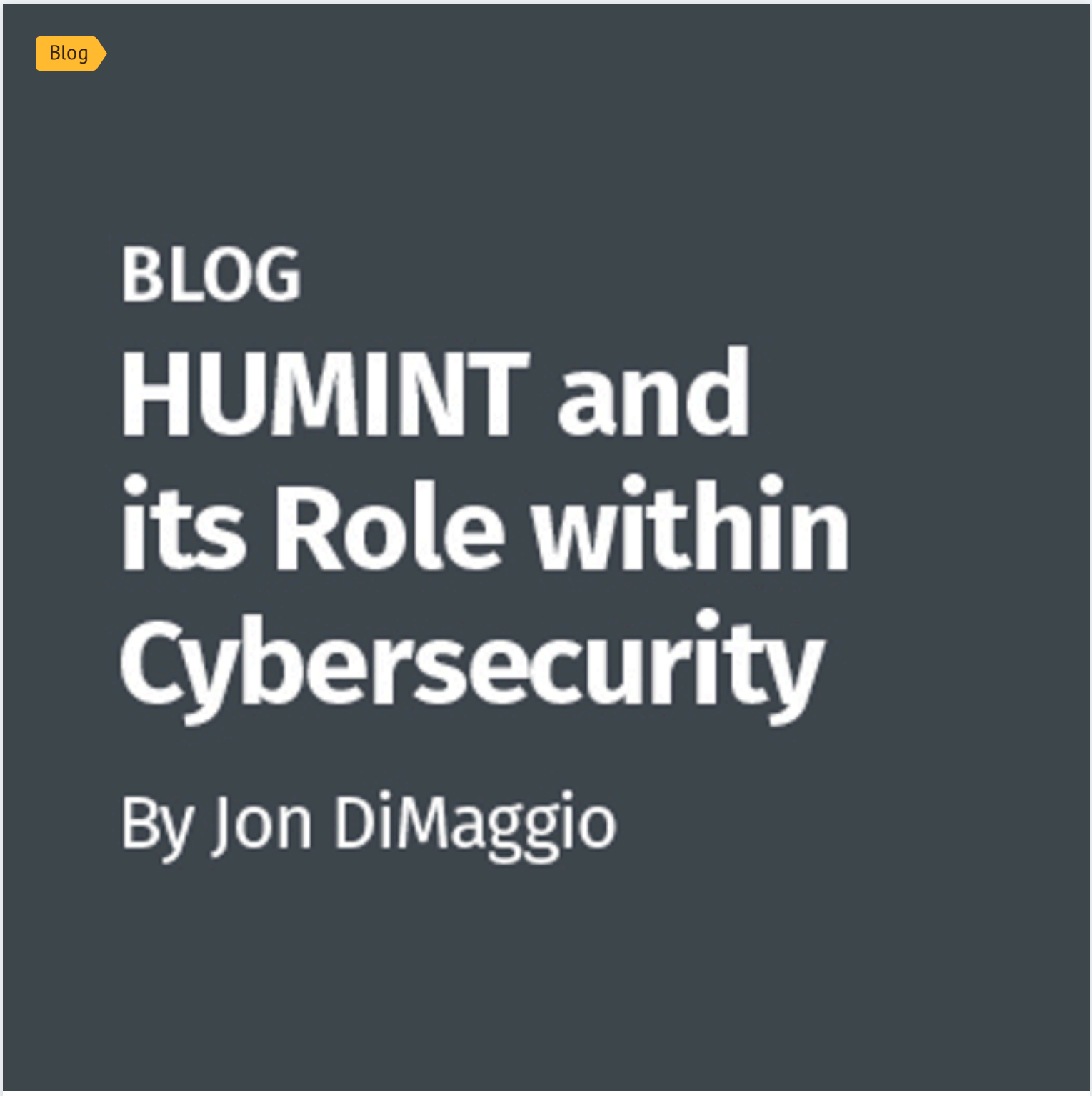
Find status of a specific service?note that 'caption' is needed in the where clause, but it is actually the 'displayname' (for all, leave off ?where caption='):

```
wmic /node:<remote-ip> /user:<username> service where caption="PsExec" get displayname,startname,state,status
```

This is by no means an exhaustive list of useful WMIC commands. I've found that you can do just about anything with it with respect to querying a machine or starting and stopping processes and services. The one thing it doesn't do is interactive access, which is why the use of PsExec can still be useful on occasion.

Tags: Digital Forensics, Incident Response & Threat Hunting

Related Content

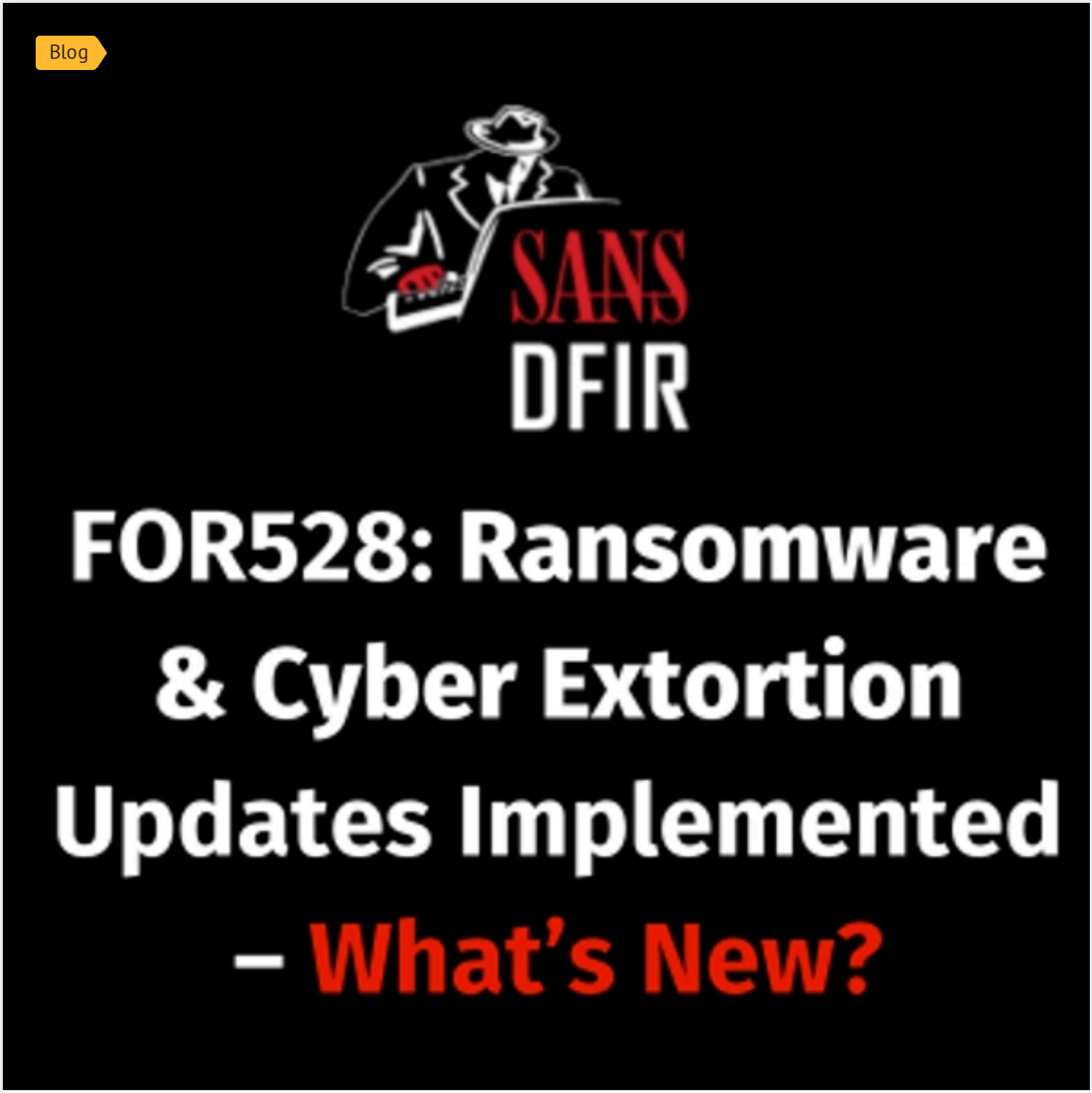


Digital Forensics, Incident Response & Threat Hunting · October 4, 2024

HUMINT and its Role within Cybersecurity

This blog explores HUMINT's role in cybersecurity, detailing its implementation, benefits, and potential risks.

Jon DiMaggio

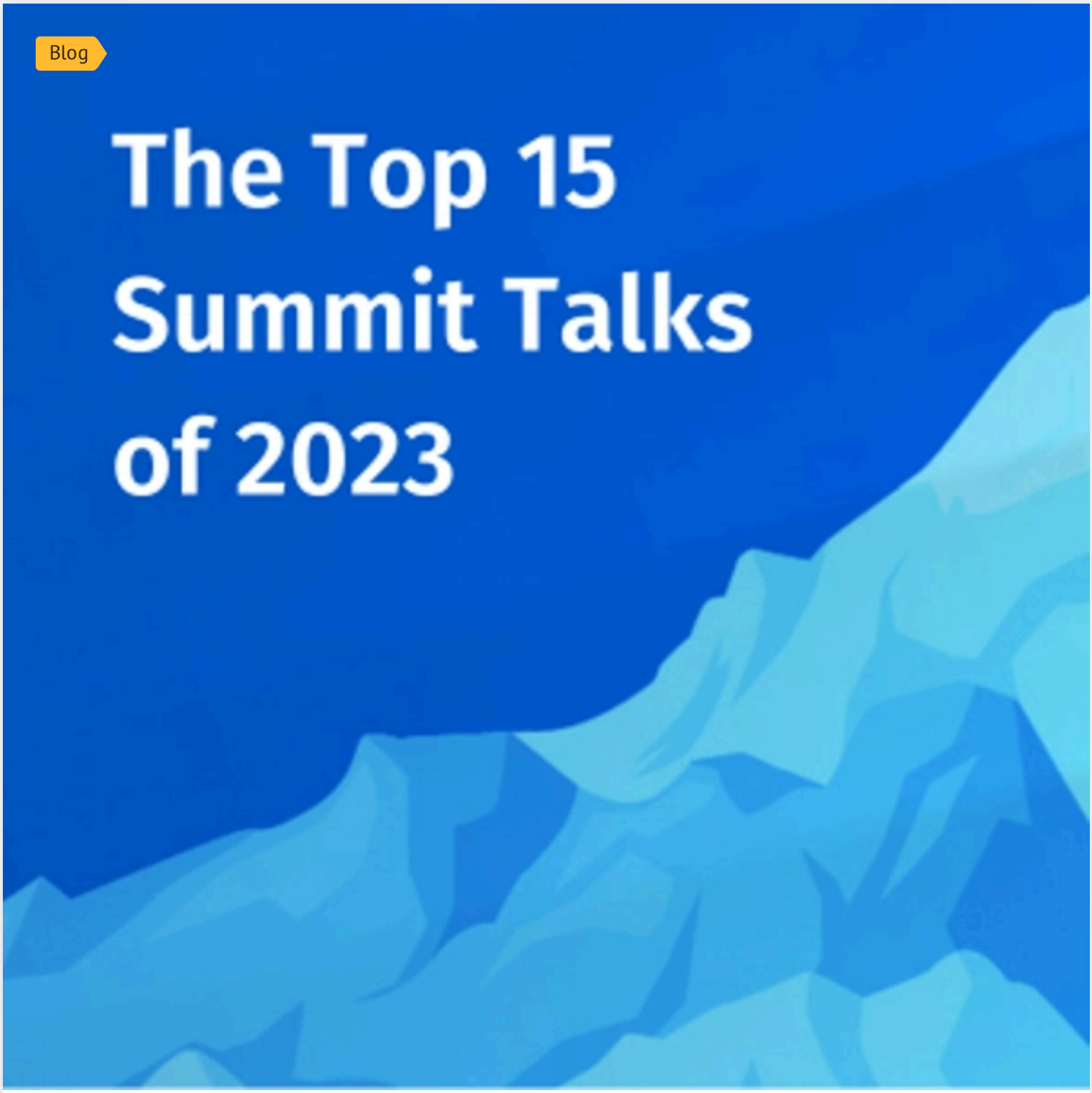


Digital Forensics, Incident Response & Threat Hunting · January 16, 2024

FOR528: Ransomware & Cyber Extortion Course Updates Implemented – What's New?

The recent FOR528 course better addresses the differences between ransomware and cyber extortion, and provides new hands-on labs and bonus content.

Ryan Chapman



Cybersecurity Insights, Digital Forensics, Incident Response & Threat Hunting, Cyber Defense, Cloud Security, Open-Source Intelligence (OSINT), Cybersecurity Leadership, Security Awareness, Artificial Intelligence (AI)

· December 18, 2023

Top 15 SANS Summit Talks of 2023

This year, SANS hosted 16 Summits with 209 talks. Here were the top-rated talks of the year.

Alison Kim