Presented By NeoSystems® & SNC®

Hiding in the Shadows

How Threats Exploit the Unprepared

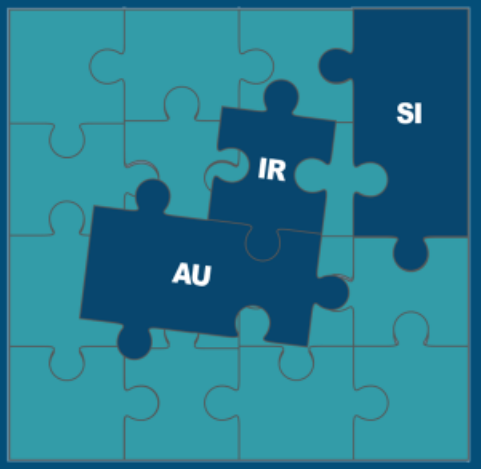
NeoSystems®

CMMC: Why We Do It, Episode 7

JUNE 5, 2025

CMMC: Why We Do It
Episode #7: Hiding in the Shadows

(How Threats Exploit the Unprepared)



Contractors comply with FAR, DFARS, and NIST because the Federal Government says they must.

But to be effective, cybersecurity must align with the actual threats. In this series, we will explain the linkage between threats and the cybersecurity measures that counter those threats.

These webinars should help you make better choices about cybersecurity and reduce the likelihood that you will become a victim.

EPISODE 1	EPISODE 2	EPISODE 3	EPISODE 4	EPISODE 5	EPISODE 6	EPISODE 7	EPISODE 8
Shut the Front Door	Loose Lips Sink Ships	The K.I.S.S. Principle	All Together Now	Thinking Critically About Security	Rip the Band-Aid Off	Hiding in the Shadows	Working Hard or Hardly Working
How unauthorized access happens	*The role of user behavior in cyber attacks*	*How complexity & connectivity increase the probability and impact of a cyber incident*	*Exploiting the supply chain*	*You've already been hacked, or at least should act like it*	*Old security only leaks when it rains*	*How threats exploit the unprepared*	*How threat can tell the difference between real security versus fake security*

Our Speakers

Megin Kennett
NeoSystems

Ed Bassett
NeoSystems

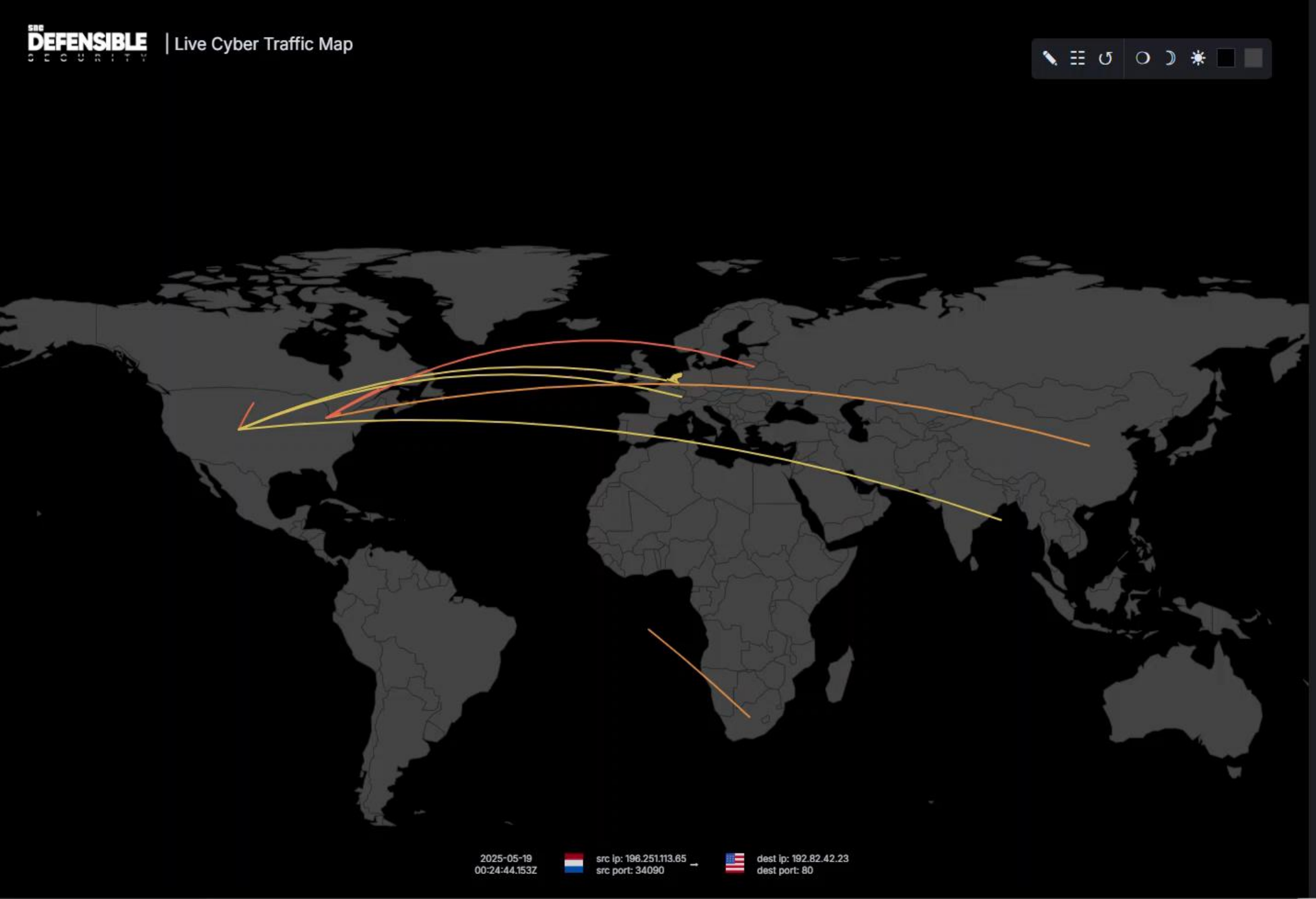
Robert Daugherty
SNC

Agenda

EPISODE 7:
Hiding in the Shadows

- The Threat Map
- The Modern Day Espionage
- The Detection Window is Shrinking
- Bad Actors Playbook
- Case Studies
- Best Practices for Prevention
- AI and Looking Forward
- Tying it Back to NIST 800-171

SNC DEFENSIBLE SECURITY | Live Cyber Traffic Map



TRAFFIC BLOCK REASONS

- Known Cyber Threat
- Country of Origin
- Unapproved Traffic Denied by Policy

BLOCKED ATTACKS THIS MONTH

17,936,686

TOP 5 ATTACKERS

The top countries attempting to breach our systems in the last month.

The Netherlands - 2,987,593 attempts	17%
China - 2,938,917 attempts	17%
Romania - 2,832,079 attempts	16%
Canada - 1,211,801 attempts	7%
United Kingdom - 1,020,993 attempts	5%

TOP 5 IPS ATTACKED

The top SNC internal IPs being targeted in the last month.

192.82.42.198 - 619,400 attempts	3%
192.82.42.74 - 371,099 attempts	2%
192.82.42.112 - 317,786 attempts	1%
192.82.42.115 - 302,679 attempts	1%
192.82.42.11 - 276,453 attempts	1%

TOP 5 PORTS ATTACKED

The top ports being targeted in the last month.

80 - 839,980 attempts	4%
23 - 781,135 attempts	4%
53 - 484,083 attempts	2%
8000 - 441,314 attempts	2%
443 - 435,063 attempts	2%

Federal Security Service (FSB)

Ministry Of State Security (MSS)






ADVERSARIAL MINDSET

A sophisticated, multidisciplinary long-game approach to compromising a U.S. national security system or weapons platform by a sophisticated nation-state adversary will involve a combination of cyber, human, technical, political, and economic strategies, deployed over *years* or even *decades*. Such a comprehensive strategy will involve several stages, aiming to penetrate, influence, degrade, or ultimately neutralize the targeted system.

The strategy will be slow and methodical, relying on persistence and long-term exploitation of systemic vulnerabilities, all while avoiding overt detection or retaliation. The goal will be to erode U.S. military superiority, disrupt decision-making, and create vulnerabilities that can be exploited in times of crisis or conflict.

Hacking is China's *preferred* mode of espionage, of which there are hundreds of examples from the past 10 years. But *hacking is not the only form of spying*. China uses traditional methods of agent recruitment (usually sex or money) as well as unconventional approaches, such as buying property next to a military or research facility and engaging direc[illegible]with [illegible]ers[illegible]s.

$600B

- **49% of incident directly inv[illegible] C[illegible]e [illegible]ilit[illegible] go[illegible]r[illegible]ent employees**
- **41% were private Chinese [illegible]ens**
- **10% were non-Chinese actors (usually U.S. persons recruited by Chinese officials)**
- ***46% of incidents involved cyber espionage, usually by State-affiliated actors***
- ***29% of incidents sought to acquire military technology***
- **54% of incidents sought to acquire commercial technologies**
- **17% of incidents sought to acquire information on U.S. civilian agencies or politicians.**

Detection Window is Shrinking

84
Minutes

51
Minutes

SECONDS

48
Minutes

Speed is survival.

NeoSystems


Days
External
Days

- ***Real-time threat detection*** *to identify and halt intrusions before they spread*
- ***Identity and access controls*** *to prevent adversaries from simply "logging in"*
- ***A counterintelligence mindset*** *– assume breach, proactively hunt for anomalous behaviors to block adversary movement*

The Bad Actor’s Playbook

1. Start with the Obvious: *Public info is Gold*
2. Find the Weakest Link: *Look for an open door*
3. Use People, Not Exploits: *Trick someone into letting you in (phishing, pretexting)*
4. Be Sneaky: *Stay quiet and avoid detection at all costs*
5. Create a Backdoor: *Establish a way to get back in whenever you want*
6. Live off the Land: *Use what's already there*
7. Go for the Crown: *Escalate privileges until you own the network*

NeoSystems

The Adversary's Advantage: Why Attackers Succeed

- Lack of visibility – not collecting activity logs
- Lack of detection – not able to discern bad behavior
- Checklist approach – security tools not used effectively
- Single layer security – trusting anything already inside the perimeter

Case Studies

SNC & Solarwinds: Rapid Detection & Response = Damage prevented

Unauthorized Change: A “Quick” change to an externally facing firewall led to a short window of vulnerability and over 9M brute force attempts by RU and CN

MSS Aerospace Industry Targeting

Image: Aerotime

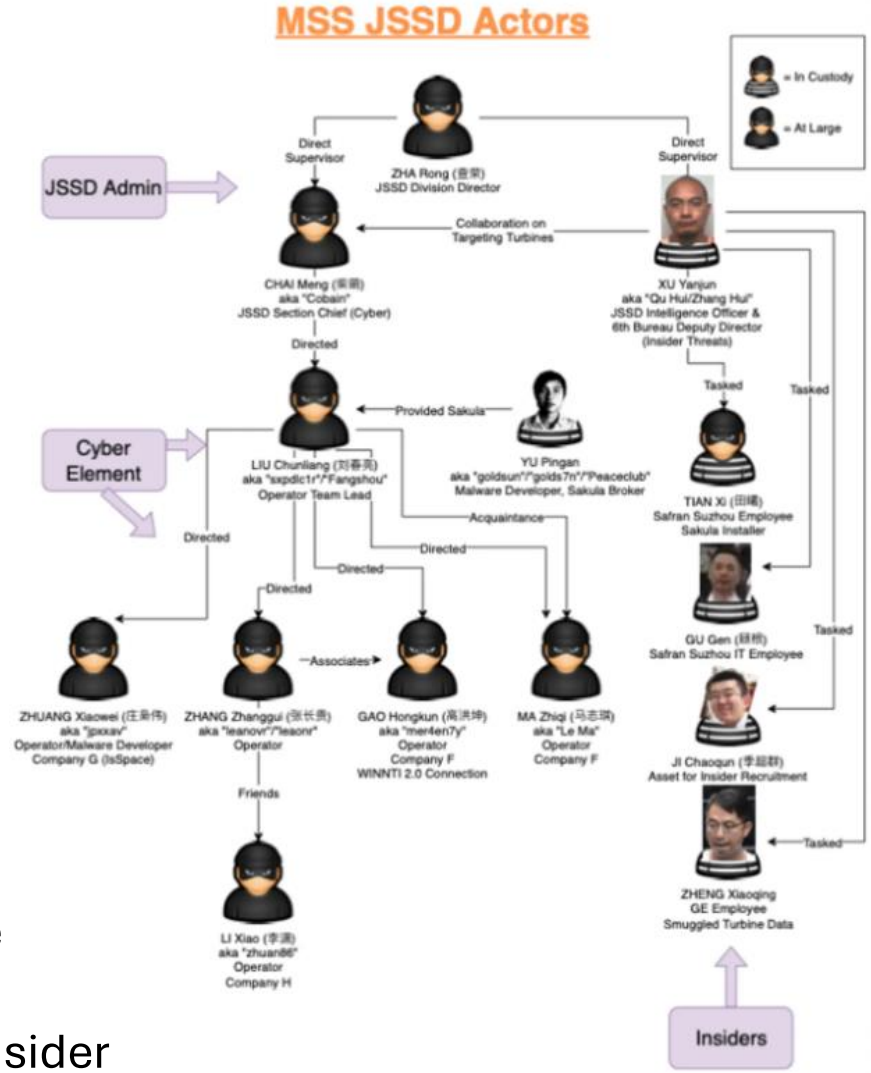


Image: Crowdstrike

- Direct competitor to Boeing and Airbus
- Development of China's COMAC C919 involved a lot of espionage
- Two teams of intel officers; one recruiting, one hacking
- Remote installation of malware, or delivered by USB through an insider
- Successful supply chain breaches – Honeywell, GE, Capstone Turbine, etc.

Best Practices for Prevention

- Real-time threat detection to identify and halt intrusions before they spread
- Identity and access controls to prevent adversaries from simply “logging in”
- A counterintelligence mindset – assume breach, proactively hunt for anomalous behaviors to block adversary movement
- Know Your Normal: Maintain a real-time inventory of assets and logs
- Establish alert thresholds and escalation workflows
- Run tabletop exercises
- Tune your controls—don’t just “set it and forget it”

AI and Looking Forward

Government Playbook

Requirements to address these risks:

- System and Information Integrity
- Audit and Accountability
- Incident Response

System and Information Integrity

- Fix flaws
- Stop malware
- Monitor alerts and take action
- Detect attacks
- Identify unauthorized use

Audit and Accountability

- Log system activity
- Know who did what when
- Protect logs
- Use logs for investigation and response

Incident Response

- Prepare, detect, analyze, contain, recover
- Track and report incidents
- Test incident response

Takeaway Summary

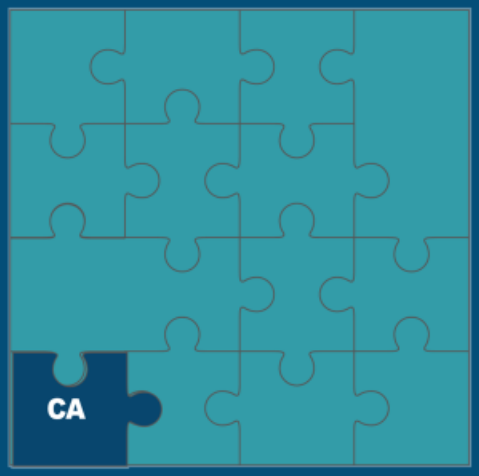
1. **Speed is Survival. Threat actors move fast.** Vulnerabilities are identified almost immediately by the adversary. Keeping your systems patched and your defenses dynamic and agile are foundational to preventing a breach.

2. **Visibility is key. Threat actors are quiet** and experts at evading detection. Having top-notch visibility with cross team and tool integration with automated alerting is key.

3. **AI and Automation. Threat actors** are already using AI, getting smarter and faster. Don’t let them stay ahead.

Episode #8: Working Hard or Hardly Working

(How threat can tell the difference between real security versus fake security)



Contractors comply with FAR, DFARS, and NIST because the Federal Government says they must.

But to be effective, cybersecurity must align with the actual threats. In this series, we will explain the linkage between threats and the cybersecurity measures that counter those threats.

These webinars should help you make better choices about cybersecurity and reduce the likelihood that you will become a victim.

EPISODE 1	EPISODE 2	EPISODE 3	EPISODE 4	EPISODE 5	EPISODE 6	EPISODE 7	EPISODE 8
Shut the Front Door	Loose Lips Sink Ships	The K.I.S.S. Principle	All Together Now	Thinking Critically About Security	Rip the Band-Aid Off	Hiding in the Shadows	Working Hard or Hardly Working
How unauthorized access happens	*The role of user behavior in cyber attacks*	*How complexity & connectivity increase the probability and impact of a cyber incident*	*Exploiting the supply chain*	*You've already been hacked, or at least should act like it*	*Old security only leaks when it rains*	*How threats exploit the unprepared*	*How threat can tell the difference between real security versus fake security*

Questions?

Thank you.

Feel free to contact us:

megin.kennett@neosystemscorp.com

ed.bassett@neosystemscorp.com

robert.daugherty@sncorp.com

www.neosystemscorp.com