AI gedreven cybercrime:
is jouw organisatie voorbereid?

U-Tech Community workshop

orange™ Cyberdefense

INTRODUCTIE

Sebastiaan de Vries

Head of Technology Services

Orange Cyberdefense

Cyberdefense

HET CYBERLANDSCHAP OP AI

AI's Impact on the Landscape

- Profound Shift: Generative and agentic AI are fundamentally altering the dynamics between attackers and defenders, with current efficiencies favoring attackers in the short term.
- Expanded Attack Surface: The integration of AI introduces new vulnerabilities across model inputs, plugins, data pipelines, and vendor ecosystems, making every component a potential exposure point.

AI in Offensive Operations

- Malicious Applications: State-aligned actors and cybercriminals have used large language models for phishing, malware development, and disinformation, as documented in multiple campaigns.
- Autonomous Attacks: Research shows that AI models can theoretically execute entire attack sequences, such as ransomware, without human intervention.
- Prompt Injection Vulnerabilities: Attacks like "EchoLeak" exploit the way language models process input, leading to data exfiltration and other risks through prompt injection, an architectural flaw rather than a simple bug.

AI as a New Attack Vector

- Integration Risks: AI tools with privileged access (to data, code, or communications) can escalate a single compromise into a systemic breach, as seen in incidents like the Salesloft-Drift OAuth token breach.
- Unpredictable Expansion: Each AI agent or integration unpredictably extends an organization's digital footprint, increasing the potential for compromise.

HET CYBERLANDSCHAP OP AI

Defensive Potential and Limitations

- AI for Defense: Agentic AI systems, such as OpenAI's Aardvark, can autonomously audit code and suggest patches, signaling a shift toward AI-driven defense.
- Unproven Reliability: Despite promise, current AI defense tools are not yet reliable replacements for specialized security solutions and require careful security measures themselves.

Business and Geopolitical Risks

- Economic Instability: Many AI companies operate at significant losses, raising the risk that enterprises may lose access to unsupported or withdrawn AI tools if vendors fail.
- Geopolitical Asymmetries: Reliance on AI platforms hosted in specific countries introduces exposure to state influence, regulatory changes, and diplomatic tensions, especially amid global competition.

Strategic Recommendations

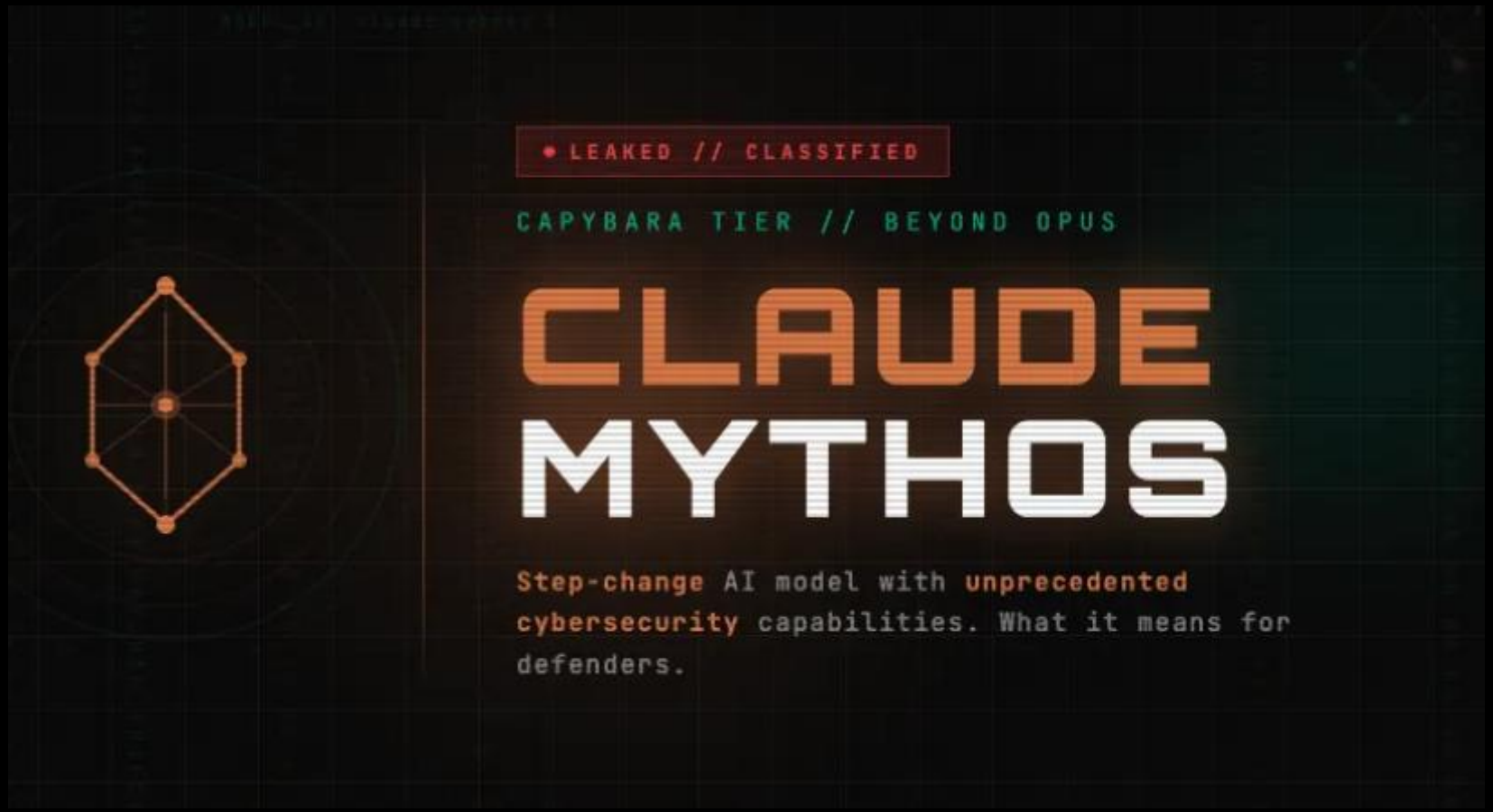
Balanced Approach: AI should be treated as both an opportunity and a liability, requiring deliberate, well-governed adoption and a clear understanding of its limitations.

Dedicated Security Controls: Every AI model and agent should be managed as a privileged asset, with strong controls, audit trails, and continuous monitoring to mitigate risks.

Long-Term Risk: AI's deep integration into enterprise infrastructure makes it a persistent risk that must be addressed as part of overall security strategy.

HET CYBERLANDSCHAP OP AI

HET CYBERLANDSCHAP OP AI



HET CYBERLANDSCHAP OP AI

Subject: You have an issue with your billings info
From: Support <support@teeela.zendesk.com>
To: [redacted]
Reply-to: Support <support+id550989@teeela.zendesk.com>
Date: Aug 11, 2023, 7:03pm ET

UPDATE REQUIRED ACCOUNT IS ON HOLD

Dear Customer,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account here.
2. Choose your preffered plan and enter your payment details.

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

If you need any assistance or have questions about your subscription, our Customer Support team is available 24/7 to help. You can reach us through the live chat on our website, or you can call us at 1-800-123-4567.
Thank you for choosing Netflix as your streaming partner. We've dedicated to making your viewing experience better every day, and we hope you continue to enjoy the world of entertainment we offer.

Dear Customer,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account here.
2. Choose your preffered plan and enter your payment details.

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

If you need any assistance or have questions about your subscription, our Customer Support team is available 24/7 to help. You can reach us through the live chat on our website, or you can call us at 1-800-123-4567.
Thank you for choosing Netflix as your streaming partner. We're dedicated to making your viewing experience better every day, and we hope you continue to enjoy the world of entertainment we offer.

HET CYBERLANDSCHAP OP AI

1.Recon
Research, identification and selection of attack targets

3.Delivery
Transmission of payload to target environment

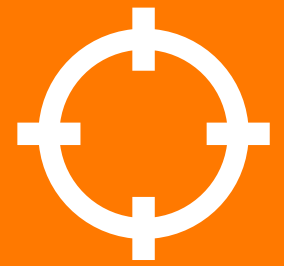
5.Install
Deploy the payload within the target environment

7.Action
Leverage the compromised asset to achieve the target objective

2.Weaponize
Build attack plan and selecting the tools for the job

4.Exploit
Leverage vulnerable assets to push the objective

6.C&C
Establish control of the targeted asset for remote control



DE CIJFERS

orange Cyberdefense

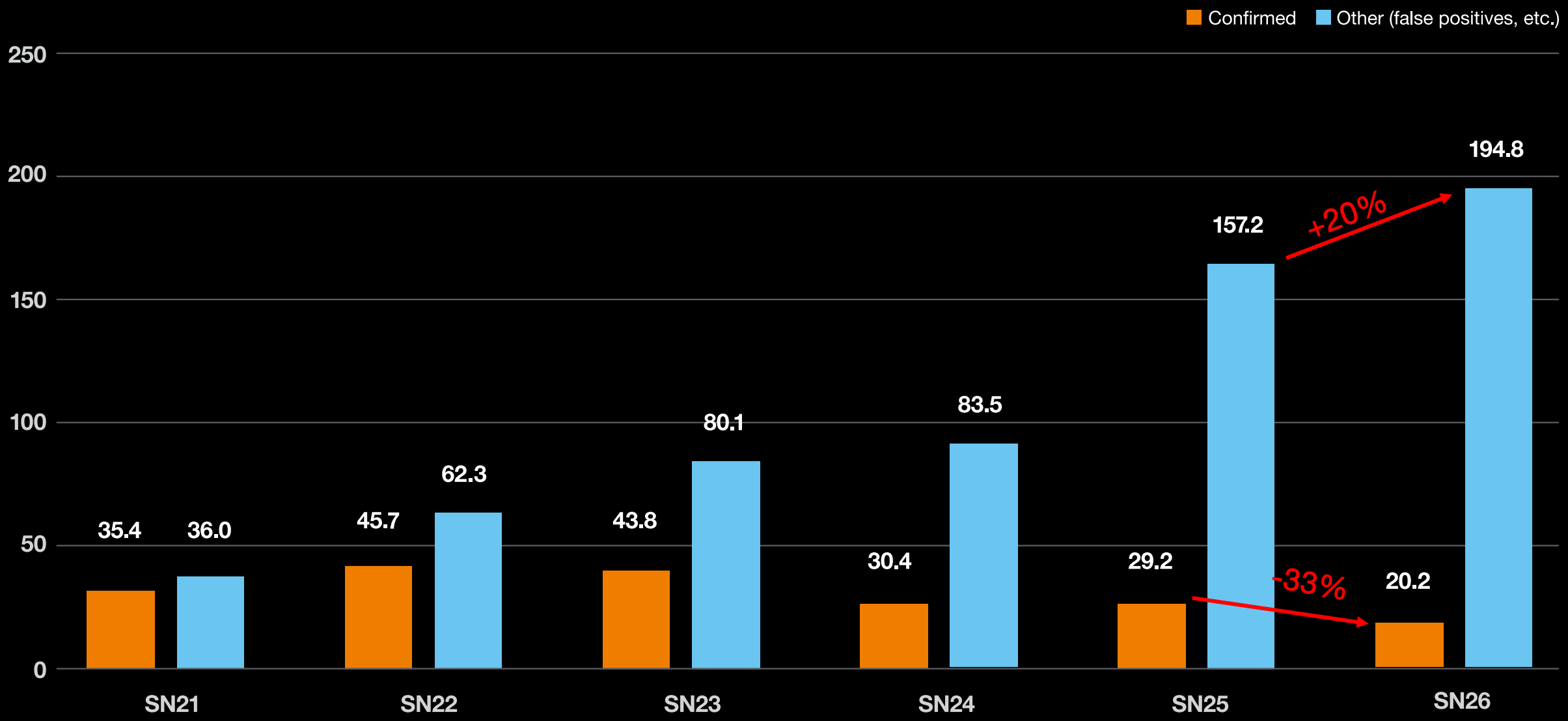
Professionals read the
Security Navigator

- Get the ‘big picture’ of cybersecurity
- 100% first-hand information from the 18 SOCs and 14 CyberSOCs of Orange Cyberdefense
- Gain invaluable insights into the threat landscape
- Expert reports and technology reviews
- Check vulnerabilities, attack patterns and statistics for your business size and vertical

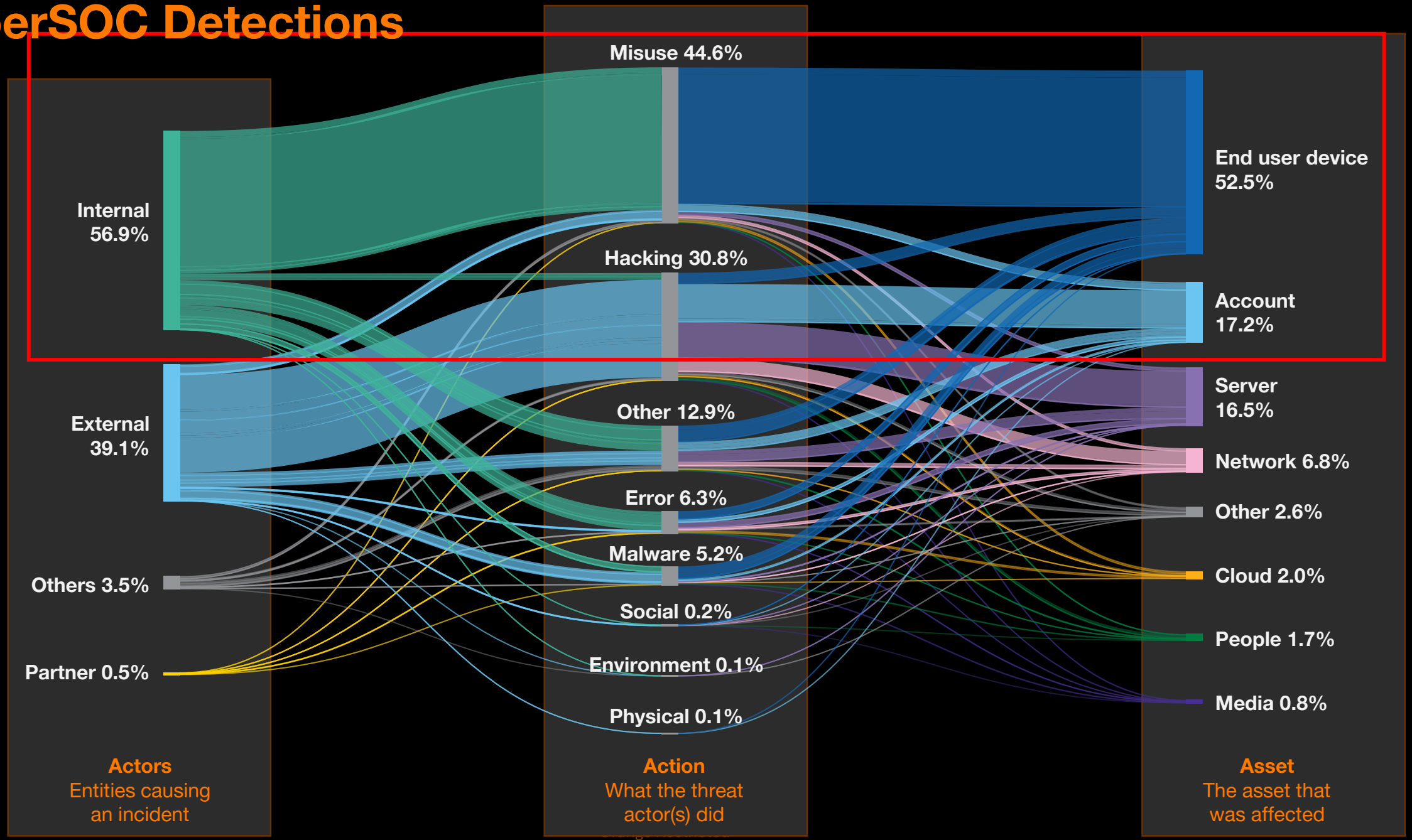
www.orangecyberdefense.com/global/navigator/

Detections per Month per Client

Detection Efficiency for Clients Older Than 36 Months Over Time

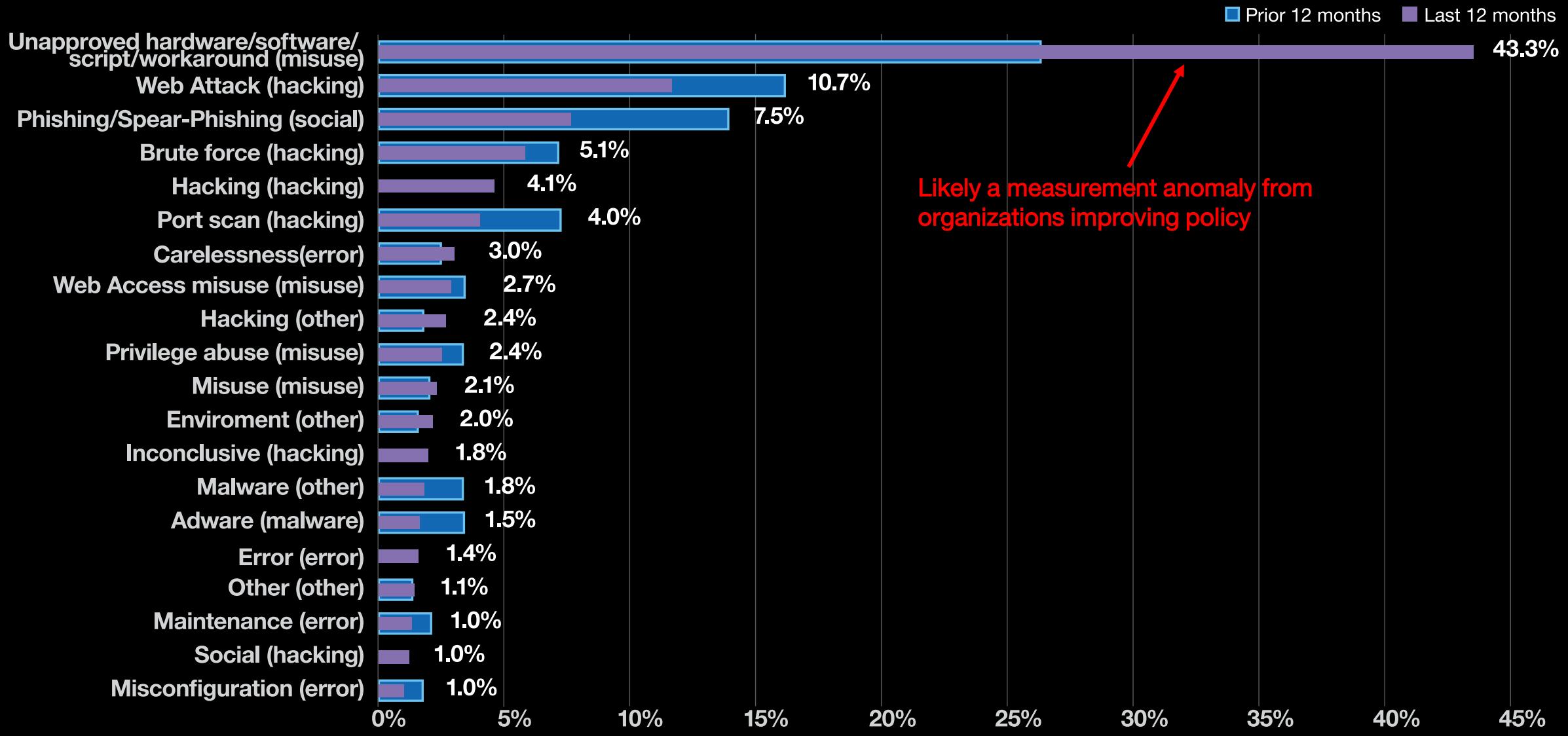


CyberSOC Detections

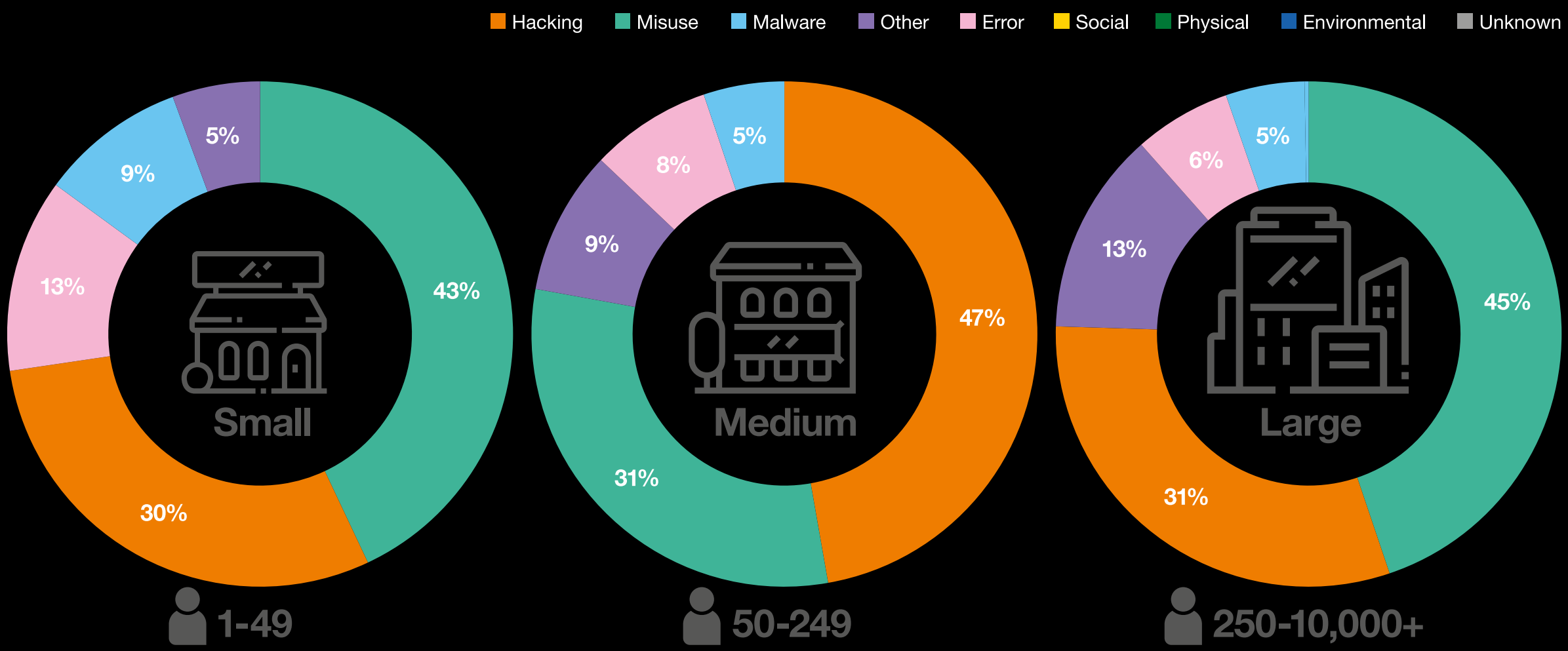


Detection Threat Actions in Detail

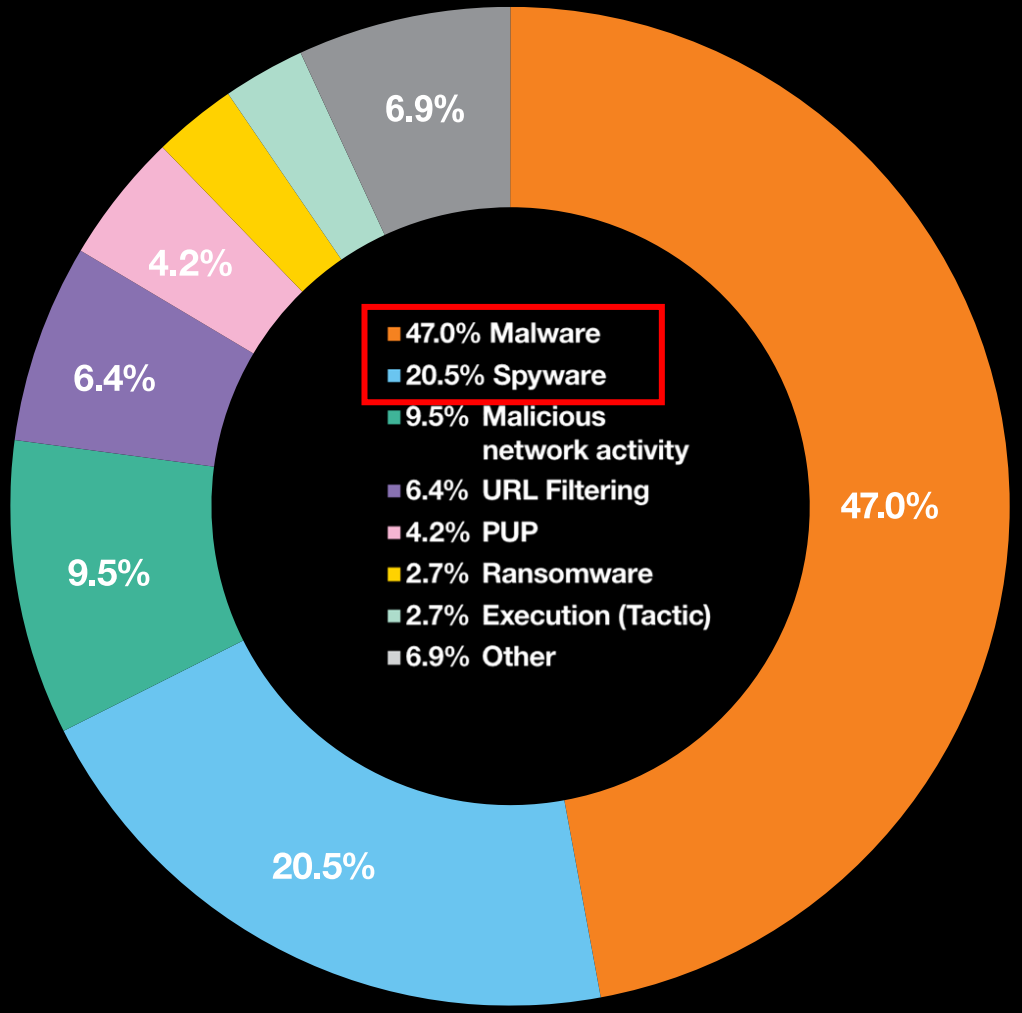
Top 20 Threat Action and Threat Action Level 2 Combined



Detection Actions by Business Size



True Positive Detections by Classification (for SMB)



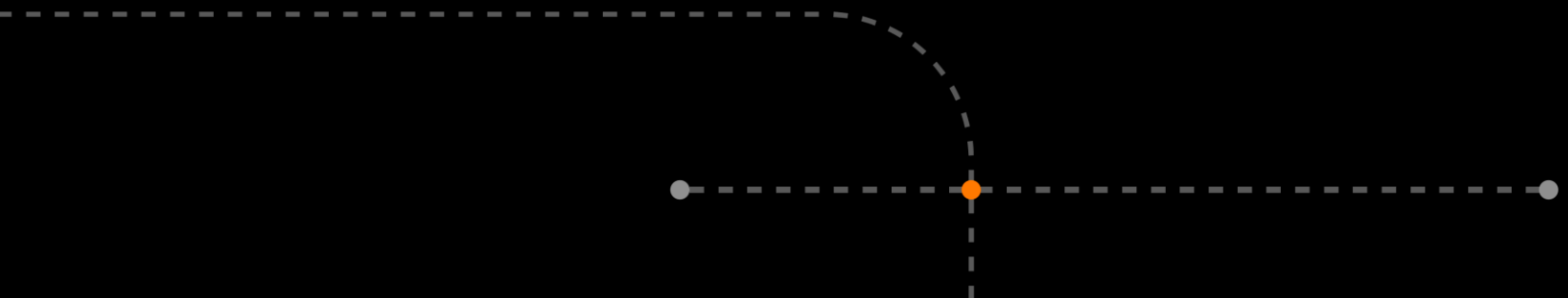
DE CIJFERS

Conclusie:

- Er is veel verschil tussen alle detecties en alle incidenten
- Cyberdreigingen komen zowel van extern, als intern
- Security Hygiëne blijft saai maar effectief

orange Cyberdefense

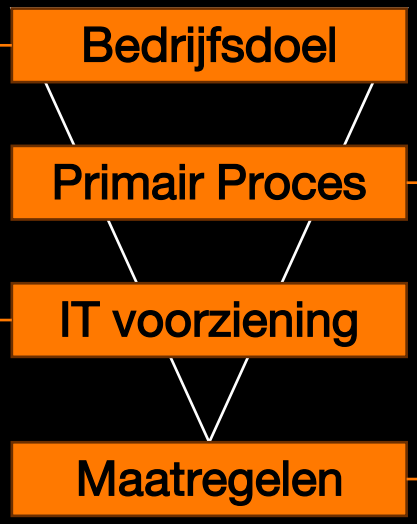
Workshop Time!



DE WORKSHOP

We gaan de verkorte versie doen van de methodologie die grote internationale organisatie gebruiken om hun IT landschap veilig te houden. Deze oefening dient periodiek herhaald te worden om de digitale weerbaarheid van jouw organisatie op niveau te krijgen, en houden.

Voor deze oefening laten we verplichte maatregelen op basis van wet- en regelgeving buiten beschouwing



1. Wat is het hoofddoel dat jouw organisatie bestaansrecht geeft?

Denk bijvoorbeeld aan waar je inkomsten vandaan komen. Ben je een stichting? Denk dan ook aan de verwachtingen van je donateurs!

2. Wat is het proces waarmee je jouw bedrijfsdoel realiseert?

Een groenteboer wil verkopen, maar moet daarmee ook inkopen. Zijn Primaire proces begint dus bij de inkoop en eindigt bij de verkoop.

3. Welke IT systemen gebruikt dit proces?

De groenteboer heeft natuurlijk een betaalsysteem. Maar omdat het inkoop proces ook nodig is, zal hij ook op een manier zijn bestellingen doen.

4. Welke maatregelen moeten we nemen om deze systemen te beschermen?

Voor alle belangrijke systemen willen we een Preventieve, Detective en Correctieve maatregel.
Als voorbeeld:
Preventief: USB porten deactiveren op de kassa
Detectief: een Anti-Virus oplossing op de kassa
Correctief: Een contract met de leverancier om binne 24 uur een nieuwe kasse te leveren (in de tussentijd kunnen we door met Cash)

Voor een overzicht van alle aanvalstechnieken waar je maatregelen op kan overwegen, ga naar: https://attack.mitre.org/

Cyberdefense

Circle Back & Share