black hat
MIDDLE EAST AND AFRICA

QATAR CHAPTER – 974sec

JAN 27th 2024

black hat
MIDDLE EAST AND AFRICA

OPENING REMARKS

```
rami.shaath@BlackHatMEA2023 ~ # whoami

++++++++++++++++++++++++++++++++++++++

 [+]  Based in Middle East for the 15+ years
 [+]  Senior Threat Intelligence Analyst at CROWDSTRIKE
 [+]  Career background span between blue team and intelligence
 [+]  Started my career working as network admin “Intern”
 [+]  Founder of infosec community “971sec”, since 2016, ~300 members
 [+]  BlackHat MEA UAE Co-Chapter Lead
 [+]  Mentoring Cybersecurity Students

++++++++++++++++++++++++++++++++++++++
```

black hat
MIDDLE EAST AND AFRICA

.:agenda:.

- Community Annoucements
- Two Presenations
- Networking Sessions / Breaks
- Group Photo
- Survey | QR Code

black hat
MIDDLE EAST AND AFRICA

.:house rules:.

- Chatham House Rule, anyone in here is free to use information from the discussion without attributing the comment to the person

black hat
MIDDLE EAST AND AFRICA

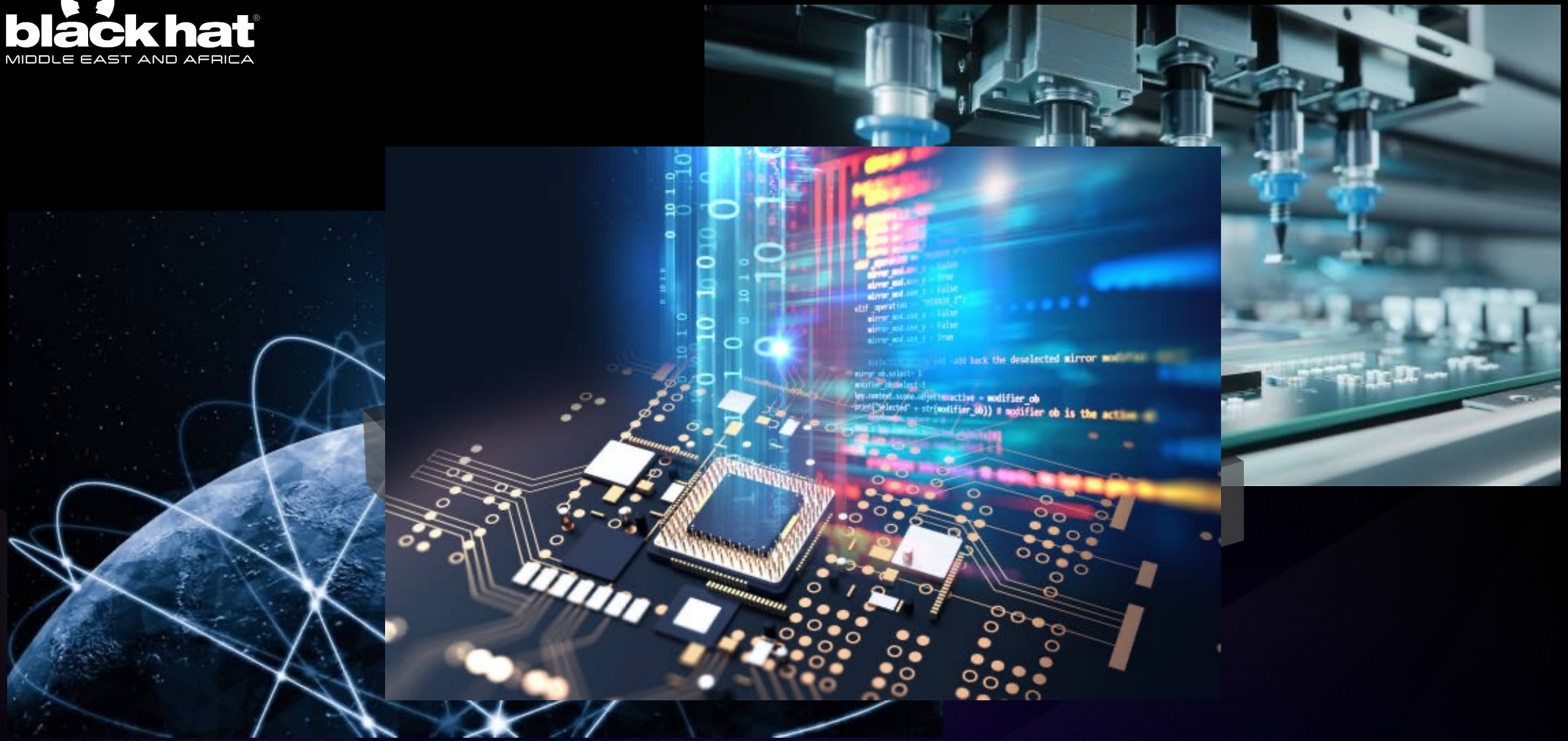
.:talks:.

- Rami Shaath | *There is no "I" in Intel* – the pillasrs of a successfull intelligence program management
- Dindo Geron | *Ransomware Preparedness* – Intro to Cyber Insurance as part of your incident response management

black hat
MIDDLE EAST AND AFRICA

WHO.ARE.YOU

black hat
MIDDLE EAST AND AFRICA



INTEL: WHAT IT IS / NOT

WHAT IS NOT INTELLIGENCE…

- It is not forecasting nor future telling
- it is not simply True or False, Yes or No
- It is not just indicators of compromise (IOCs) and intel feeding into systems
- It is not just malware, signatures, and rules
- It is not about who published more information
- It is not about making an assessment from a single news article
- It is not a one person team
- It is not personal or biased
- It is not the same assessment or outlook from various intel providers
- It is not just “Cyber Threat”
- It is not set and forget
- It is not just only short term

WHAT IS INTELLIGENCE…

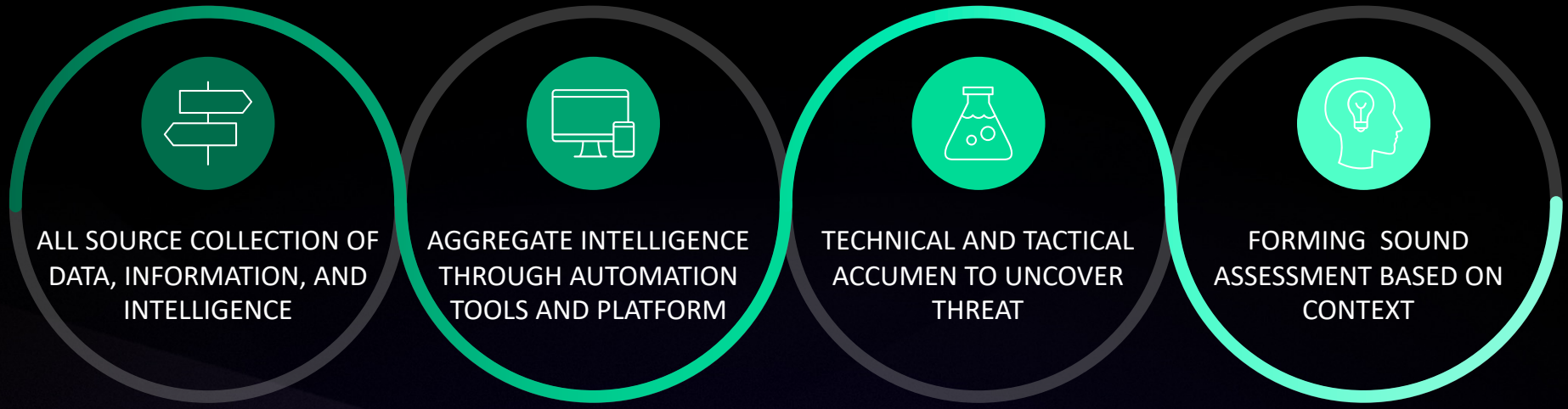
- There is no 'I" in an intelligence team.
- Tactical, Operational, and or Strategic
- Intelligence is a feedback loop consisting of planning, collection, processing, assessment, production & dissemination
- Intelligence is intended to continuously provide timely answers, and insight on situations or events, to decision makers to act accordingly
- Intelligence can be used to identify Disinformation and/or Misinformation outliers
- Intelligence is actionable
- Intelligence is context
- Intelligence is the ability to articulate what matters most to your audience
- Intelligence from multiple intelligence service providers/sources are ideal
- Intelligence empowers businesses

THE PILLARS

black hat
MIDDLE EAST AND AFRICA


4

black hat
MIDDLE EAST AND AFRICA



01 THE COLLECTION

02 THE AUTOMATION

03 THE RESEARCH

04 THE ASSESSMENT

THE FOUR PILLARS

THE COLLECTION:

- All-source collection of data, information, intelligence curated into geo-political/worldwide, sector/industry, cybersecurity/technology events, situations, and incidents.

THE RESEARCH:

- Technical and tactical acumen of a threat. The ability to disassemble, fingerprint, uncover and discover existing or new techniques a target intrusion.

THE AUTOMATION:

- The heart of the Intelligence Lab. The automation of tools to aid in ingesting, intersecting, identifying and interfacing with all-sources data sets and information to identity patterns, group information, and cluster activities.

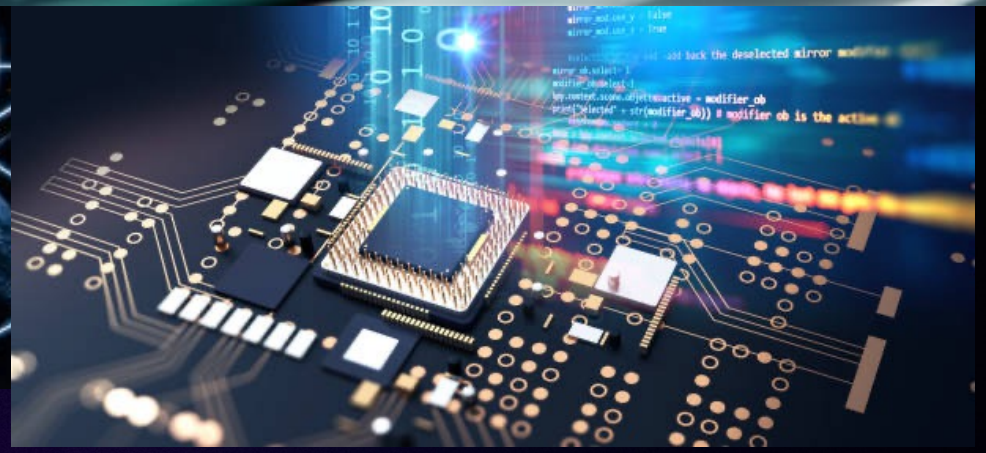
THE ASSESSMENT:

- Finished Intelligence (FINTEL) is comprised of an assessment and analysis of a threat, the likelihood of the threat, and the threat target scope. Priority Intel Requirements (PIR) along with Essential Elements of Information (EEI) provide context and focus to threat that matters.

black hat
MIDDLE EAST AND AFRICA

WHO.ARE.YOU.AGAIN


Livebox
Internet OK
orange



black hat
MIDDLE EAST AND AFRICA

THREAT NOTICE

black hat
MIDDLE EAST AND AFRICA

SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security

January 10, 2023 CrowdStrike Intelligence Team Counter Adversary Operations

CROWDSTRIKE

- In December 2022, CrowdStrike reported on a campaign by SCATTERED SPIDER, targeting organizations within the telecom and business process outsourcing (BPO) sectors with an end objective of gaining access to mobile carrier networks.
- In the weeks since that post, the CrowdStrike Falcon® platform prevented a novel attempt by SCATTERED SPIDER to deploy a malicious kernel driver through a vulnerability (CVE-2015-2291) in the Intel Ethernet diagnostics driver.
- The activity exploits a well known and pervasive deficiency in Windows security that enables adversaries to bypass Windows kernel protections with the Bring-Your-Own-Vulnerable-Driver tactic.
- CrowdStrike Services has observed the actor attempting to bypass other endpoint tools including Microsoft Defender for Endpoint, Palo Alto Networks Cortex XDR and SentinelOne using more traditional defense evasion techniques targeting Windows registry hives.

ADDITIONAL (OSINT) INDUSTRY REPORTING REVEALS…

ADVERSARY MOTIVATION

Financially Motivated / Sophisticated eCrime Adversary

ACTIONS ON OBJECTIVES

Currency Generation via Ransomware Op (RaaS) Affiliates

OPERATIONS / CAMPAIGNS

Credential Harvesting Campaign, Elaborate Lures and SIM Swapping

TTP & TRADECRAFT

Bring-You-Own-Vulnerable-Driver (BYOVD) and MITRE ATT&CK MAP

TOOLS & MALWARE

POORTRY and STONESTOP

VULNERAIBLITIES

CVE-2015-2291

SECTORS & INDUSTRIES

Telecommunication and Business Process Outsourcing (BPO) entities, and Opportunistic

TARGETED REGIONS

North America,
Europe,
Asia

black hat
MIDDLE EAST AND AFRICA

CONTEXT IN INTELLIGENCE

ADDRESSING THE “SO WHAT?”

(MOCK) THREAT ADVISORY

ACME-TIA-2023-11-321 | eCrime Actor Targeting ACME with Credential Harvesting Campaign

Based on multiple industry reports, the Intelligence Team identified SCATTERED SPIDER, a sophisticated financially motivated threat actor, actively targeting entities in telecommunication sectors in various countries/regions our company operates in. SCATTERED SPIDER’s objectives are theft of sensitive data, currency generation by leveraging ransomware on compromised targets and or to broker remote access for profit to other threat actors.

ADDRESSING THE “SO WHAT?”

ACME-TIA-2023-11-321 | eCrime Actor Targeting ACME with Credential Harvesting Campaign …cont’d

The Intelligence Collection team has obtained phishing emails samples, and malware samples (ie POORTRY and STONESTOP) associated with SCATTERED SPIDER. The phishing campaign leverages elaborate lures for credential harvesting and malware for evading endpoint defenses. The Intel Security Research team have confirmed these findings. The Security Operation Center team have implemented mitigation strategies as per the actionable intelligence provided. Monitoring is on-going.

ADDRESSING THE “SO WHAT?”

ACME-TIA-2023-11-321 | eCrime Actor Targeting ACME with Credential Harvesting Campaign …cont’d

Business units, along with Governance, Risk and Compliance (GRC) team, confirms 35% of the purposed-built hardware product v3 sold to our telecommunication customers are vulnerable to SCATTERED SPIDER exploitation tactics (ie Bring-Your-Own-Vulnerable-Driver). The intelligence security research team were successful in proving the exploitation in the vulnerability (ie CVE-2015-2291) found in our internet-facing product.

Upon successful exploitation, SCATTERED SPIDER, or other threat actors, can leverage the remote monitoring and management (RMM) tools embedded in our product, likely resulting in supply chain compromise of our cloud and backend infrastructure, impacting our business and other customers worldwide.

The assessment in this advisory was produced by our intelligence analysis team and is made with high confidence based on analysis of multiple reliable sources. Threat level set to ELEVATED. Threat briefing is scheduled to provide situational awareness.

black hat
MIDDLE EAST AND AFRICA

INTELLIGENCE OVERLOAD

THE RULE OF THREE

NICE TO KNOW:

- For awareness or informational purposes and it may be limited. Threat is unfolding
- Of interest to your company but low prevalence. Specific engagement with internal teams
- Alerting as per periodic discretion (General Advisory)

MUST AND SHOULD KNOW:

- For awareness and informational purposes where threat has the likelihood of impacting the business indirectly. Threat level set to GUARDED
- Tracking the situation as it develops. Research where there are gaps, if needed
- Alerting those are likely impacted (Advisory Report)

ACT NOW:

- Threat is actively targeting. Threat level set to ELEVATED. Full engagement with taskforce
- Threat has the likelihood of impacting the business directly
- Alerting concerned team / business units. Execute SOPs and Playbooks following through actionable intelligence (Alert Notice)

black hat
MIDDLE EAST AND AFRICA

THANK YOU!

Questions and Answers