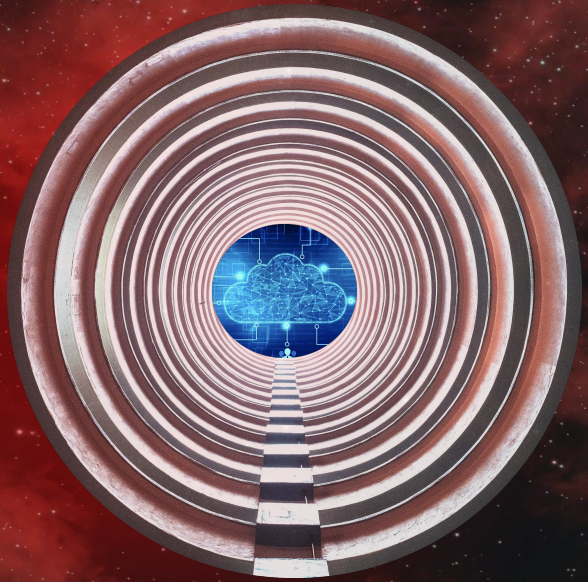
Threat Intelligence for the Cloud



Nitin Sharma

CyberSecurity and DevSecOps Engineer

LinkedIn: linkedin.com/in/nitins87

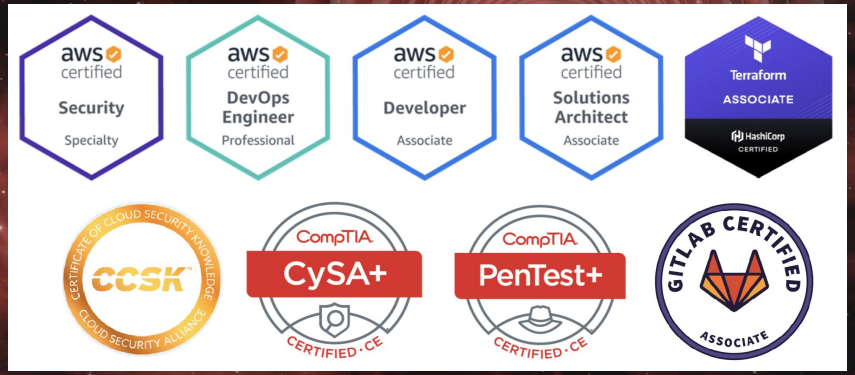
Quora: quora.com/profile/NitinS-1

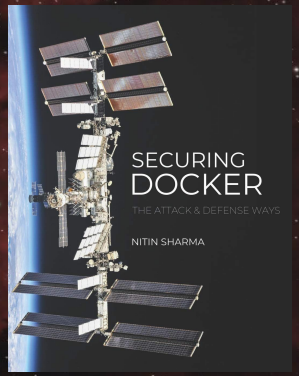
Blog: 4hathacker.in

Contents

$ whoami

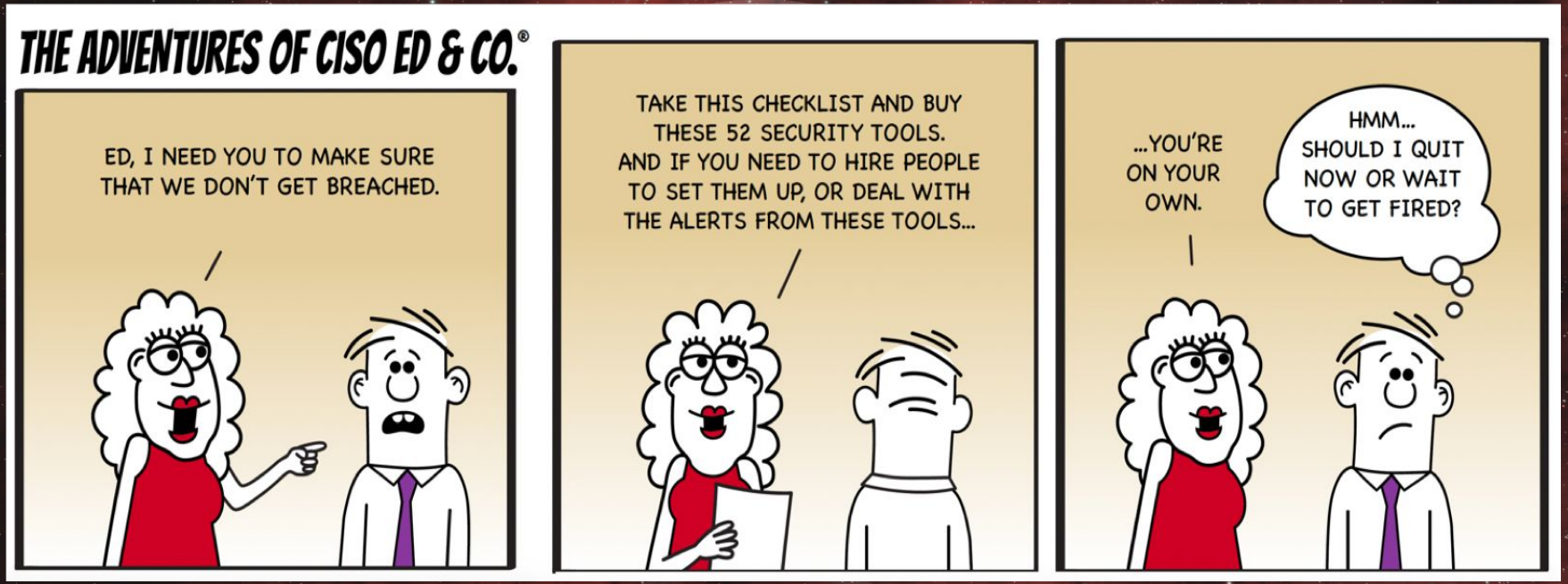
- Cybersecurity and DevSecOps professional experienced in Cloud Security, Container Security and DevOps Research.
- Certifications:





- Published Author for "Securing Docker - The Attack & Defense Ways" book under CyberSecrets Publication
- Half Marathon Runner, Cyclist and Fitness Enthusiast
- Helping out beginners in Cloud, DevOps and CyberSec at Quora

$ UNEXPECTED Ground Reality...



(Source: Balbix)

$ Cyber Threat Intelligence and Risk

- According to NIST, **cyber threat** can be defined as,

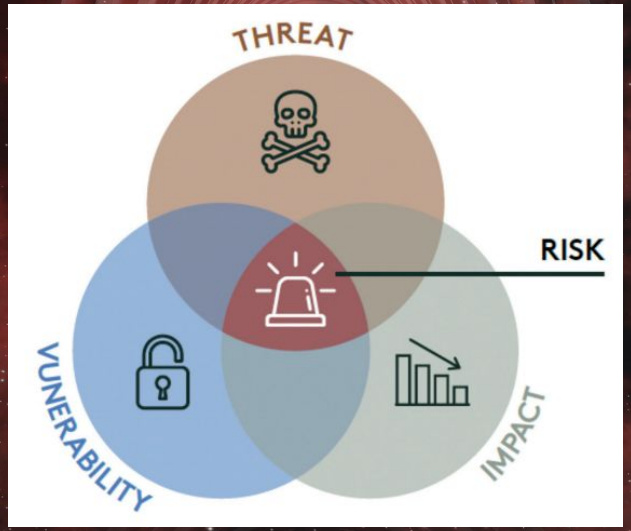
"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."

- According to CIA,

"**Intelligence** is knowledge and foreknowledge of the world around us - the prelude to decision and action…"

$ Cyber Threat Intelligence and Risk

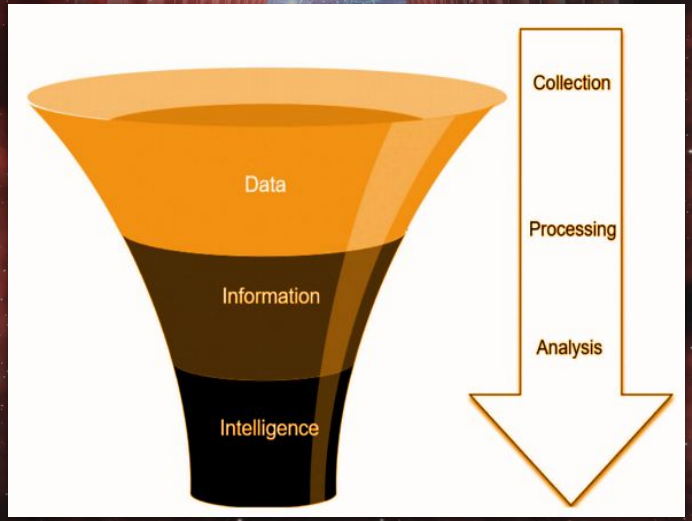
- When an organisation knows how to answer key questions regarding the threats it faces – such as **who** is likely to target **what** assets, **where**, **when**, **how** and **why** then they stand a much better chance of defending themselves.



(Source: CREST Cyber Threat Intelligence)

$ Data vs Information vs Intelligence

- **Data**: simple facts available in large volumes. Eg. logs.
- **Information**: useful output from collated data. Eg. logs showing spike in suspicious activity.
- **Intelligence**: processing and analysis of information that helps in decision making.



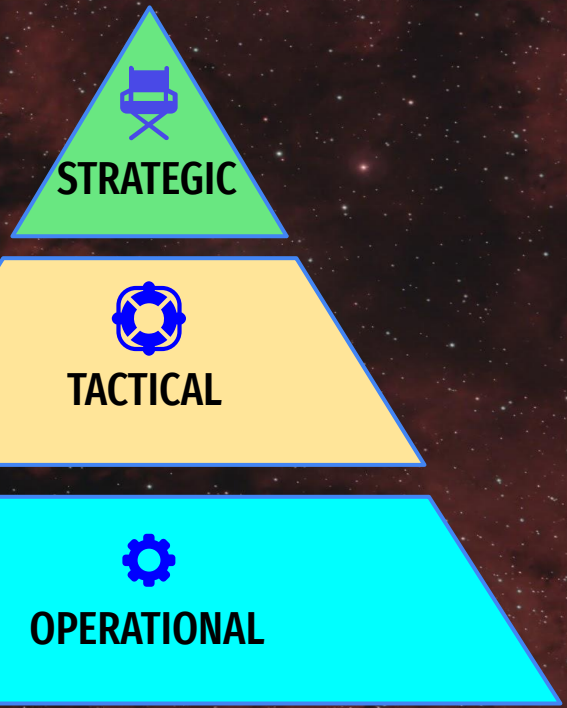
(Source: CREST Cyber Threat Intelligence)

$ Types/Levels of Threat Intelligence

Plain Language, business risk focused,less frequent, for senior decision makers only.
STAKEHOLDERS: C-Suite & Mgmt.

For signature based and proactive systems, combination of human and machine readable formats.
STAKEHOLDERS: DFIR & Threat Hunter team

Large volume, impending attacks, machine and human-readable, for network defenders.
STAKEHOLDERS: SOC Analyst, SIEM, IDS/IPS, F/W, etc.



$ Cloud Threat Landscape

The Notorious Nine

1. Data Breach

2. Data Loss

3. Account Hijacking

4. Insecure APIs

5. DoS Attack

6. Insider Threat

7. Cloud Abuse

8. Insufficient Due Diligence

9. Shared Technology Issues

$ Cloud Threat Landscape

- EE1: Data Breaches
- EE2: Misconfiguration & Inadequate Change Control
- EE3: Lack of Cloud Security Architecture and Strategy
- EE4: Insufficient Identity, Credential, Access and Key Management
- EE5: Account Hijacking
- EE6: Insider Threat
- EE7: Insecure APIs
- EE8: Weak Control Plane
- EE9: Metastructure and Applistructure Failures
- EE10: Limited Cloud Usage Visibility
- EE11: Abuse and Nefarious Use of Cloud Services

$ Cloud Security & Threat Scenario

Capital One

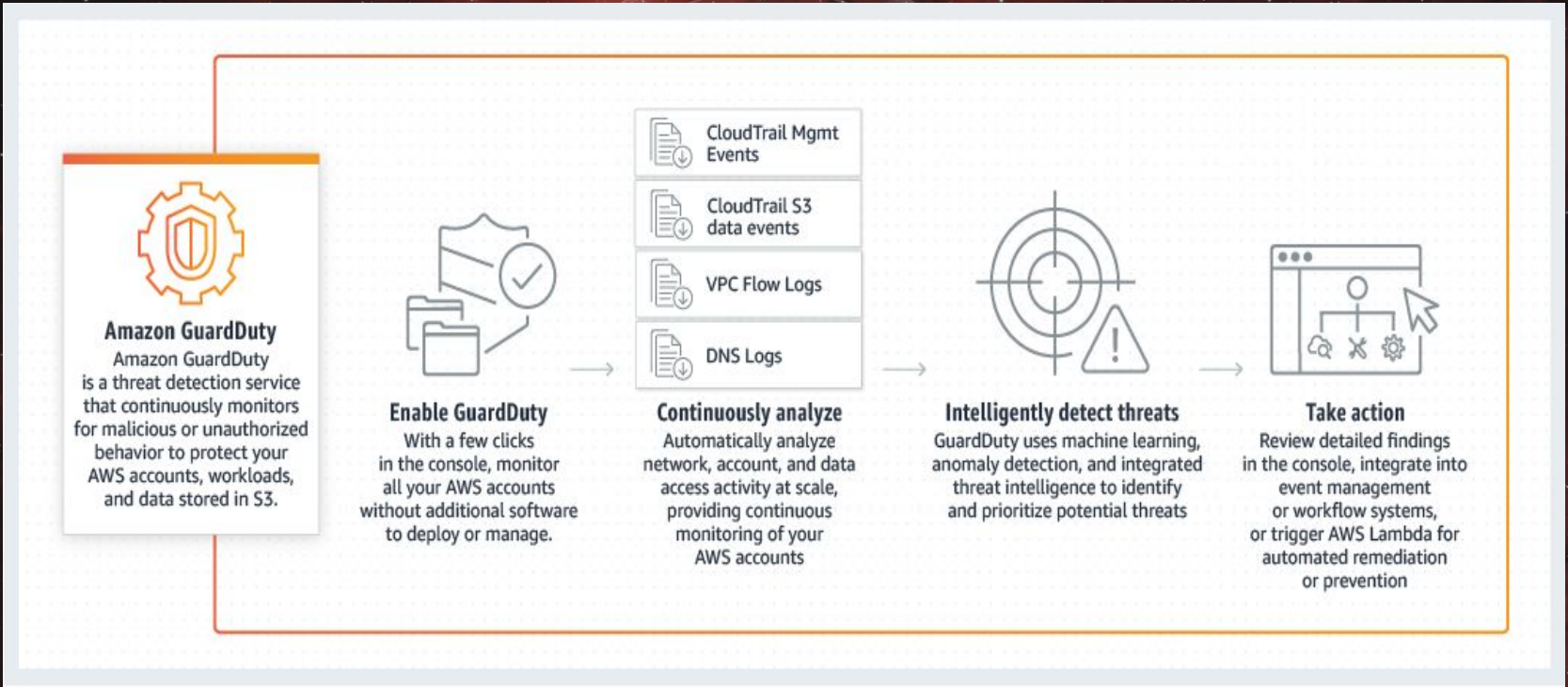
Threat actor	Threat	Vulnerabilities	Technical impacts
Internal: Less Experienced Cloud Architects, Less Experienced Solutions Architect.	**EE1** *Data Breach:* Attacker exfiltrated sensitive information from 106M customer accounts.	**EE 2** *Misconfiguration and Inadequate Change Control* - ModSecurity Web Application Firewall allowed Server-Side Request Forgery (SSRF).	**EE9** *Metastructure and Applistructure Failures:* default hypervisor trust allows service discovery and interrogation
	EE11 *Abuse and Nefarious Use of Cloud Services:* VPN and anonymous network services used to manipulate identity.	**EE4** *Insufficient Identity and Credential Management* - overprovisioned EC2 and S3 roles for WAF and storage.	Over privileged cloud application exposes protected cloud storage and allows access to too much data.
External: *EE5 Insider Threat* - Former CSP Trusted Insider with intimate knowledge of AWS operations.	**Complicated Environment** Intimate knowledge requirements for correct implementation and configuration decisions.	**EE8** *Weak Control Plane* - AWS allows meta data interrogation.	PII from 106M consumer credit applications are exfiltrated.
		EE10 *Limited Cloud Usage Visibility* - AWS IMDS v1 vulnerability to SSRF attack was unknown or not addressed.	

(Source: Top Threats to Cloud Computing: Egregious Eleven Deep Dive)

Actor: Former engineer of AWS with insider knowledge on platform vulnerabilities gained credentials from a misconfigured web application to extract sensitive information from protected cloud folders.

Attack: Open-source anonymity network (Tor) and VPN services (iPredator) hides attacker. Misconfigured ModSecurity WAF relayed AWS cloud metadata services including credentials to cloud instances. Over privileged access given to the WAF allowed the attacker to gain access to protected cloud storage (AWS S3 buckets) with the ability to read data sync and exfiltrate sensitive information.

$ Threat Intel with Cloud Fabric Service: AWS GuardDuty



(Source: Amazon GuardDuty Documentation)

$ Threat Intel with Cloud Fabric
Service: AWS GuardDuty

DEMO REVIEW...


Thank You...
ROCHESTON® REINVENT
CYBERSECURITY CONFERENCE
July 23rd - 25th 2021