M T W T F S S
Page No.:
Date:
YOUVA

24/09/2022
W2

module-6

# Cyber Threat Intelligence

⇒ Cyber threat Intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace.

## ↳ Today's Security Drivers

- Breached Records
- Human errors
- IOT Innovation
- Breach cost Amplifiers (3rd party-costliest factor)
- Skills gap

→ average size of 25,575 records of data breach ($150/record)

→ Insider threats

- negligence
- criminal Insider
- Credential theft

## ↳ Threat Intelligence Strategy Map

- Collect (Integrate data) - Internal, external, Technical, human, raw, packaged
- Process (put data in context) - normalize, Correlate, Confirm, enrich
- Analyze (find insights and actions) - Investigate, Contain, remediate, prioritize

- Share (Inform decisions) - Personalize based on
  - ↳ who, what purpose
  - ↳ What, how often
  - ↳ what format/medium

→ Tactical

↳ level 1 Analysts : need to support real time monitoring, detection, initial investigation and escalation in SOC

↳ level 2/3 Analysts: support in depth prioritization, investigation, containment and remediation of an IR Team and proactive efforts of experts on threat hunting and counter fraud teams

↓ operational

↳ Operational leaders : help leaders of security operations and IT operations, guide and prioritize day-to-day activities/actions of Reputive technical staff

↳ Strategic leaders : help CISO and other senior leaders allocate resources and make better informed business decisions about managing CyberSecurity related risk to an Acceptable level.

↓ strategic

⇒ Threat Intelligence Sources

- Bleeping Computer
- DARKReading
- Trend Micro
- Krebs on Security
- InfoSecurity Magazine
- X-force Exchang.

M T W T F S S

Page No.: YOUVA

Date:

## Threat Intelligence Platform Capabilities

1. Collect
2. Correlate
3. Enrichment and Contentualization
4. Analyze
5. Integrate
6. Act

Ex: Recorded Future,
FireEye,
IBM X-Force Exchange,
TruStar

## Threat Intelligence is heavily rooted ion one of 3 basic models

- lockheed Martin's Cyber kill chain
- MITRE's ATTACK Knowledge-base
- Diamond model of Intrusion Analysis (2 players) (socioeconomic or sociopolitical payoffs)

## Cyber Threat framework

preperation > Engagement > Presence > Effect / Consequence

## Best practices : Intelligence detection

1. Predict and prioritize Security Weaknesses
2. Detect deviations to identify malicious Activity
3. React in Real time to Exploits.

## Security Intelligence

→ real time collection, normalization, and analytics of the data generated by users, applications, and Infrastructure that impacts IT Security and risk posture of an enterprise.

### Exploit timeline

- prediction/prevention phase
- Reaction/Remediation phase.

## 3 pillars of effective threat detection

- See Everything (Centralized Solution)
- Automate Intelligence (Automate security intelligence)
- Become Proactive (proactively hunt threats)

M T W T F S S

Page No.: YOUVA

Date:

## ↳ Key takeaways

- Visibility - key concern for many organizations.
- concerns regarding privileged user and/or credential abuse
- Endpoint alerts and network alerts devices as top sources of incident-information.
- many orgs have blend of on-premises and cloud environments.

M T W T F S S

Page No.: YOUVA

Date:

W2

25/09/2022

## ⇒ Data Security and protection

↳ Protecting CIA of data: in transit, at rest (DB, endpoints, files)

↳ data protection Attacks

- Deliberate Attacks
  - Hackers
  - DoS
- Inadvertent attacks
  - Operator error
  - Natural disaster
  - Component failure

↳ Top Challenges to keep data secure

- Explosive data growth (more data to manage and protect)
- New privacy regulations (new policies and procedures to implement)
- Operational Complexity (complex resource intensive projects to plan)
- Cybersecurity skills shortage

↳ Common pitfalls

- failure to move beyond compliance
- failure to recognize the need for centralized data security
- failure to define who owns responsibility for data itself
- failure to address known vulnerabilities
- failure to prioritize and leverage data activity monitoring

## Industry specific data challenges

- Healthcare ①
- Transportation ②
- financial markets ③
- Retail ④

→ ①. stores Combination of personal health information and payment card data
· subject to financial standards and regulations
· highest cost per breach

→ ②. combines financially sensitive information and personal identification information

→ ③. most targeted industry
· strong financial motivation
· industry-specific regulations require complex compliance measures

→ ④. highly targeted
· large number of access points in retail data lifecycle.

## Top 12 critical data protection Capabilities

- Data discovery (determine data and its sensitivity)
- Data classification (assign labels based on data type)
- Vulnerability assessment (scan data environments to detect vulns and exposures)
- Data risk Analysis (assign risk levels on data sources to prioritize data)
- Data and file activity monitoring (capture and record real time data accss activity)
- Real time Alerting (detect abnormal activity to identify risk around sensitive data accss etc...)
- Blocking, masking, and quarantining (provide only level of accss to data necessary)
- Active Analytics (develop recommendations for actions to reduce risk)
- Encryption (protect data at rest and in transit)
- Tokenization (encryption - hide data from unauthorized user)
- Key management (centralize key mgt, securely distributed, organized)
- Automated Compliance Report

M T W T F S S

Page No.: YOUVA

Date:

## IBM Security Guardium

- powerful data security and compliance solution that supports a staged implementation.
- Guardium helps to
  1. prevent data breaches
  2. Ensure data privacy
  3. Reduce the cost of Compliance
  4. Identify risk.
- Guardium provides following capabilities
  - database discovery and classification
  - unstructured data discovery and classification
  - vulnerability assessment
  - real time database access monitoring
  - real time unstructured data monitoring
  - real time alerting, blocking, masking, session termination, quarantining and query rewriting actions
  - built in and custom reporting
  - compliance workflow automation
  - out of the box and custom reporting
  - compliance accelerators for industry regulations and standards (GDPR, SOX, HIPAA, Basel II)
  - Configuration auditing
  - Active threat Analytics.

M T W T F S S

Page No.: YOUVA

Date:

↳ Guardium is also

- Transparent, noninvasive, real-time data activity monitoring
- scalable, multitier architecture

↳ IBM Security Guardium Data Encryption

- provides encryption, tokenization and key management capabilities
- Secure assets residing in cloud, virtual, big data and on-premise environments
- Integrated suite of highly-scalable products built on common infrastructure

↳ IBM Security key lifecycle manager

- untralizes, simplifies and automates encryption key management process
- key serving and key lifecycle managment for IBM and non-IBM storage solutions

⇒ IBM Guardium Virtual lab ⇒ create, install, and update a Guardium policy

## ↳ Mobile Endpoint Protection

- IOS → ①
- Android → ②

### ↳ mobile endpoints notables

- Users do not interact directly with the OS
- A series of applications act as a broker between user and OS
- OS stability can be easily monitored and any anomalies reported that present risk
- Anti-Virus software can see apps on devices but not its contents

### ↳ Primary mobile endpoint threats

- System based threats
  - Jailbreaking
  - Rooting
- App based threats
  - phishing scams - via SMS or Email
  - irrelevant hardware access
- External
  - network based attacks
  - tethering devices to external media
  - Social engineering to gain unauth access to mobiles

## ↳ protecting mobile assets

- **MDM** (Mobile device management)
  - control content allowed on devices and restrict access to extraneous, potentially hazardous features

- **App Security**
  - Report on health and suitability of apps, before they make it onto devices

- **User Training**
  - Educating users on threats that can impact them.
  - Especially on BYOD scenarios.

## ↳ Day-to-day operations

- Monitor device OS Versions
- Monitor app installs and versions
- Monitor and enforce encryption
- Distribute secure payloads
- Automate Compliance actions
- Ensure proper NAC policies are enforced.
  - ↳ Network Access Control
- Educate Users regularly
- Update contigency plans
  - ↳ provision for possible event or circumstance

M T W T F S S

Page No.:

Date:

YOUVA

⇒ Virtual lab → IBM MaaS360 Overview for Help Desk Administrators using Androids or IOS Devices

M T W T F S S
Page No.: YOUVA
Date:

W3
27/09/2022

## ⇒ Vulnerability Assessment Tools

### ↳ Vulnerability Scanners Components

- Engine Scanner → performs security checks according to its installed plugins, identifying system info and Vulnerabilities
- Database → stores vulnerability information, scan results and other data used by scanner
- Report Module → provides scan result reporting, such as technical reports for sys admins, summary reports
- User Interface → allows admin to operate the Scanner.

### ↳ Host and Network

↳ Internal: scan is done by running vulnerability scanner on critical components of Network - core router, switches, workstations, web server, database, etc

↳ External: scan is done by running vulnerability scanner on host from the internet.
Eliminate open issues/loopholes before it can be used and exploited.

↳ Common Vulnerability Scoring System (CVSS)

- Base Score – how easy it is to exploit vulnerability and how much damage it can inflict
  - exploitability subscore
    - Attack vector
    - UI
    - attack complexity
    - privileges required
  - impact subscore
    - CIA
- Temporal Score – ranks how aware people are of the vulnerability
  - exploit code maturity
  - Remediation level
  - Report confidence
- Environmental Score – provides customized metric specific to an organization
  - Impact Score
  - security req subscore

↳ Security Technical Implementation Guides (STIGs)

↳ Center for Internal Security (CIS)

- provide guidelines and recommendations for security settings for any application or process.
- 5 critical tenets for effective cyber defense systems are:
  - offense informs defense
  - prioritization
  - Measurements and metrics
  - Continuous diagnostics and mitigation
  - Automation.

⇒ Notable OWASP Vulnerability Tools listing

- https://owasp.org/www-community/Vulnerability Scanning Tools

## ⇒ Port Scanning

### ↳ Port

- Central docking point for the flow of information from a program or the interrut to a device or another Computer in the network and vice versa.
- parking spot for data to be exchanged

- port 20 - data transfer - FTP (UDP)
- port 22 - SSH (TCP)
- port 53 - DNS (UDP)
- port 80 - http (TCP)

### ↳ They can be :

- open, accepted : ping
- closed, not listening : acknowledges its presence and unavailability
- filtered, dropped or Blocked : no response

### ↳ Types of Scans

(Internet Control Message protocol)

- ping : sending ICMP echo requests
- TCP/half Open : deuplive scan . A.K.A SYN Scan .
  : notes connection and leaves target hanging
- TCP Connect : Completing TCP Connection. (slower n noisier)

- UDP : when UDP port scan is run, you send an empty or payload filled packet which gives you a response if port is closed. (only if it is closed)
  : faster than TCP.

- Stealth : quieter TCP Scans and can get past firewalls.
  : can escape IDS.

↳ Tools

- NMAP (CLI)
- ZENMAP (GUI)

⇒ Network Protocol Analyzers

↳ Sniffers : operate at the data link layer.
: they allow users to see all the data contained in the packet
: ex ÷ wireshark

↳ Packet Capture : allows to collect network traffic and translate it into a format that's human-readable.
: monitoring bandwith usage, identifying rogue DHCP servers, detecting malware, DNS Resolution, and incident response

↳ Wireshark uses .pcap files to record packet data that has been pulled from a network scan.

↳ pcaps come in 4 variance
- Libpcap (Linux)
- Winpcap (windows - old)
- PCapng (default, next-gen) - stores data as well.
- Npcap (used by NMAP)

⇒ Security Architecture

- The foundation of robust ~~structure~~ security is a clearly communicated & structure with a systematic analysis of threats and controls
  - build with a clearly communicated structure
  - Use systematic analysis & threats and controls.

- The architecture of a system describes its overall static structure and & dynamic behaviour.

- ISO/IEC 42010:2007 defines architecture as fundamental organization of a system embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.

M T W T F S S

Page No.: YOUVA

Date:

→ Enterprise Architecture ①
→ Solution Architecture ②

↳ ①
- considers wide scope for the whole enterprise.
- shows main components of problem space at very high level with small number of components
- showing generic business processes, proposed generic IT components providing high-level business services.
- encompasses Security Domains and security Capabilities

↳ ②
- Describes main elements of solution
- add content
- describes how specific products or tech are used
- more detailed.
- adds tech perspective

↳ ① → Architecture Building Blocks (ABBs)
- guides development of Solution Architecture
- data Security
- Application Security
- Identity and access management
- Infrastructure and endpoint Security
- Detect and Respond.
- product and vendor neutral
- ~~specifies technical components to implement a function~~
- Captures and defines requirements such as function, data and application

↳ ② → Solution Building Blocks (SBBs)

- Key Security manager
- Certificate Authority
- WAF
- Directory
- Virus protection
- Network IPS
- application firewall
- SPAM filter
- Hardware token
- privilege acess manager
- Incident workflow manager.

↳ Solutions Architecture

⇒ Enterprise Architecture

↳ • High level building blocks giving content
• Don't identify circuit Connectivity
• Doesn't identify tech or products

⇒ Solutions Architecture

↳ Architecture Overview
• provides structure at high level

↳ System Content
• Identifies system boundaries
• Describes external actors
• identify use cases and data

M T W T F S S
Page No.: YOUVA
Date:

↳ Functional / Component Model
- definition of functional components
- Includes data flows and dependencies b/w components within system.

↳ Operational Model
- Definition of physical nodes
- Includes physical connection between nodes

→ Start with a solution architecture with an architecture overview giving an overview of system being developed
→ Continue by clearly defining external content describing boundary, actors and use cases that process data
→ Examine system internally looking at functional components and examine threats to data flow.
→ finally, look at where the function is hosted, the security zones and specific protection required to protect data.

↳ Security Architecture pattern : reusable solution to commonly occuring problem.
: no context; not a design
: vendor specific
: available at all levels of abstraction

# ⇒ Application Security

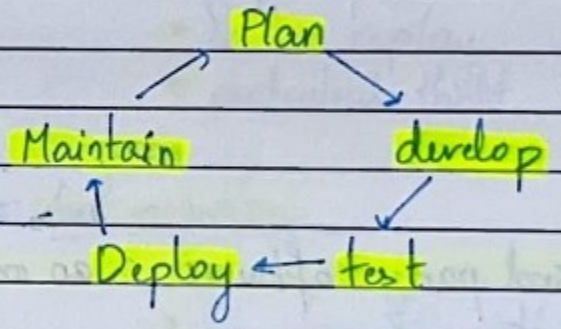
- measures taken to improve security of an app by finding, fixing and preventing security ↓ vulnerabilities.
- protection of application front-ends, source code and information assets at software level.

- Threat: potential for security violation
  : malware and hackers biggest threats

- Risk: liklehood of an attack
  : malware hacker attacking the Confidentiality, Integrity or availability

- Vulnerability: security flaws in code.

## ↳ Software Development Lifecycle




## ↳ Some Common methodologies

- Waterfall → finish week by week
- Iterative
- Agile and Scrum → short burst of analysis, design, coding testing in 1-4 week sprints
- Spiral → series of cycle emaphisis on security

## ↳ Pentesting tools

- Secure Code Analysis tools

  - SAST - Static Application Security testing

    Saurce code Analysis tool

  - DAST - Dynamic Application Security testing

    find visible vulnurabilities by feeding url into an automated scanner

  - IAST - Interactive Application Security testing

    assesses applications from within using software instrumentation.
    Combines power of both SAST and DAST, as well as providing accss to code, http traffic, library information, back-end Connections and Configuration information

## ↳ Third party Software

- while using a 3rd party software in an org one should chuk about
  - → standards
  - → Patching
  - → Testing

  and Conduct a supplier risk assessment.

↳ Important element of Application Security is Web Application Firewall

- filters, monitors and blocks http traffic from and to a web app.

↳ Application Threats / Attacks

- Input Validation
  - Buffer overflow
  - cross-site scripting
  - SQL-Injection
  - Canonicalization
- Authentication
  - Network eavesdropping
  - Brute force and dictionary attacks
  - cookie replay
  - credential theft
- Authorization
  - Elevation / Escalation of privilege
  - disclosure of confidential data
  - data tampering
  - luring attacks

- Configuration management

  - Unauthorized acess to admin interfaces
  - Unauthorized acess to config stores
  - retrieval of clear text config data
  - lack of individual accountability; over-privileged proces and service accounts

- Exception management

  - Information disclosure
  - Denial of Service

- Auditing and logging

  - User denies performing an operation
  - Attacker exploits an application without trace
  - attacker covers his/her tracks

↳ Threat Modelling

process by which potential threats, such as structural vulnerabilities or absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.

↳ methoddigies

1. STRIDE Technology
2. P.A.S.T.A
3. TRIKE
4. VAST

↳ (1) → introduced in 1999 at microsoft providing developers to find threats to our products.

↳ (2) → Process for attack simulation and threat Analysis, seven step risk centric methodology.

↳ (3) → Using threat models as risk management tool.

↳ (4) → Visual agile and simple threat modelling. necessity of scaling threat modelling process across the infrastructure and entire SDLC and integrating it seamlessly into Agile software development methodology.

↳ CERT Secure Coding Standard is a software coding standard for C programming language.

⇒ DevSecOps and Security Automation

⇓

Integrated, automated, continuous security : always

→ Develop Securely

- plan
  - Threat modeling & Risk Analysis
  - Security Backlog
  - Architecture and design
- Code and build
  - Secure app code
  - Secure Infra Configuration
  - OSS/COTS Validation
    - Open-source software
    - Commercial off the shelf
- Test
  - Internal/ External Testing
  - Continuous Assurance
  - Compliance Checking

→ Secure Operations → creation of immutable images

- Release, Deploy and Decommission
  - Versioning of architecture
  - Continuous Component Control
  - App and Infra Orchestration
  - Data Cleansing and Retention

M T W T F S S

Page No.:

Date:

YOUVA

- Operate and monitor

  - Detect and Visualize
  - Respond (virtual patching)
  - Recover

→ Define your operating and governance model early
→ A succesful program starts with people and culture
→ Continuous improvements and feedback

↳ Apply the model to everything-as-Code :

Containers
Apps
Platform
Machines

↳ Shift Security to the left and embrace Security-as-Code

↳ NIST Alignment: Protect

---

## Deploy Securely

→ Orchestrate Everything and include Security
→ Manage Secure creation and distruction of workloads
→ Automate Sign-off to certified levels of data distruction

} Release, Deploy and Decommission

→ If you don't detect it, you can't fix it
→ Integrated operational Security helps ensure the security health of system is as good as it can be with latest information
→ playbooks-as-Code run automatically, as issues are detected they are remediated and reported on

} Operate and Monitor

## Secure Operations.

⇒ **Why DevSecOps ?**

- Reduce risk and cost
- Increase Quality
- Improve Team Synergy
- Enhance Visibility
- Meet Compliance
- Accelerate Development
- Secure, Rapid Innovation

# ⇒ Cross-Site Scripting (XSS)

## ↳ Mitigating Product Security Risk

- prevent new bugs
- Address existing bugs

↳ allows attackers to inject client-side scripts into web page.
↳ can come from anywhere
- HTTP Parameters
- HTTP headers and Cookies
- Data in JSON and XML files
- Databases
- files uploaded by users

↳ XSS can be used to:
- harvest credentials
- Take over user sessions
- CSRF
- Steal Cookies, local store data
- Elevate privileges
- Ridirect users to malicious sites

## ↳ Attack Scenario

- Suppose malicious user enters a script along with name

Jith<script>alert('GOTCHA')</script>

The script runs

- Once the record is added (here), it will be stored in the database, So everytime the list of users is rendered this script will run.
- this is called stored XSS
- retained by application and affects other users.
- Reflected XSS is usually sent as part of an email or malicious link, and affects just one user.

↳ preventing XSS with HTML Encoding

- Output Encoding works well for server side generated pages and is quite effective in neutralizing XSS payloads.

  - HTML Encoding for labels and messages
  - URL Encoding for values stored in ~~lists~~ links
  - HTML encoding alone will not prevent charset attacks
  - To enforce charset > output header: Content-type: text/html; charset=UTF-8
  - Hence, it be no longer will be interpreted.

↳ Preventing XSS with JavaScript Escaping

  - Escaping single quotes will prevent injection
  - x = '-alert(1)-' becomes x = '\'-alert(-1)-\''

↳ Preventing XSS by using DOM Elements

  - Using innerHTML Attribute allows user input to be rendered as HTML and XSS with JS events is possible.
  - Safe alternative is to use textContent or innerText

M T W T F S S

Page No.: YOUVA

Date:

↳ Use Eval and Dynamic Code Generation with Care

- JS eval() function accepts JS expression as a String Argument and executes it. (discouraged and must be avoided)

↳ Input Validation

- Whitelisting
- OWASP XSS Evasion → website shows XSS evasion

↳ Use proven Validation and encoding functionality

- protect both input and output
- Use proven, reputable libraries to validate and encode the input and output
- But to implement a framework that has one central set of functionality that validates and encodes data.

⇒ Notable websites for additional training

- SANS - https://www.sans.org/security-training
- OSCP - https://www.offensive-security.com
- WhitehatSecurity
- OpenSecurityTraining

⇒ Certificates

- EC-Council CEH
- GIAC
- OSCP
- WhiteHat Security

M T W T F S S

Page No.: YOUVA

Date:

W4

29/09/2022

## ⇒ SIEM Concepts and Benifits

↳ Security System information and event management is a data aggregator, search, and reporting system.

↳ Key terms

- log Collection
- Normalization
- Correlation
- Aggregation
- Reporting

↳ Collects logs and other security-related doc for analysis

↳ core function - manage network security by monitoring flows and events

↳ consolidates log events and network flow data from thousands of divius endpoints and apps throughout a network.

↳ two approaches - rule based approach or a statistical correlation engine to establish relationships between logs and entries

↳ Capture log event and network flow data in near real time and apply advanced analytics to reveal security offenses.

↳ can be deployed on-prem or cloud environment.

## ↳ Events and flows

### Events

log of specific action such as user login, occurs at a specific time and event is logged at that time.

### flows

record of network activity between 2 hosts that can last for seconds ~~seconds~~ to days depending on activity within session

eg: web request might download multiple files such as images, ads, videos, and last 5 to 10 seconds, or user using netfix lasting 5-10 hours in a session

↳ **Data Collection**: process of collecting flows and logs from different sources into a common repository
: can & send directly to SIEM or external device collect log data from source and move it to SIEM

↳ **Normalization**: → indexes data records for fast searching and sorting
: turning raw data into formats that has fields such as IP address that SIEM can use
: involves parsing raw data (event) and preparing data to display readable info.

↳ **License Throttling**: monitors number of incoming events to system to manage input flows and EPS licensing.

↳ Coalescing : come together to form one mass or whole

- QID
- Source IP
- Destination IP
- Destination port
- Username

} if all these match in a span of say 3 events then they are coalesced into a single event.

↳ offense
- offence identification (credibility, severity, relevance)
- Activity baseline and monitoring (Activity of user, db, etc)
- Event Correlation (logs, flows, IP reputation, geolocation)

↳ SIEM Deployment

- Compliance
- Cost Benifit
- Cybersecurity

} aspects to take care of while deploying SIEM

↳ Events

- Event Collector

- collects events from local and remote log sources, and normalizes raw log source events to format them for use by SIEM.
- Bundles or coalesces identical events to conserve system usage and sends data to event processor

- Event processor

- processes events that are collected from one or more event Collectors
- processes events by using Custom Rules Engine (CRE)

↳ flows

- flow Collector

- generates flow data from packets and those are collected from monitor reports like a span or tap or sessions like that.
- then data is converted to SIEM flow format and sent down pipeline for processing.

- flow processor

- deduplicates these flows.
- If flow sources are coming into different flow collectors but its the same source, the flow processor will dedupe that.
- Then Asymmetric recombination, ie, combining 2 sides of the flow when data is provided asymmetrically
- license throttling

→ In a SOC, comprising of people, process and Technology, a SIEM sits in the Technology aspect.

↳ tools required

- monitoring
- alerting
- escalation
- investigation
- incident logging
- Reporting

## ↳ SOC Data Collection

- Visibility (feeding everything possible into SIEM)
- Analysis (SIEM must provide its data and imp intelligence)
- Action (actions can be taken based on findings)

## ↳ Deployments

- Gartner defines a small deployment as one with 300 log sources and 1500 EPS (Events per second)
- medium – 1000 log sources and 7000 EPS
- large – 1000 log sources and 15000 EPS

## ↳ Important Concepts

- **SIEM**: Combines Security info mgt and Security event mgt to provide real time analysis of security alerts generated by network/hardware
- **Rule**: programmed procedure that attempts to correlate events and generates new events that report on correlation when it occurs.
- **Rule Threshold**: point at which rule is triggered and a correlation event generated.
- **Event Threshold**: no. of times event must occur before triggering rule threshold.

- **Rule Action**: automatic procedure that occurs when all rule conditions and threshold settings have been met
- **Trend**: is a resource that defines how and over what time period data will be aggregated and evaluated for trends.
- **Event**: log of a specific user action like login, firewall permit occurs at specific time
- **flow**: record of network activity that can last for seconds, minutes, hours or days.
- **Data Collution** • **Normaligation** • **License Throttling** • **Coalescing**

↳ **IBM QRadar Components**

- Vulnerability Manager
- User Behaviour Analytics
- Network Insights

↳ **ArcSight SEM**

- ArcSight Manager
- CORR-Engine (Correlation optimized Retention and Retrieval Engine)
- ArcSight Console
- ArcSight Command Center (ACC)
- ESM Service Layer APIs

M T W T F S S

Page No.: YOUVA

Date:

## SPLUNK

→ offers wide range of products to -

- turn machine data into valuable information by monitoring and analysing all activities.
- known as operational intelligency and is the unique value proposition of Splunk

- example of add on → Distributed management console (DMC) helps put all splunk architecture management together in one set of dashboards.

## LogRythm's Security Intelligence platform

- platform Manager (PM) (centralized management and admin)
- Data Processor (DP) (performs log collection mgt)
- Data Indexer (DX) (indexes data and metadata)
- AI Engine (AI) (correlation and Analysis capabilities)
- All-in-One (XM) (combines PM, DP, DX and AI components)
- Network Monitor (NM) (deep analysis of network traffic contents)
- Data Collector (DC) (collects log data from secure systems and prepares for secure transfer to centralized LogRythm Security Intelligence Platform implementation)

↳ QRadar

- Insider and External threats
- Cloud and Vulnerability risks
- Critical data

- Solve Security Challenges (protect critical data, detect threats, etc)
- Become predictive
- Automate Intelligence (watsonplatform - scours internet for security info to feed into QRadar)
- See Everything
- Deployment models (on prem, as a service, cloud, service)

⇒ User Behaviour Analytics (UBA/UEBA) (→ entity)

- Detecting insider threats require a 360 degree view of both logs and flows.

↳ To get started with UBA

- log source input:
  ↓ parsing properly
- LDAP setup:
  ↓ Reference maps
- User ID Coalescing
- KYUC & Align with Big needs
- Config and tune UCs (systems)

M T W T F S S
Page No.: YOUVA
Date:

## ⇒ Artificial Intelligence and SIEM

- Some pressures being faced today
  - Unaddressed threats → (overlooking information)
  - Insights overlooked → (volume, variety, speed → overwhelming)
  - lack of Cybersec talent (overworked, overwhelmed, etc)
  - Dwell times getting worse (duration a threat actor has undetected access in network until completely removed.)
  - Stakes → very high

- There needs to be a partnership between analysts and their technology. (not mutually exclusive)
- AI teams environment and provides actionable intelligence based on data being fed.

### ↳ Qradar Advisor with Watson → Built with AI for front line Security Analyst

- Some Benifits
  - force multiply your team's efforts (Automate repetitive SOC tasks)
  - Drive Consistent and deeper investigations (gain actionable insights into critical incidents)
  - Reduce dwell times (adopt quicker and more decisive escalation process)

### ↳ How it works

① set up Automatic offense analysis to advisor.

② performs local data mining and learning using observables
③ applies powerful cognitive analytics leveraging external data sources to convert insights
④ provides actionable feedback and content for faster triage decisions.

i.e. Using

① QRadar Security Analytics platform
② QRadar Advisor
③ Watson for Cyber Security
④ QRadar Advisor.

Basically,

① Builds knowledge (internal and external)
② Aligning incidents to ATT&CK chain
③ Cross-Investigation analytics
④ Using Analyst feedback to drive better decisions

⇒ human Expertise → include common sense, generalization, morals, etc...

human Expertise → Artificial intelligence

human Expertise → Security Analysts include Anomaly detection, pattern identification, Data correlation, etc... Data visualization

(W5)

## ⇒ Threat Hunting Overview

08/10/2022

- breaches caused by malicious or criminal acts
- Average 191 days to detect and 66 days to resolve situation.
- too many tools from too many vendors

- # 1 SOC Challenge is the detection of advanced threats (hidden, unknown and emerging)
- Threats → 20% unknown
  80% known

- Threat hunting helps in finding unknown and undetected threats before its too late

↳ Cyber Threat Hunting : The act of proactively and aggressively identifying, interrupting, tracking, investigating and eliminating cyber adversaries as early as possible in the cyber kill chain.
(↗ control situation rather than just responding)
: TTPs → Tactics, techniques and procedures.

↳ Know Your Enemy : Cyber Kill Chain

1. Reconnaissance – gather targets
2. Weaponization – prepare to deliver malware & exploit
3. Delivery – Initiate launch of malware
4. Exploitation – Access targets vulnerabilities
5. Installation – Deploy malware in target environment
6. Command and Control – Manipulate and control remotely.

M T W T F S S

Page No.: YOUVA

Date:

⑦ Actions on Objectives - Take action to achieve goals

↳ Enterprise Insight Analysis (EIA) Capabilities Overview

- Information and Intelligence
- Investigative Analysis tools
- Collaboration and sharing

↳ i2 Cyber Users

- Stakeholder level (CISO, CIO)
- Departmental level (Head of Cyber threat info / Attack Analysis) (Head of SIEM)
- Practitioners (Cyber threat Analysts, SOC Analyst (L2 or L3))

↳ SOC levels

- tier 1 → firewall
- tier 2 → SIEM
- tier 3 and tier 4 → Threat hunting / cyber forensic investigations.

} activity performed in each tier

## ⇒ IBM Virtual lab

### ↳ Why QRadar SIEM?

- collect logs → fed into an asset database
  - ↳ Nflows → SRC/DEST ports, IPs, protocols, applications
  - ↳ Qflows → 1st 64 bytes of each packet to detect
    - User ID
    - SSN
    - PII. etc (Using regex)
  - ↳ Vflows → network flows in hypervisors (for VMs)
- Xforce also a data source (best for IP and URL reputation)
- Bigfix → another data source (feeds latest vulnerabilities)
  - server discovery
- 750 rules → knowledge about things that aren't normal
- Risk Manager → reads config files from
  - router
  - firewall
  - switches (helps detect paths, Network topology. etc)
- Saved Searches
- Vulnerability manager
  - network scanner
  - App scanner
  - DB Scanner

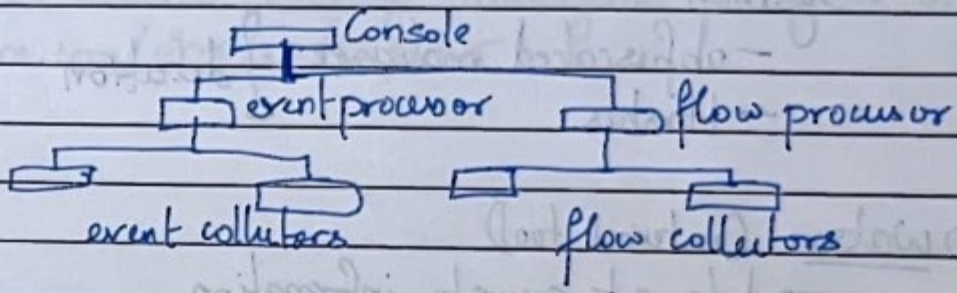
  } fed into Asset DB post scanning
  - finds patches available for the vulnerabilities found using Bigfix
- Activity Recently

- Early warnings
- Accessible from internet

↳ QRadar has a data structure called Reference Sets which are nothing but lists with optional TTL
Contains
- Baseline Users
- fresh passwords

- forensic module → another component of QRadar
- Distributed architecture

↳




EP/FP ⇒ correlation + Storage + Searches.
Data Node ⇒ facilitates fast response time on searches
⇒ does storage + searches
⇒ no license required

↳ Integration Capabilities

- Bigfix – availability patches
- Guardium – No LOG / AUDIT
  – Bidirectional data flow (from QRadar to Guardium and vice versa)
- IPS – right click login
- TRUSTEER APEX – alerts from cloud

- Identity manager using IDI – revoke rule
- Domains (duplicated IP management)
- Multi tenancy → (using single advisor on QRadar to investigate offenses from multiple domains and tenants)
- DSM/Parser — no super knowledge

distributed system management

↳ new updates
- SCAN Data
- full visual
- Automated remediation
- Hashes
- Sysmon
  - obfuscated malware } detection
  - Hashes

↳ Watson (external tool)
- used to get security information

↳ Flows in QRadar

Gigamon
STAP
MIRROR

QFlow
(inspect first 64 bytes & payload)

QRadar incident forensics full packet capture

QRadar Network Insights
→ extract 404 key fields
↳ Compute key attributes
file hash file size

↳ QRadar Network Insights

- forensics (PCAP files)
- flows
- qflows

↳ dynamic detection is possible ie while it is happening not just post mortem

⇒ IBM QRadar Intelligence platform documentation at:

→ IBM QRadar Security Intelligence platform 7.5
→ ibm.com/docs/en/qsip/7.5

⇒ Virtual lab → QRadar Advisor with Watson

→ cognitive applied for Cybersecurity

- ingest mass amounts of data
- classify, select, and normalize data
- NLP for security processing
- training and learning with feedback
- Relational Analysis visualized through knowledge graphs

→ 4 capabilities that make cognitive systems different from traditional ones

- Understand
- Interact
- Reason
- learn

M T W T F S S

Page No.: YOUVA

Date:

## Watson for Cyber Security

- Ingestion → ingesting structured and unstructured data
- Classification and Normalization
- NLP
- Training and learning → ingestion based, SME and Research training
- Knowledge graphs → visualization of large networks of entities
- Data Quality Assessment (using feedback, interrogation and automated learning)
  - Using NLP to classify and normalize raw data and feed only cybersecurity related information.

## Overview of Security Activities

- Threats & Risk Detection → includes IBM QRadar
- Investigation & Qualification → Advisor and Watson come into play
  - Tier 1 Analyst - Security monitoring
    Tier 2 Analyst - Incident escalation / Security Analysts
    Tier 3 Analyst - Threat Hunting
- Incident Response

## QRadar Advisor in action

→ QRadar advisor lives locally in QRadar.
→ We use QRadar to analyze security events, run analytics and run offense itself.

(ex: IP addresses, URL, MD5, filename, etc..)

→ We then use QRadar Advisor for data mining to gain local content and form threat research strategy
→ we then pass these observables (pieces of data) onto Watson residing on a SaaS platform which then extracts information from local threat strategy and performs threat research
→ we then provide these research results back to advisor to apply intelligence gathered to investigate and qualify incident

[QRadar → Advisor → watson → Advisor]

↳ Investigation workflow (IBM Advisor with Watson)

- Blocked / allowed Events and flows
- Malware Blocking and Execution
- Assets
- UBA Users (User behavior Analytics)
- Export of Results

↳ Tuning QRadar for QRadar Advisor

- Network Hierarchy & Defining your Environment
  - 3 valid contents: Local2Local
    : Local2Remote
    : Remote2Local
- Host Reference Building Blocks - Using reference sets
- Tuning Methodology
  - SIEM Tuning Report
  - Modifying Rule tests and threshold

M T W T F S S

Page No.:

Date:

YOUVA

## Best practices for tuning Advisor

- Data sources matter - L2R and R2L data is ✓
- Implement and map custom properties.
- Network Hierarchy is accurate
- Use on offenses that are L2R, R2L, or contain file hashes.
- Known false +ves offenses tuned out.

- Advisor property mapping process
- The observables (IOCs) in your Data are important

## Tuning and Install process

- Study your data sources
- Install and configure Advisor
- Iterate to see if additional tuning helps
  - QRadar Admin needs to get feedback from Advisor end user
  - Examine:
    - event payload for events in an offense, any missed custom property Advisor could use?