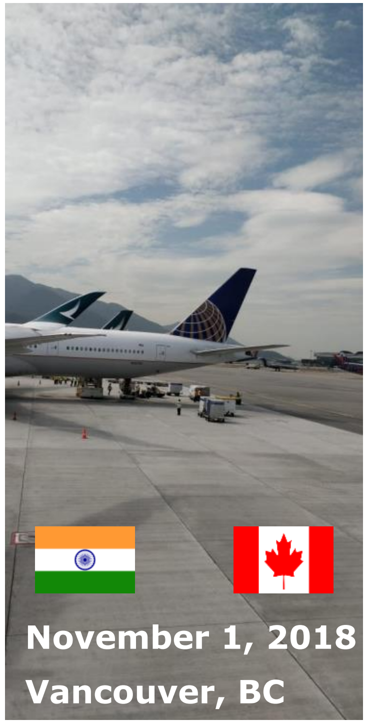
# Get The Basics Right!

# Improving detection capabilities with SIEM

SIEM Summit & Training 2019

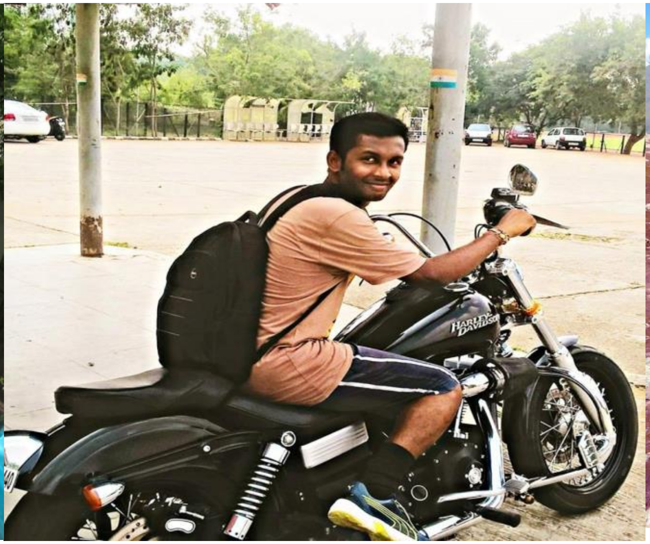
# Balaji Nakkella

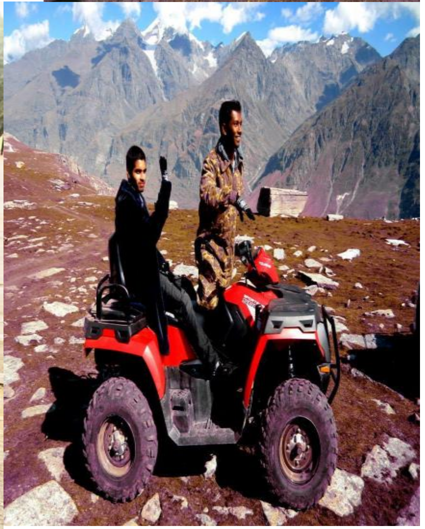


November 1, 2018

Vancouver, BC

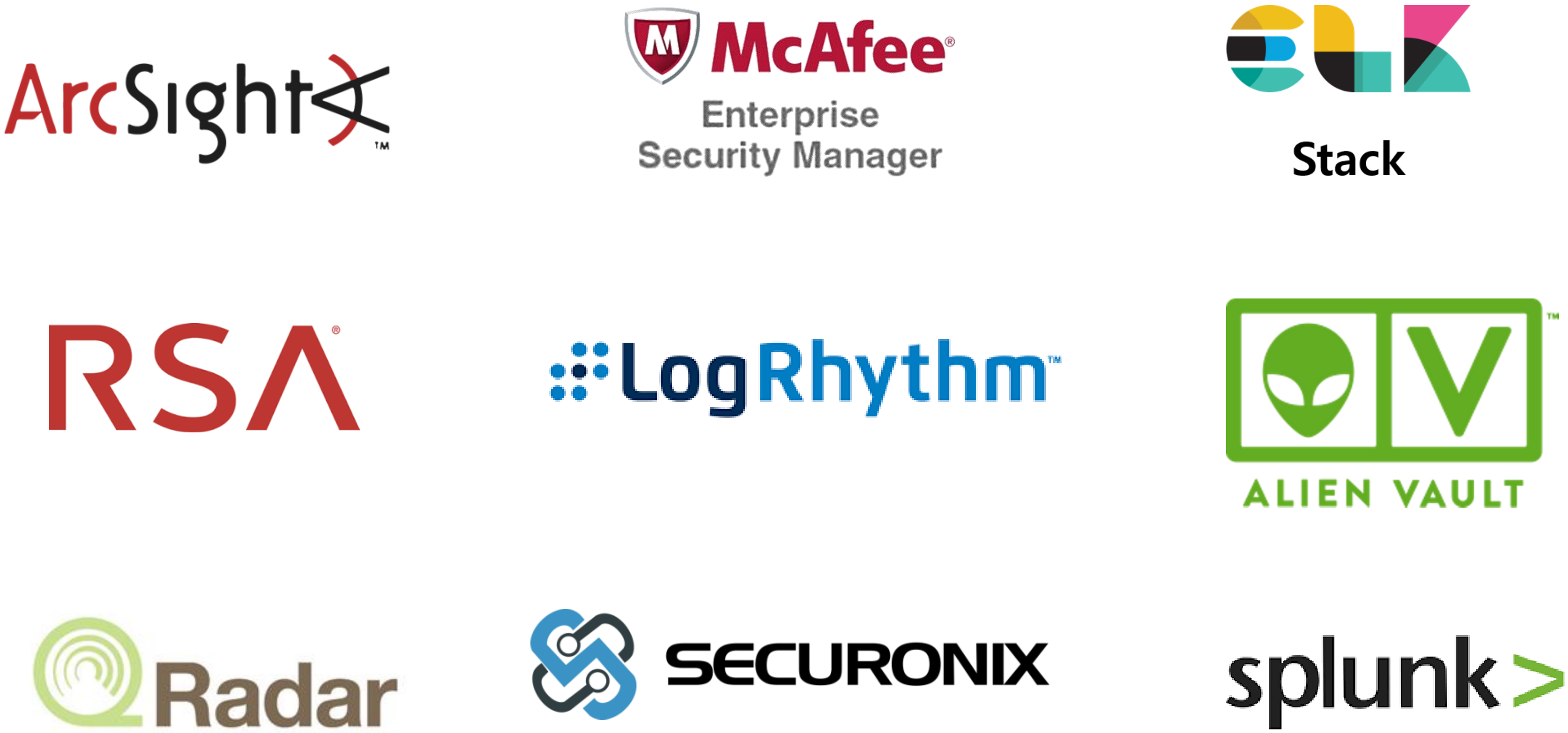
# Rakesh Kumar Narsingoju





# Get The Basics Right!

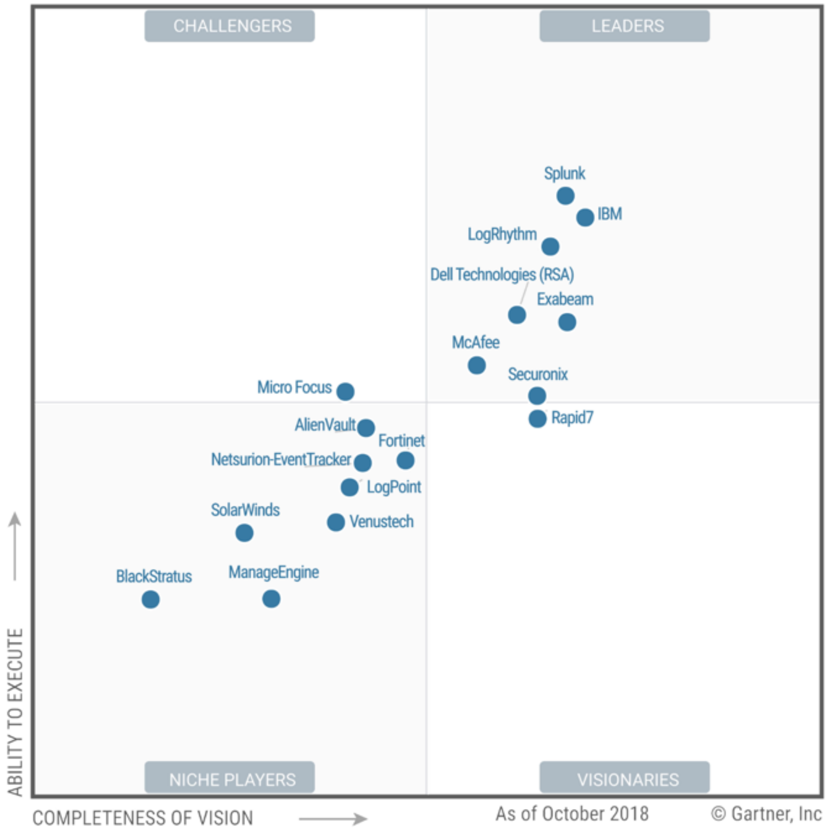
## What/How to choose?



# Get The Basics Right!

## The Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



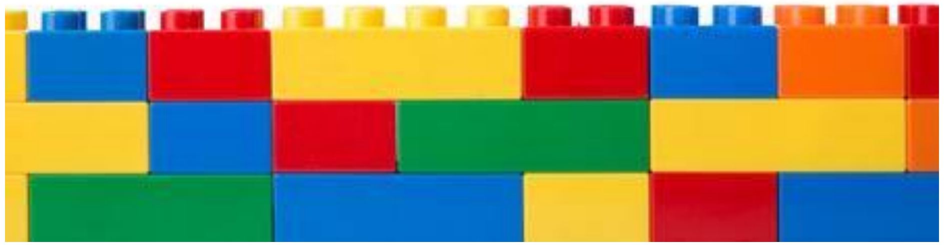
Source: Gartner (December 2018)

# Get The Basics Right!

## Buying a SIEM - What we have

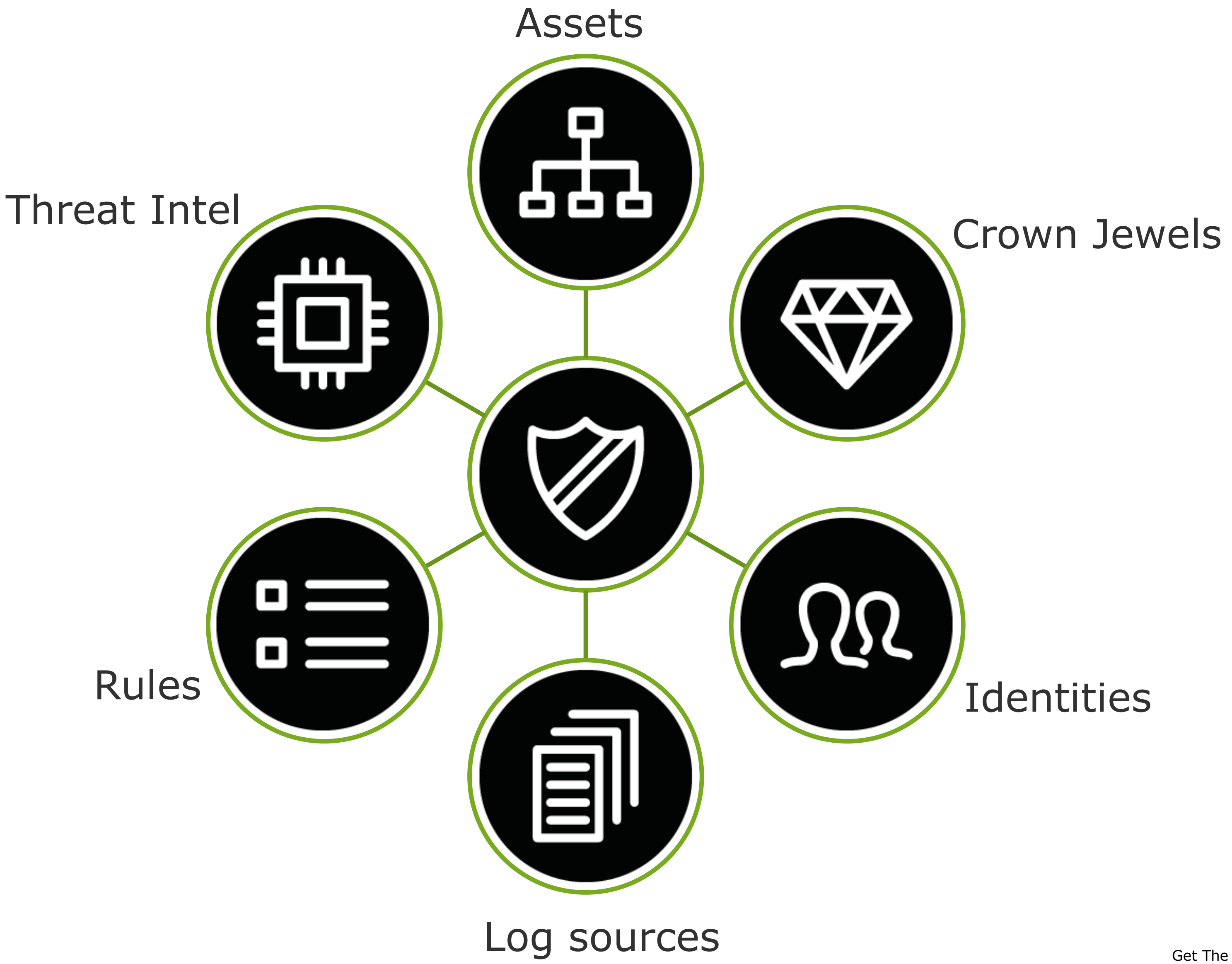
# Get The Basics Right!

## Deployed SIEM - Expectation vs Reality



# Get The Basics Right!

## Key Elements



# Get The Basics Right!

## Key Challenges

1. **Assets** – what to protect
2. **Crown Jewels** – Protecting a pawn vs Protecting a king
3. **Identities** – who are your players
4. **Data Sources** – what to log
5. **Rules –** what to detect
6. **Threat Intel** – whom to rely on

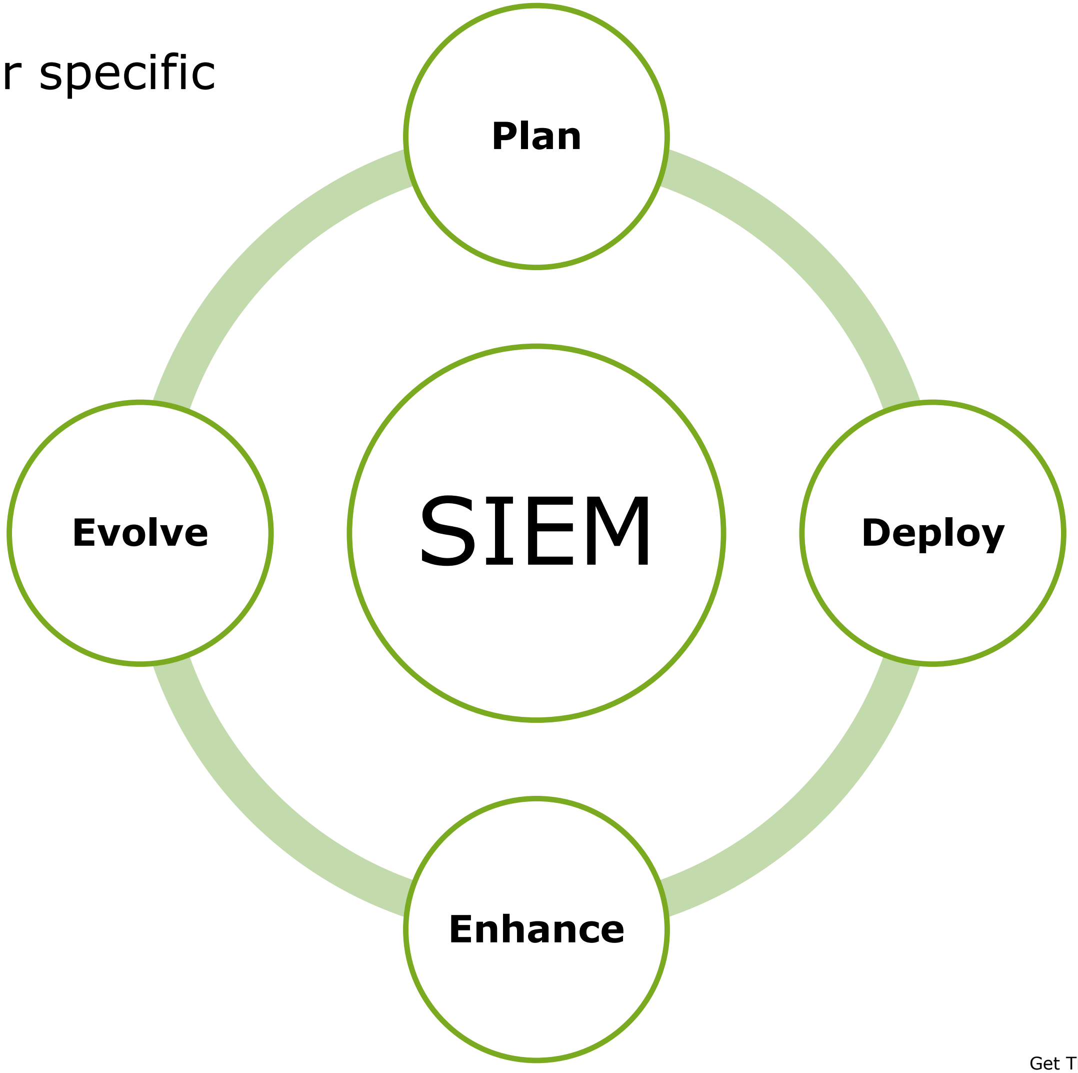
# SIEM Deployment Checklist

## A holistic view

# Improving detection capabilities using SIEM

## SIEM Deployment Life Cycle

- ❖ Neither industry nor vendor specific
- ❖ Non exhaustive
- ❖ Detection centric



# SIEM Deployment checklist

## Phase #1: Plan

❑ Start with Governance, Risk Management and Compliance

| Business Risks | Regulatory Risks |
|---|---|
| | |
| | |
| | |

❑ Review existing Security Controls

| Risks (Business/Regulatory) | Preventive | Detective | Corrective |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Get The Basics Right!

# SIEM Deployment checklist

## Phase #1: Plan

❑ Use of Cyber Security Framework(s)

- ❖ Identify and Review existing frameworks
- ❖ Implement
- ❖ Control/ Program/ Risk Frameworks
- ❖ PCI DSS, ISO, CIS, NIST etc. to start with

❑ Shortlist use cases

| Risk | Use case name | Description | Log source |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Get The Basics Right!

# SIEM Deployment checklist

## Phase #1: Plan

❑ Finalize log sources and their logging levels

| Log source | Logging level |
|---|---|
| | |
| | |

❑ Shortlist Threat Intel feeds

- ❖ Relevance
- ❖ Variety (IPs, Hashes, URLs, Domains)
- ❖ Output format(s)

❑ Shortlist and finalize SIEM products based on requirements

- ❖ In-house skillset

❑ Select Ticketing tool, if required

# SIEM Deployment checklist

## Phase #2: Deploy

- ❑ SIEM Architecture Design based on organization's network architecture
- ❑ Implementation of approved design
- ❑ Data onboarding
  - ❖ Add context to raw logs
  - ❖ Parse – Verify – Ingest
- ❑ Threat Intel feed integration
  - ❖ Test – Deploy
- ❑ Use case development
  - ❖ Develop – Test – Deploy
- ❑ Ticketing system integration

# SIEM Deployment checklist

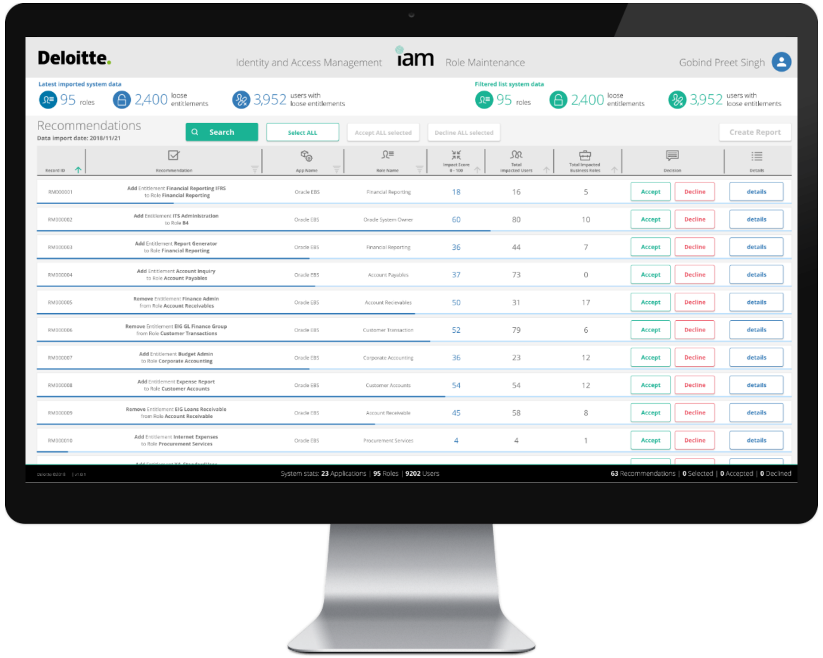
## Phase #3: Enhance

- ❑ Use case Tuning - False positive reduction
  - ❖ Scripts
  - ❖ Security expertise and processes
  - ❖ Analytics
- ❑ Additional detection tools
  - ❖ IPS/IDS (Cisco, PA, FortiGate, Fidelis, Juniper, Checkpoint,...)
  - ❖ Endpoint Detection & Response (CrowdStrike, Carbon Black, FireEye,...)
  - ❖ Email protection (Proofpoint, IronPort, Symantec,...)
  - ❖ AV solutions (McAfee, SEP,…)
  - ❖ Vulnerability Scanners (Qualys, Nessus,…)
  - ❖ Web Proxy(Bluecoat, Websense,…)

# SIEM Deployment checklist
## Phase #4: Evolve

**Deloitte Omnia** – In house AI driven Product development team

### IAM Analytics



Deloitte. Identity and Access Management iam Role Maintenance Gobind Preet Singh

Latest imported system data: 95 roles | 2,400 loose entitlements | 3,952 users with loose entitlements

Filtered list system data: 95 roles | 2,400 loose entitlements | 3,952 users with loose entitlements

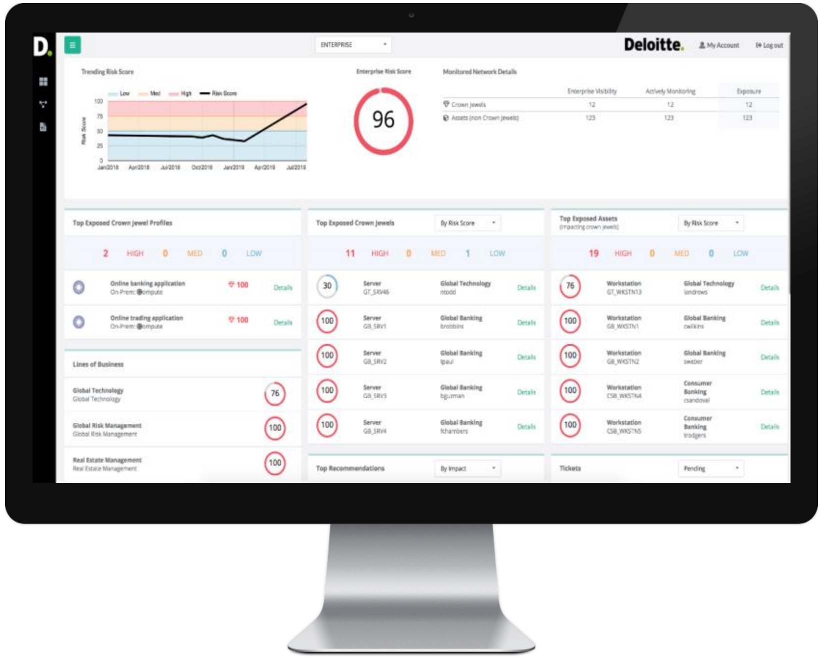
Recommendations
Data import date: 2018/11/21

| Record ID | Recommendation | App Name | Role Name | Impact Score 0 - 100 | Total Impacted Users | Total Impacted Business Roles | Decision | Details |
|---|---|---|---|---|---|---|---|---|
| RM000001 | Add Entitlement Financial Reporting IFRS to Role Financial Reporting | Oracle EBS | Financial Reporting | 18 | 16 | 5 | Accept Decline | details |
| RM000002 | Add Entitlement ITS Administration to Role B4 | Oracle EBS | Oracle System Owner | 60 | 80 | 10 | Accept Decline | details |
| RM000003 | Add Entitlement Report Generator to Role Financial Reporting | Oracle EBS | Financial Reporting | 36 | 44 | 7 | Accept Decline | details |
| RM000004 | Add Entitlement Account Inquiry to Role Account Payables | Oracle EBS | Account Payables | 37 | 73 | 0 | Accept Decline | details |
| RM000005 | Remove Entitlement Finance Admin from Role Account Receivables | Oracle EBS | Account Recievables | 50 | 31 | 17 | Accept Decline | details |
| RM000006 | Remove Entitlement EIG GL Finance Group from Role Customer Transactions | Oracle EBS | Customer Transaction | 52 | 79 | 6 | Accept Decline | details |
| RM000007 | Add Entitlement Budget Admin to Role Corporate Accounting | Oracle EBS | Corporate Accounting | 36 | 23 | 12 | Accept Decline | details |
| RM000008 | Add Entitlement Expense Report to Role Customer Accounts | Oracle EBS | Customer Accounts | 54 | 54 | 12 | Accept Decline | details |
| RM000009 | Remove Entitlement EIG Loans Receivable from Role Account Receivable | Oracle EBS | Account Receivable | 45 | 58 | 8 | Accept Decline | details |
| RM000010 | Add Entitlement Internet Expenses to Role Procurement Services | Oracle EBS | Procurement Services | 4 | 4 | 1 | Accept Decline | details |

System stats: 23 Applications | 95 Roles | 9202 Users

63 Recommendations | 0 Selected | 0 Accepted | 0 Declined

### APM



Monitored Network Details

| | Enterprise Visibility | Actively Monitoring | Exposure |
|---|---|---|---|
| Crown Jewels | 12 | 12 | 12 |
| Assets (non Crown Jewels) | 123 | 123 | 123 |

Top Exposed Crown Jewel Profiles: 2 HIGH 0 MED 0 LOW

- Online banking application, On-Prem: Compute, 100, Details
- Online trading application, On-Prem: Compute, 100, Details

Lines of Business

- Global Technology, Global Technology, 76
- Global Risk Management, Global Risk Management, 100
- Real Estate Management, Real Estate Management, 100

Top Exposed Crown Jewels (By Risk Score): 11 HIGH 0 MED 1 LOW

| | | | |
|---|---|---|---|
| 30 | Server<br>GT_SRV46 | Global Technology<br>rtodd | Details |
| 100 | Server<br>GB_SRV1 | Global Banking<br>brobbins | Details |
| 100 | Server<br>GB_SRV2 | Global Banking<br>tpaul | Details |
| 100 | Server<br>GB_SRV3 | Global Banking<br>bguzman | Details |
| 100 | Server<br>GB_SRV4 | Global Banking<br>fchambers | Details |

Top Exposed Assets (impacting crown jewels) (By Risk Score): 19 HIGH 0 MED 0 LOW

| | | | |
|---|---|---|---|
| 76 | Workstation<br>GT_WKSTN13 | Global Technology<br>landrews | Details |
| 100 | Workstation<br>GB_WKSTN1 | Global Banking<br>cwilkins | Details |
| 100 | Workstation<br>GB_WKSTN2 | Global Banking<br>swebor | Details |
| 100 | Workstation<br>CSB_WKSTN4 | Consumer Banking<br>csandoval | Details |
| 100 | Workstation<br>CSB_WKSTN5 | Consumer Banking<br>trodgers | Details |

Top Recommendations (By Impact)

Tickets (Pending)

# SIEM Deployment checklist

## Attack Path Modelling

- Become more proactive in your strategy and increase the ability to **stop attacks even before they occur**
- Provides current state and **scenario-based analysis of threats** and control failures on technology assets
- Leverages **AI to drive recommendations** that provide a variety of options for remediation and risk mitigation while showing how each action affects your risk score

# SIEM Deployment checklist

## APM – Key Differentiators

**Predict** vulnerable entry points and the path of least resistance

**Visualize** a path an attacker might use to traverse the network

**Identify** vulnerable technology assets leading to increased risk exposure to an attack

**Prioritize** a remediation strategy through risk ranking

**Automate** remediation through integration with orchestration solution

**Develop** simulated attack path models through scenario analysis

# SIEM Deployment checklist

## IAM Analytics - AI Enabled RBAC

- IAM Analytics is **an Artificial Intelligence enabled solution** that closely monitors how end users consume the IAM recommendations.
- We utilize an intuitive GUI that prompts key business context to end users, delivering a **phenomenal user experience.**
- Our state of the art advanced analytics engine is powered with closed loop feedback mechanism **to enable Machine Learning** as we scale operations and is configurable based on your preferences.

# SIEM Deployment checklist

## Current pain points vs IAM Analytics Benefits

Lack of a sustainable role maintenance process potentially resulting in inappropriate access

Human analysis of complex data patterns may lead to sub-optimal role definitions

Time-consuming and manual role definition/maintenance processes result in low operational efficiency

Enhanced logical view of access to help ensure that the right people have the right access

Improved user experience in the organization’s IAM platform, injected with logical and business context

Increased operational efficiency, including reduced administrative effort across business and technology lines

# Scenario #1

## Prioritized Asset and Identity Inventory

# Prioritized Asset and Identity Inventory

## Know “Who” and “What” to protect

# Prioritized Asset and Identity Inventory

## Alert Fatigue

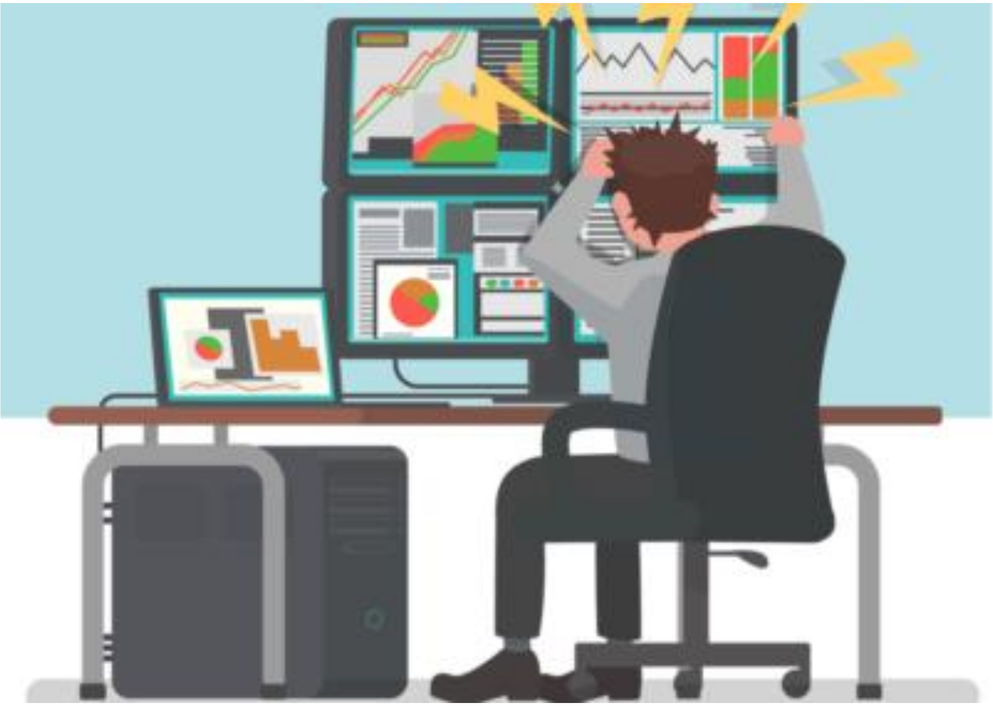
**Old school technique:**

- ❖Assign severities to use cases
- ❖One to one mapping of Severity to Priority
- ❖Minimize SLA breaches

**Drawbacks:**

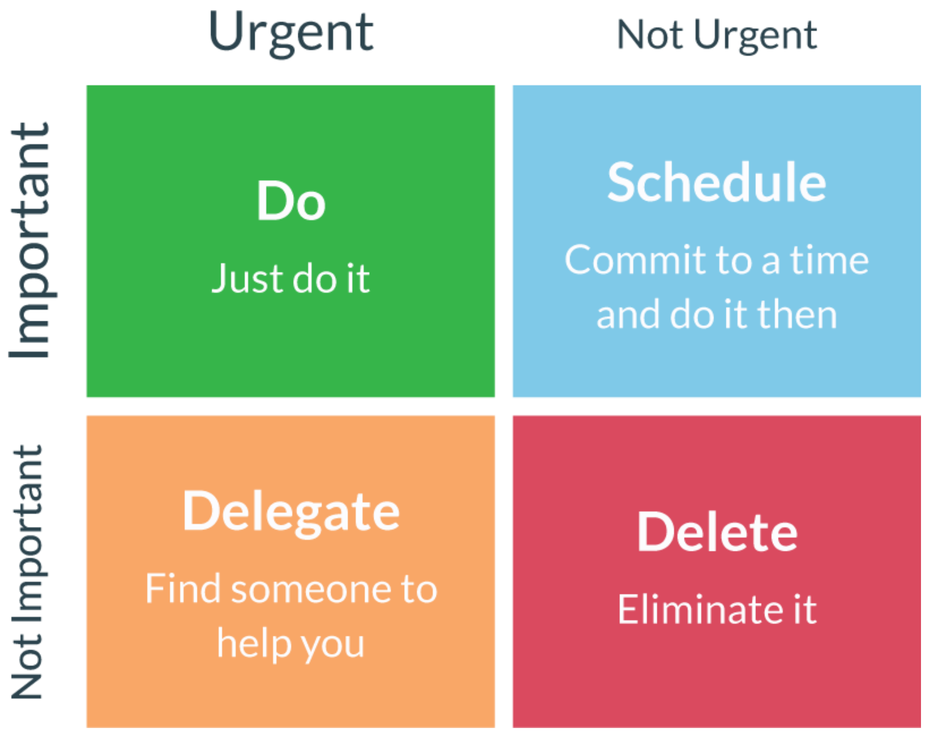
- ❖ SLA breaches/ Higher dwell times

**How do we address?**



# Prioritized Asset and Identity Inventory

## First Things First approach



Urgent

Not Urgent

Important

Not Important

**Do**

Just do it

**Schedule**

Commit to a time and do it then

**Delegate**

Find someone to help you

**Delete**

Eliminate it

|  | S1 | S2 | S3 | S4 |
|---|---|---|---|---|
| C1 | P1 | P1 | P2 | P2 |
| C2 | P1 | P2 | P3 | P3 |
| C3 | P2 | P3 | P3 | P4 |
| C4 | P2 | P3 | P4 | P4 |

**Legend**: C-Criticality, S-Severity, P-Priority

# Prioritized Asset and Identity Inventory

## The *hidden treasure!

### Asset Inventory

| Hostname | IP | MAC | Owner | *Critical (C/H/M/L) | Category | OS |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

### Identity Inventory

| Username | Email | Business Unit | *Role | Domain | Others |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

# Prioritized Asset and Identity Inventory

## Benefits

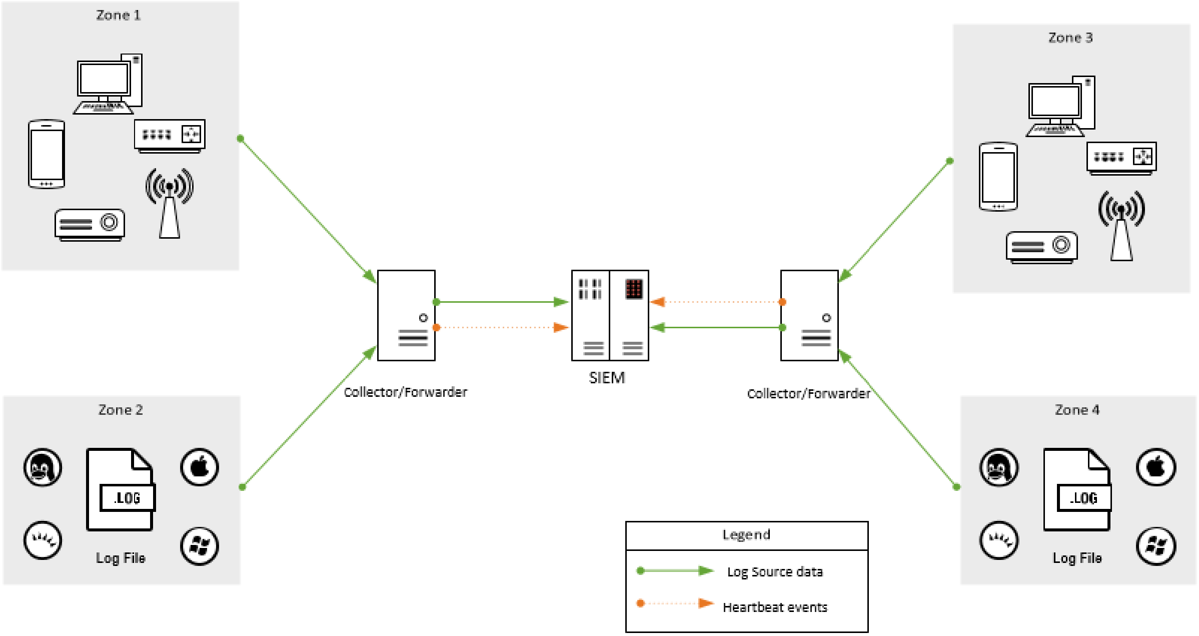
- Event enrichment – False Positive reduction
- Effectively handle alert fatigue
- Prioritized alerts – Reduce dwell time

# Scenario #2

## Health Monitoring

# Health Monitoring

## Scenario



# Health Monitoring

## Scenario

### Why?

- Reporting vs. Non reporting – Compliance
- Avoids potential true positive miss – Security

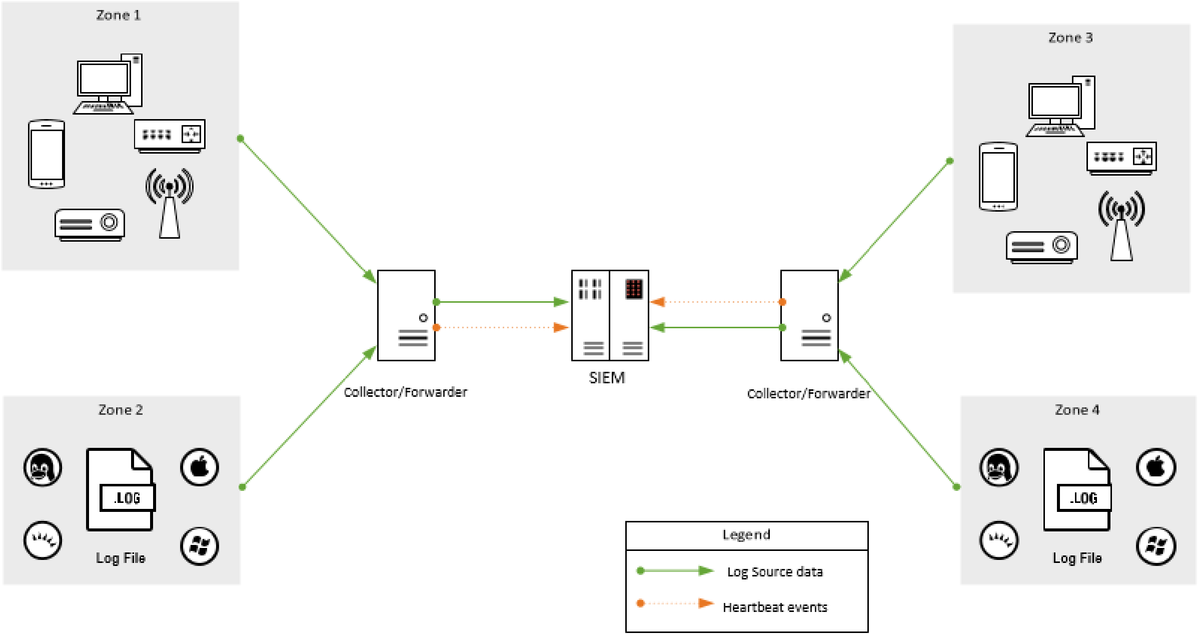
### General approach

- Level of detail till log collector(s)

### Limitations

- Visibility only to Aggregator/Collector level

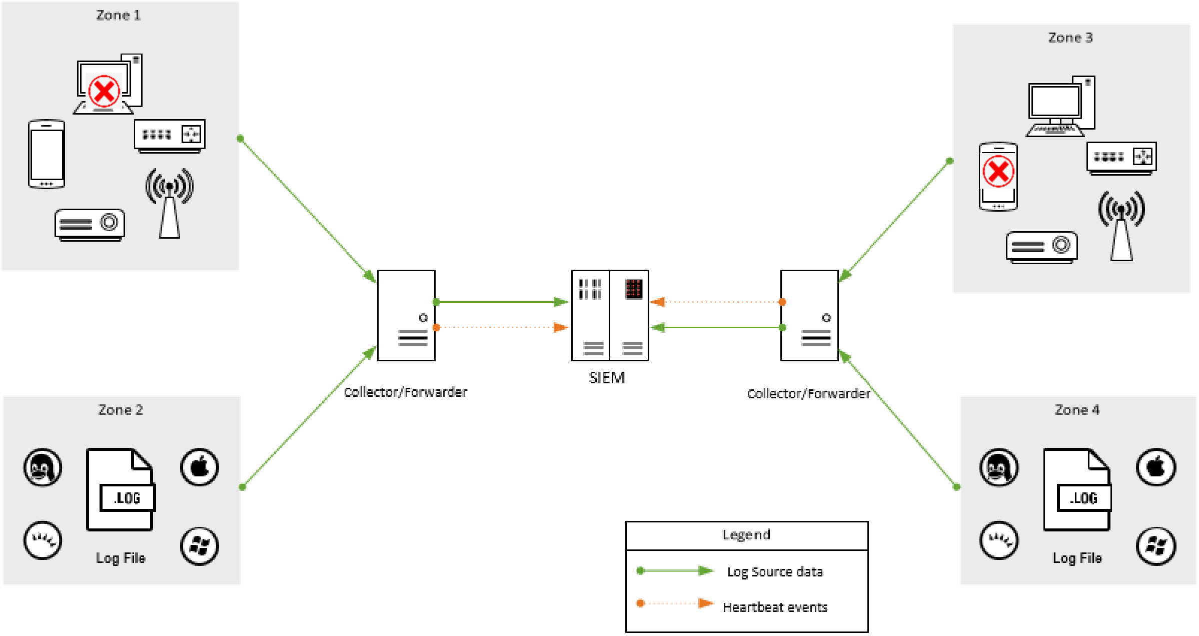
# Health Monitoring
## Scenario



Get The Basics Right!

# Health Monitoring

## Scenario



# Health Monitoring
## Solution

### What if we proceed to the host/log source level?

- ❖ Different sources have different logging frequencies
- ❖ Use cases at source level impacts SIEM productivity

### Solution

- ❖ Configure alerts for P1 sources
- ❖ Schedule Daily/Weekly reports for P2/P3 sources

### Benefits

- ❖ Reduced downtime
- ❖ No Alert fatigue

# Scenario #3

Identifying blind spots

# Identifying blind spots

## Example

| List of use cases |
|---|
| Sources Sending Many DNS Requests |
| High Volume Email Activity to Non-corporate Domains by User |
| Multiple Authentication Failures |
| Suspicious Domain/IP Communication |
| Unusual Geolocation of Communication Destination |
| Emails with Look alike Domains |
| Web Uploads to Non-corporate Sites by Users |
| Unusual Volume of Network Activity |
| Detect Use of cmd.exe/ps.exe to Launch Script Interpreters |
| Detect USB Usage/insertion |
| Hosts Sending To More Destinations Than Normal |

# Identifying blind spots

## Enrich

| Use case | Threat Category | Kill Chain Phase |
|---|---|---|
| Sources Sending Many DNS Requests | Insider Threat,<br>Advanced Threat Detection | C2,<br>Action on Objectives |
| High Volume Email Activity to Non-corporate Domains by User | Insider Threat,<br>Advanced Threat Detection | Action on Objectives |
| Multiple Authentication Failures | Insider Threat,<br>Advanced Threat Detection | None |
| Suspicious Domain/IP Communication | Insider Threat,<br>Advanced Threat Detection | None |
| Unusual Geolocation of Communication Destination | Insider Threat,<br>Advanced Threat Detection | None |
| Unusual Volume of Network Activity | Insider Threat,<br>Advanced Threat Detection | None |
| Web Uploads to Non-corporate Sites by Users | Insider Threat | Action on Objectives |
| Emails with Look alike Domains | Advanced Threat Detection | Delivery |
| Detect Use of cmd.exe/ps.exe to Launch Script Interpreters | Advanced Threat Detection | Exploitation |
| Detect USB Usage/insertion | Insider Threat | Installation,<br>Delivery |
| Hosts Sending To More Destinations Than Normal | Advanced Threat Detection | Reconnaissance |

# Identifying blind spots

## Transform

| Kill Chain Phase | APT | Insider Threat |
|---|---|---|
| Reconnaissance | Hosts Sending To More Destinations Than Normal | 🟨 |
| Weaponization | 🟨 | 🟨 |
| Delivery | Emails with Look alike Domains | Detect USB Usage/insertion |
| Exploitation | Detect Use of cmd.exe/ps.exe to Launch Script Interpreters | 🟨 |
| Installation | 🟨 | Detect USB Usage/insertion |
| Command & Control | Sources Sending Many DNS Requests | Sources Sending Many DNS Requests |
| Actions on Objectives | Sources Sending Many DNS Requests,<br>High Volume Email Activity to Non-corporate Domains by User | Sources Sending Many DNS Requests,<br>High Volume Email Activity to Non-corporate Domains by User,<br>Web Uploads to Non-corporate Sites by Users |
| None | Multiple Authentication Failures,<br>Suspicious Domain/IP Communication,<br>Unusual Geolocation of Communication Destination,<br>Unusual Volume of Network Activity | Multiple Authentication Failures,<br>Suspicious Domain/IP Communication,<br>Unusual Geolocation of Communication Destination,<br>Unusual Volume of Network Activity |

# Identifying blind spots

## Model | List – Enrich – Transform

| | APT | Insider Threat | Data protection | others |
|---|---|---|---|---|
| Reconnaissance | | | | |
| Weaponization | | | | |
| Delivery | | | | |
| Exploitation | | | | |
| Installation | | | | |
| Command & Control | | | | |
| Actions on Objectives | | | | |

# Thank You!

Balaji Nakkella - linkedin.com/in/balajinakkella/

Rakesh Kumar Narsingoju - linkedin.com/in/rakesh-narsingoju