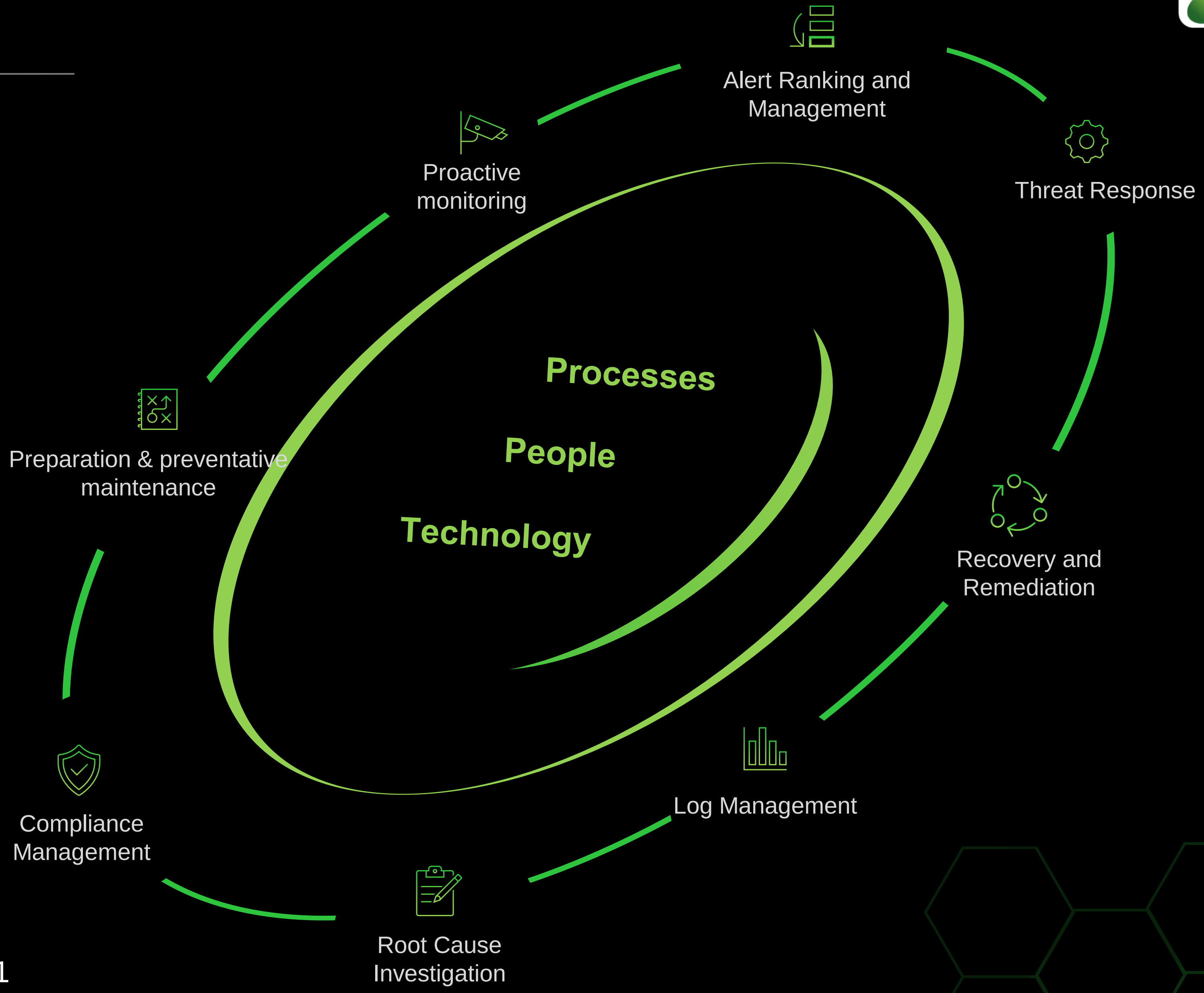
Security Operations Center

> *There are only two types of enterprises—those that know they've been compromised, and those that don't know.*

@Pi 2021

SECURITY OPS

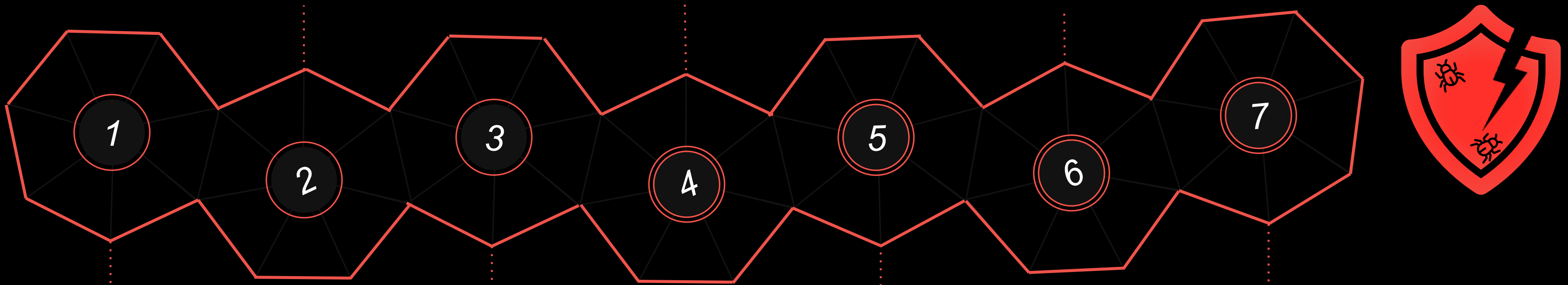
Pi SOC is a centralized function involving people, processes, and technology to continuously monitor and improve enterprise security posture while preventing, detecting, analysing, and responding to cybersecurity incidents.



@Pi 2021

Cyber kill chain

Sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it



Reconnaissance

Harvesting email addresses, conference information etc

Weaponization

Coupling exploit with backdoor into deliverable payload

Delivery

Delivering weaponized bundle to the victim via email, web, USB, etc.

Exploitation

Exploiting a vulnerability to execute code on victim's system

Installation

Installing malware on the asset

Command & Control

Command channel for remote manipulation of victim

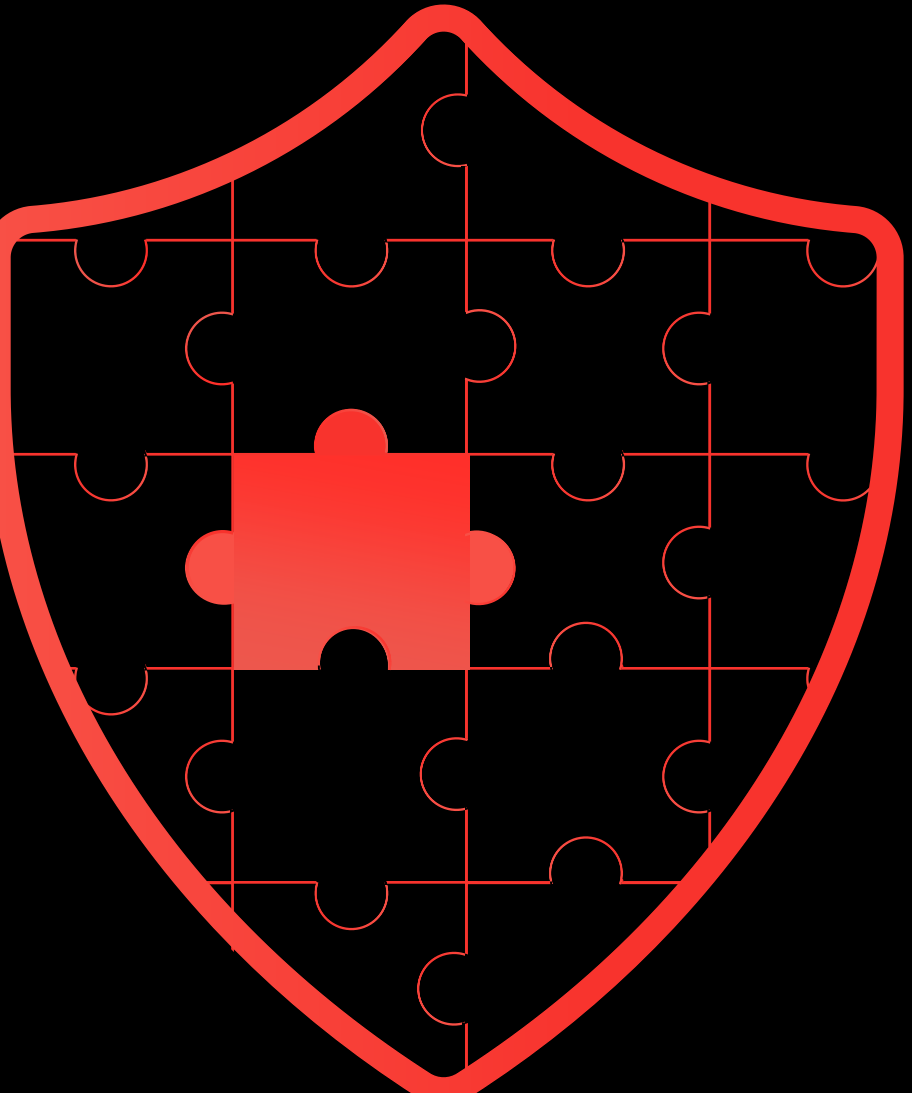
Action on objectives

With "Hands on Keyboard" access , intruders accomplish their original goals

@Pi 2021

Developed by LOCKHEED MARTIN

Internal threats are underrated



Common threats

Social Engineering

You can have the best technical systems in place, but they're not effective if people aren't educated about the risks.

Downloading malicious internet content

It's very easy for a rootkit to be hidden in a game or a video clip, and a novice user may not notice anything out of the ordinary.

Information leakage

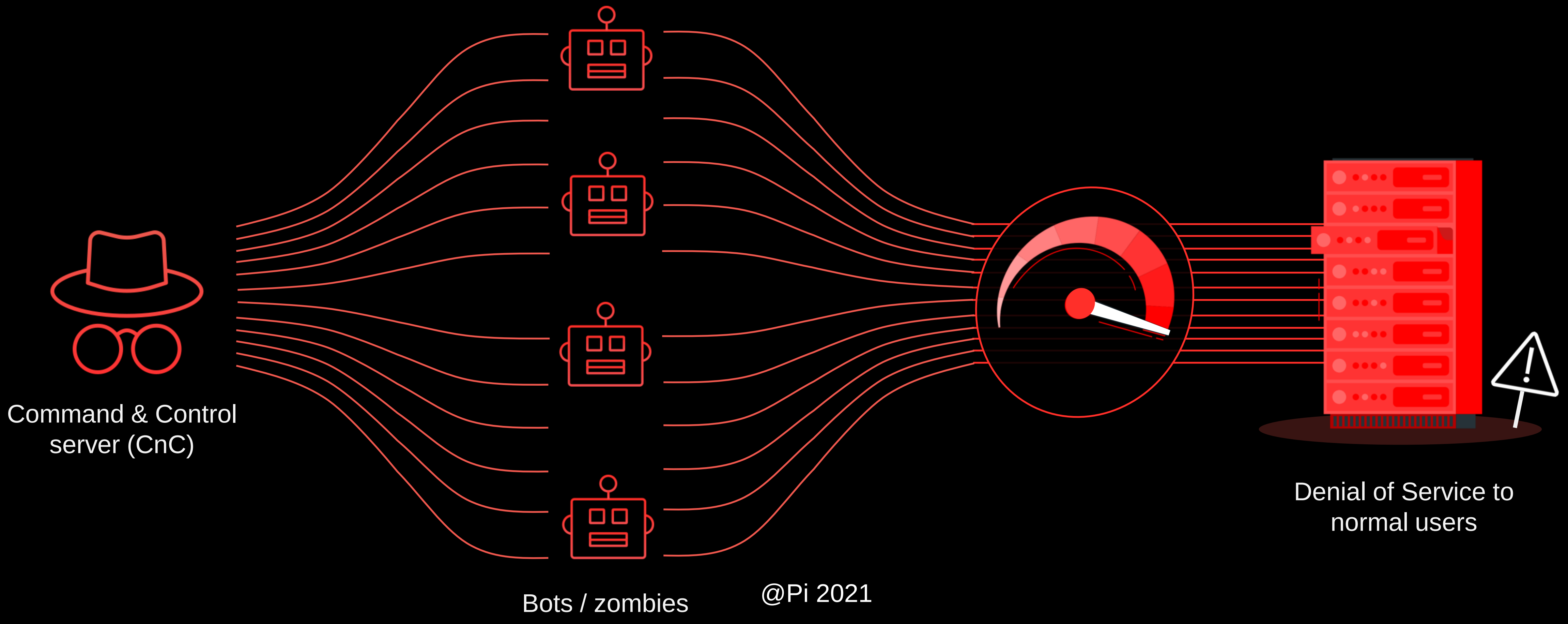
Whether it's a digital camera or USB data stick, today's employees could easily take a significant chunk of your customer database out of the door in their back pocket.

@Pi 2021

Distributed Denial of Service (DDoS)

DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices (referred as botnet)


Command & Control server (CnC)
Bots / zombies
Denial of Service to normal users

@Pi 2021

Advanced

Targeted, coordinated, purposeful

Persistent

Month after month, year after year

Threat

Person(s) with intent, opportunity, and capability

APT goals

- **Espionage** (SolarWinds hack)
  It may include the acquisition of intellectual property, or it could include sequestration of proprietary or operational information.

Or / And

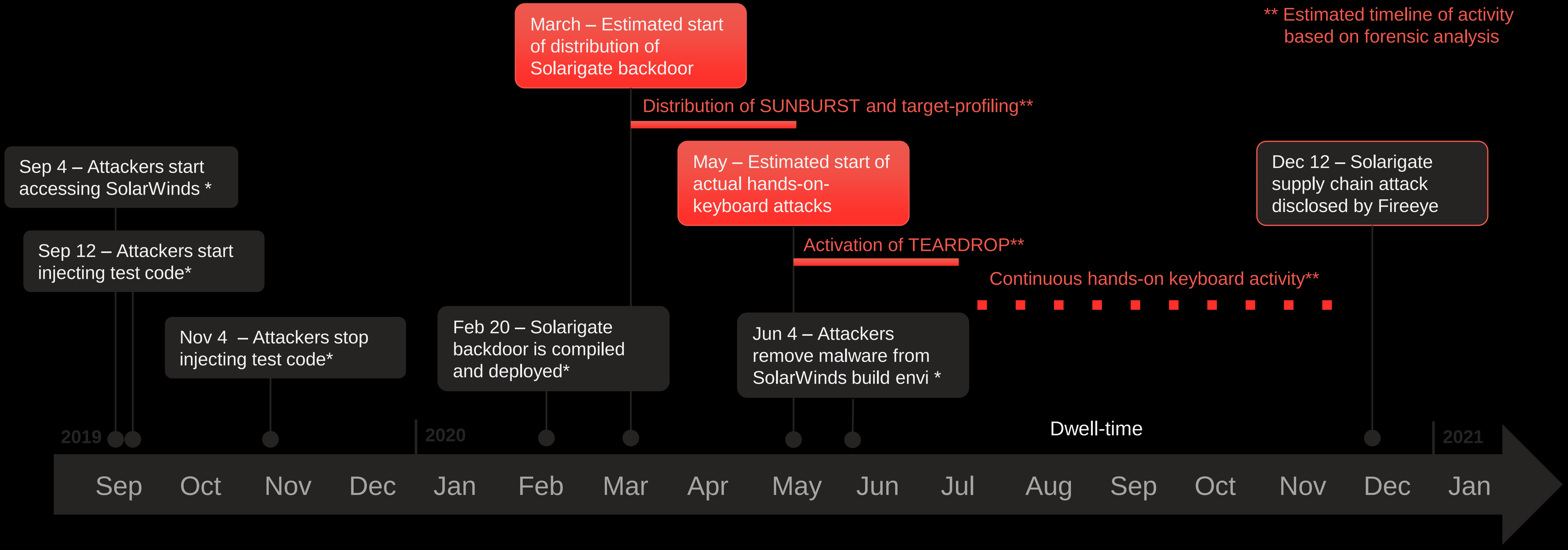
- **Sabotage** (Stuxnet)
  Deliberate action aimed at weakening an enemy through subversion, obstruction, disruption, and/or destruction.

Supply-chain attack: SolarWinds

Malware was deployed on networks as part of SolarWinds products, that allowed attackers to gain backdoor access to affected devices.

* Info disclosed by SolarWinds

** Estimated timeline of activity based on forensic analysis



Sep 4 – Attackers start accessing SolarWinds *

Sep 12 – Attackers start injecting test code*

Nov 4 – Attackers stop injecting test code*

Feb 20 – Solarigate backdoor is compiled and deployed*

March – Estimated start of distribution of Solarigate backdoor

Distribution of SUNBURST and target-profiling**

May – Estimated start of actual hands-on-keyboard attacks

Activation of TEARDROP**

Jun 4 – Attackers remove malware from SolarWinds build envi *

Continuous hands-on keyboard activity**

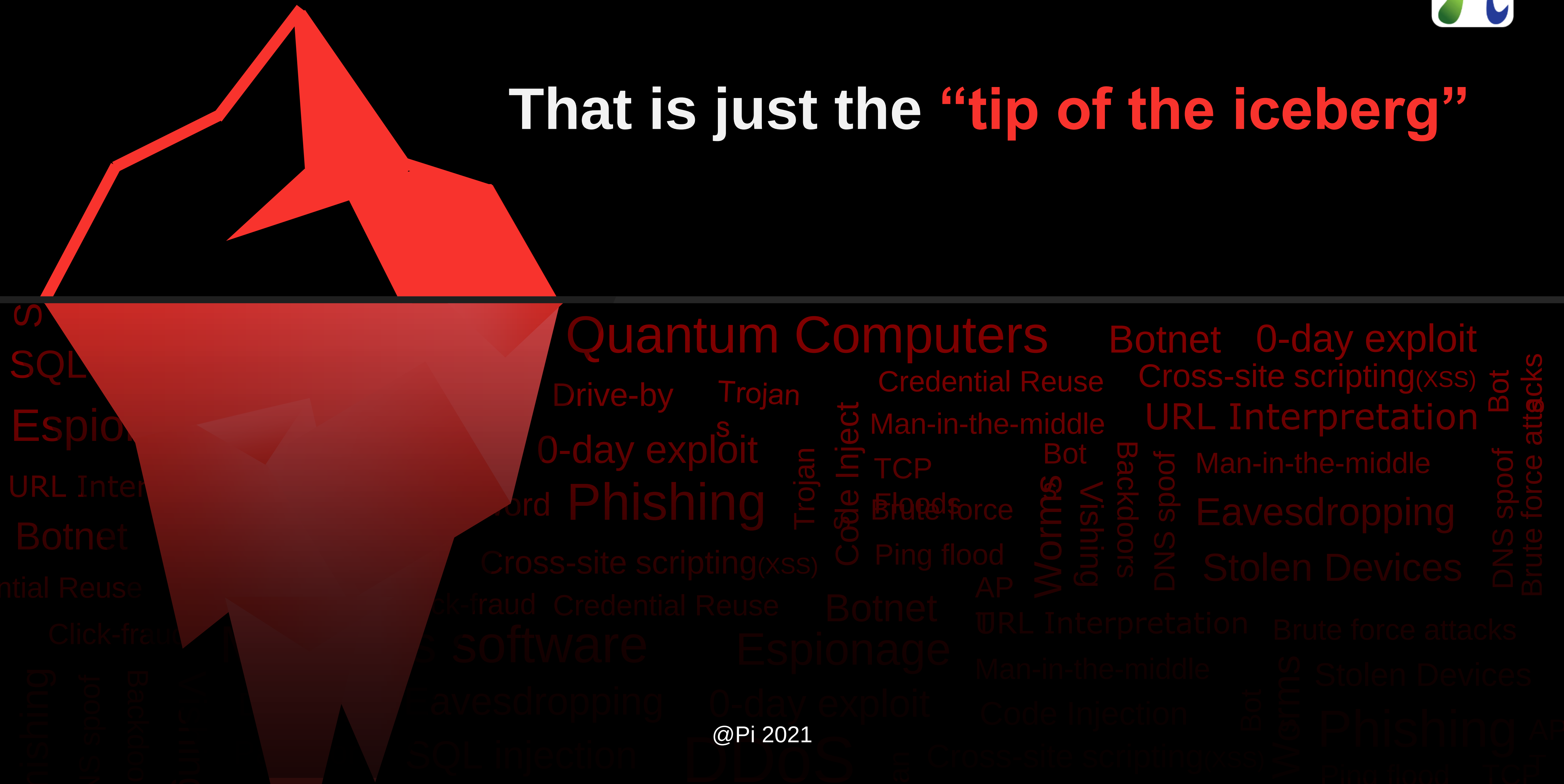
Dec 12 – Solarigate supply chain attack disclosed by Fireeye

Dwell-time

@Pi 2021

Analysis by Microsoft

That is just the “tip of the iceberg”



@Pi 2021

“The best defence is a good offense”

Defence in Depth

- Firewalls, IPS/IDS
- Anti-malware
- Role-based access controls
- Multi-factor authentication
- EPP/EDR
- Web Application Firewall
- Encryption at-rest & in -transit

Most OF INCIDENTS CAN BE PREVENTED WITH **BEST PRACTICES**

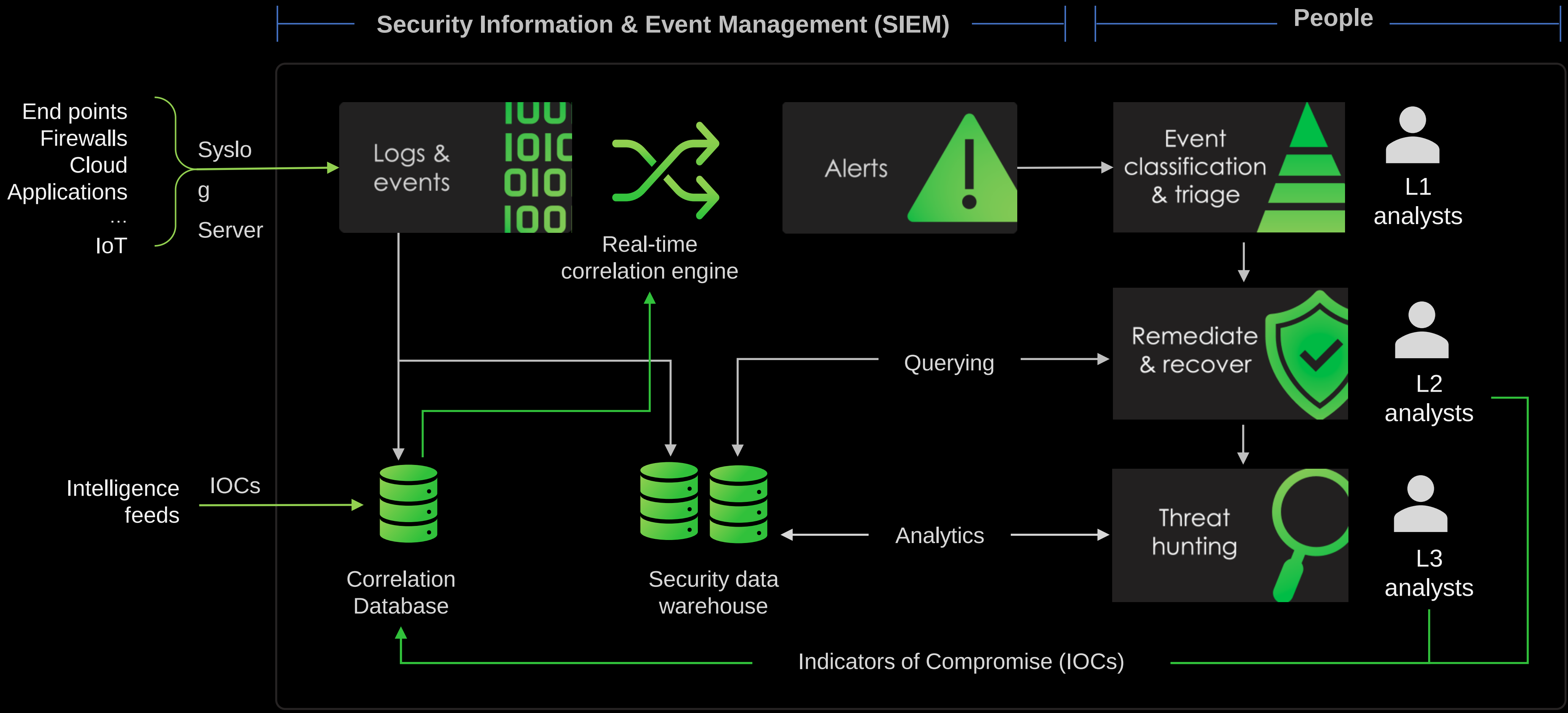
Continuous security operations

- Gaining visibility into network
- Threat intelligence
- Role-based access controls
- Automating repetitive tasks
- Reducing surface area for attacks
- Vulnerability Assessment & Penetration Testing

Awareness

- Security Awareness program
- Reporting incidents

A day in the life of Pi SOC

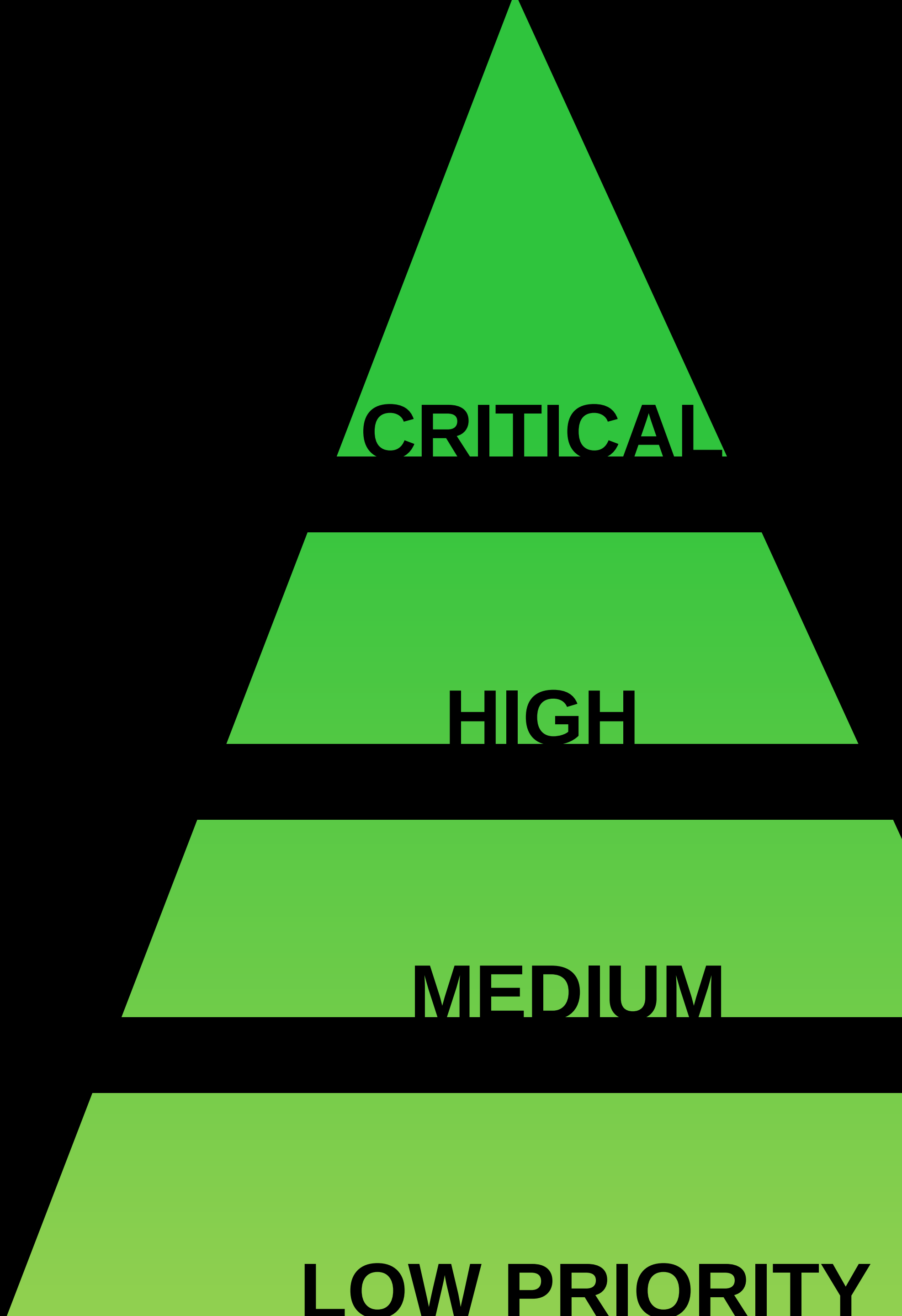


Event classification & triage

The true value of collecting, correlating, and analysing logs is that it, gives you the ability to find the “signal in the noise.”

L1 analysts who are monitoring SOC 24/7 are the first responders to perform the initial triage.

- Reviews the latest alerts
- Creates new trouble tickets for alerts
- Reduce the number of false positives
- Runs vulnerability scans(VA) and extract reports
- Manages and configures security monitoring tools.
- Notifications management


CRITICAL

HIGH

MEDIUM

LOW PRIORITY

Remediation & Recovery

Each attack will differ in terms of the appropriate remediation steps to take on the affected systems, but it will often involve one or more of the following steps performed by L2 analysts:

- ✔ Initial analysis
- ✔ Re-image systems
- ✔ Patch or update systems
- ✔ Re-configure system access
- ✔ Re-configure network access
- ✔ Review monitoring capabilities on servers and other assets
- ✔ Validate patching procedures and other security controls by running vulnerability scans
- ✔ Write custom queries across environments and timeframes

Threat Hunting

It’s always optimal to find and fix vulnerabilities before an attacker exploits them in order to gain access to system L3 analysts work proactively to prevent these attacks from happening in the first place.

- Hunt for unknown threats with analytics and ML
- Identify new IOCs to improve monitoring
- Review asset discovery
- Review Vulnerability Assessment data
- Conduct penetration tests
- Compliance management
- Optimizing security monitoring

“Prevention is better than curing”

Additional features of Pi SOC

Automation

Built-in alert remediation workflow

Instant interventional remediation capability to prevent malware propagation across your network.

Security Orchestration & Automated Response(SOAR)

Adaptive response to malicious security events thus increasing the speed, efficiency and quality

Threat detection

In-built IDS

Live intrusion detection is integral to securing internal networks and host

Correlation use cases

Advanced correlation use cases like insider/dormant threat identification, capturing network anomalies etc.

Advanced detection and UBA capabilites

To effectively identifies out of the norm events and incidents by using machine learning

Integrations

Integrated Threat Intelligence(TI)

To observe, orient, decide and quickly act against threats and identified indicators of compromises (IOCs

NOC health monitoring functions

Combine the capabilities of a SIEM and an IT service management intelligence engine

External integrations

Enterprises can integrate with their existing security technologies and minimize siloed security service delivery

Others

Data lake storage and processing engine

Supports any type of data and data collection for logs, flow data, DB, Webhook, API

Supports hybrid model

Pi SOC can work in tandem with existing security SIEMs to increase the security posture of the enterprise

How does enterprises benefit from Pi SOC-as-a-Service ?

Reduces SOC complexity & Instant expertise

Increases speed of deployment

Cost-effective security

Improves threat detection and response

Compliance reporting

Advanced visualisations and dashboards

@Pi 2021

SOC coverage matrix (1/2)

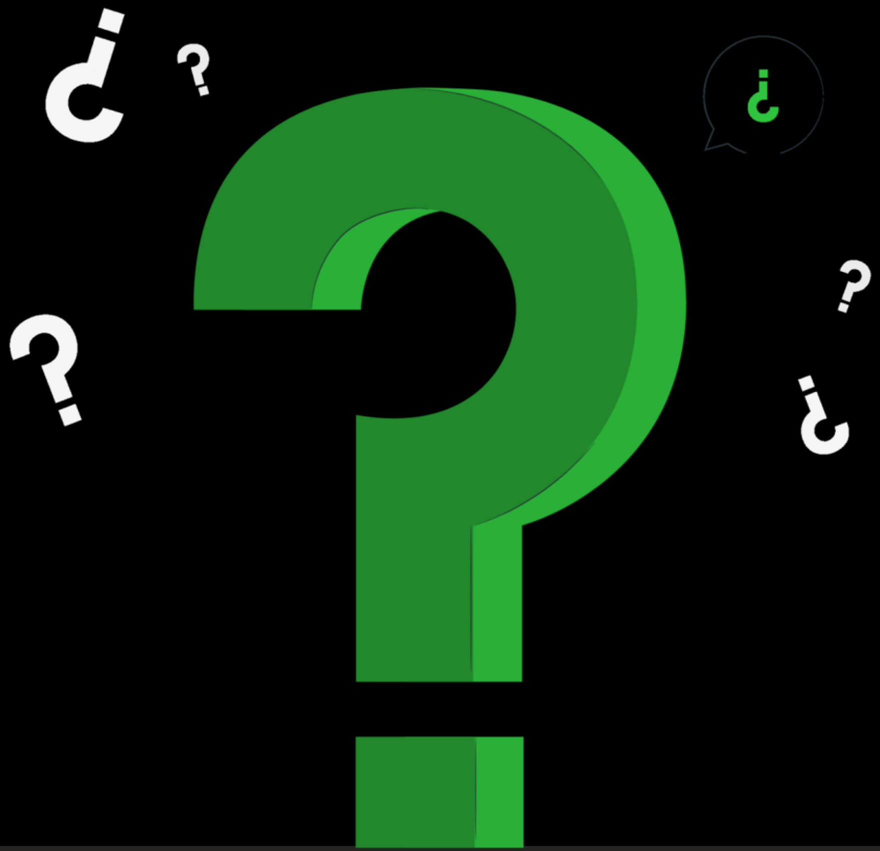
	Silver	Gold	Platinum	Diamond
Device/application integration (standard)	Yes (Max 70 assets)/(Max 500 EPS)	Yes (Max – 300 assets, 75 critical assets & 225 endpoints)/(Max 750 EPS)	Yes, max 300 assets (75 critical assets & 225 endpoints) (Max 1000 EPS)	COMPLETELY CUSTOMIZABLE SERVICE TAILORED TO MEET CLIENT REQUIREMENTS (AVAILABLE ON DEMAND)
Security Information and Event Management	Yes	Yes	Yes	
Log aggregation and correlation	Yes	Yes	Yes	
Critical event alerting & reporting (automated 24/7 alerts from tool)	Yes (Automated alerts from Pi SOC)	Yes, 8*5 (Any after-hours alerting and reporting requiring analyst intervention will be done on the next business day)	Yes, 24*7	
Compliance reporting	No	Yes (Standard Pi SOC Reporting)	Yes (Standard Pi-SOC Reporting or Reporting as per Client Policy/Any one International/National Standard)	
Alerts generated by high-probability suspicious activity	Yes (Automated Alerts from Pi SOC)	Yes	Yes	
Collects security event data 24/7 from the client's standard connectors	Yes	Yes	Yes	
Event triaging & triage reporting	Yes (Max 10 per month on request basis) (Additional triages/reports will charged in packs of 10)	Yes, 8*5 (Non-business days' works if needed will be charged extra at triaging and eye-on-the-glass-support services rates)	Yes	
Cyber analyst will analyse and interpret alerts	Yes (Remediation and Incident Response will be handled by the enterprise IT team. Hands on technical assistance for IR and Remediation by Pi SOC, if needed by the client, will be charged extra at advanced services rates)	Yes (Remediation and Incident Response will be handled by the enterprise IT team. Hands on technical assistance for IR and Remediation by Pi SOC, if needed by the client, will be charged extra at advanced services rates)	Yes (Remediation and Incident Response will be handled by the enterprise IT team. Hands on technical assistance for IR and Remediation by Pi SOC, if needed by the client, will be charged extra at advanced services rates)	
*Analyst will triage and classify				
*If determined to be anomalous, analyst will notify client for remediation				

Scope of work (2/2)

	Silver	Gold	Platinum	Diamond
Critical asset identification	No	No	Yes	COMPLETELY CUSTOMIZABLE SERVICE TAILORED TO MEET CLIENT REQUIREMENTS (AVAILABLE ON DEMAND)
Threat Intelligence	Yes (Monthly)	Yes (Monthly)	Yes (Continuous)	
Enhanced collection and response connectors	No	Yes	Yes	
Custom log source integration	No	Yes (Max 5 sources)	Yes	
Periodic reports on request	Yes (On a monthly basis) (Max 6 reports)	Yes (Max 2 custom reports + default Pi SOC reports)	Yes (Max 6 custom reports + default Pi SOC reports)	
Security monitoring	Yes (Automated alerts from Pi SOC)	Yes	Yes	
Dashboards	Yes (Standard Pi SOC dashboards)(Max 6)	Yes (Standard Pi SOC dashboards)	Yes (Standard Pi SOC dashboards + 3 custom client dashboards)	
Tailored log analysis and advanced correlation & alerts (endpoint, payload analysis, logs)	No	Yes (for sampled critical assets)	Yes (for all assets/as per design)	
Correlation use cases	Yes, (Pi SOC default use cases) (Max 20)	Yes (Pi SOC default use cases)	Yes (Pi SOC default use cases + 6 custom client defined use cases)	
Basic NOC health monitoring functions	No	No	Yes	
SOAR and other automation	No	Limited, on chargeable basis	Limited	
UBA with endpoint agent	No	Limited	Limited	

Add-on (End-points, VA & PT, Incident response etc) for each plan can be subscribed on demand

Time to DDoS our analysts
with your questions !



Contact us

sales@pidatacenters.com