convergent

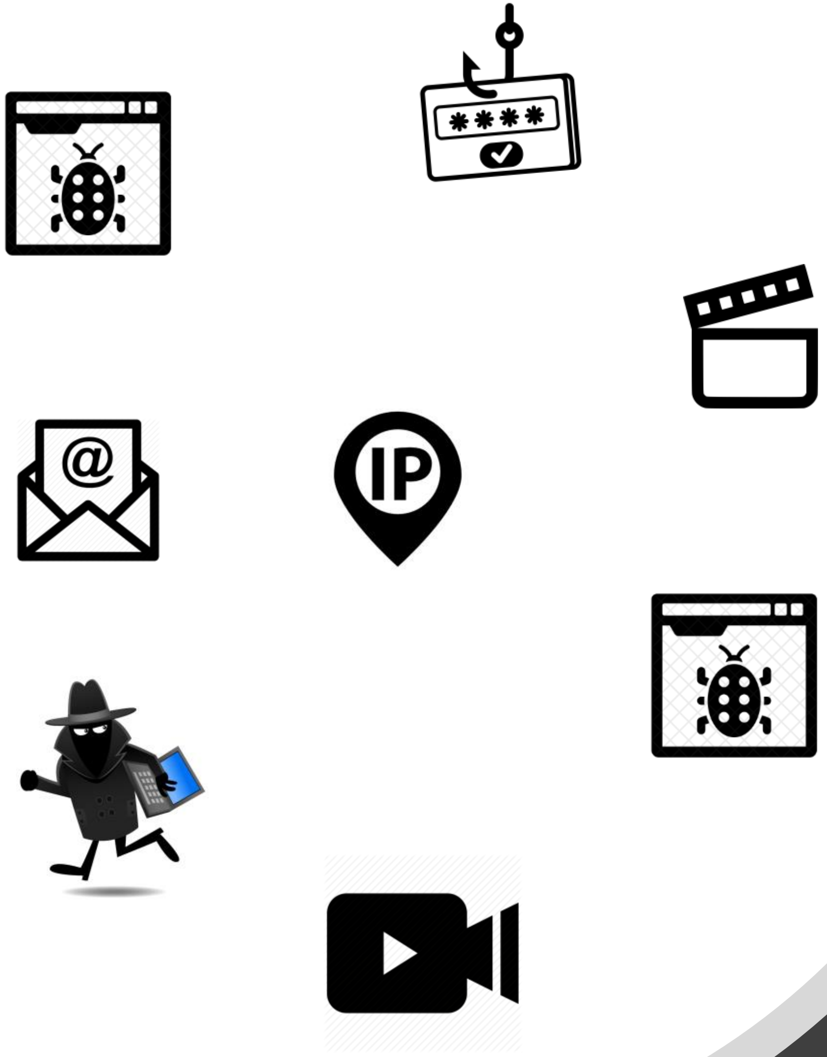
# Reducing the Fog of Cyber Warfare

## Incident Response

Cyber Security Summit NAB 2019

Janice Pearson VP, Global Content Protection &

Mathew Gilliat-Smith, Advisor, Convergent Risks



# Typical Incidents

Email Phishing attack

Attrition attack on IP address/server

Freelancer blog plot revealed

Pre-Theatrical Release prior to embargo

Web - Malware Infections

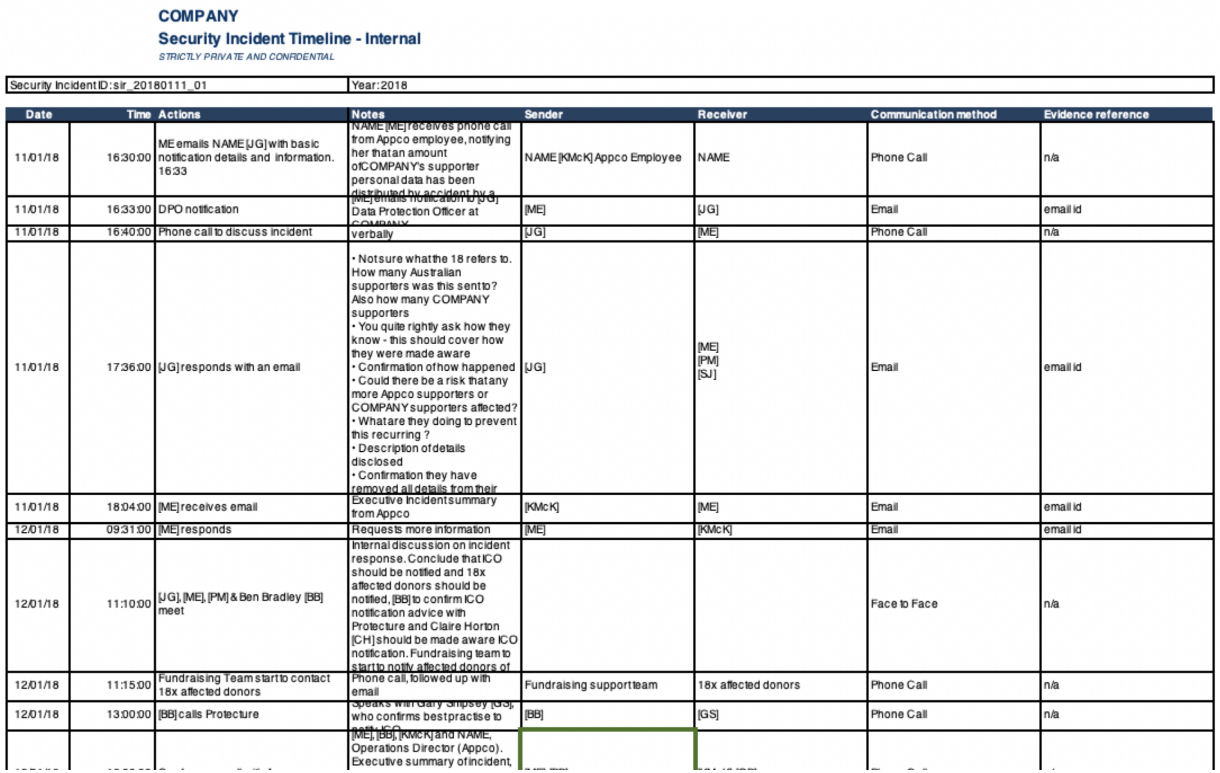
Loss or Theft of equipment e.g. laptop or smartphone trailer Leaks

Improper Usage - violation of acceptable usage policies. Post 'off-boarding'

Other - Client photography in theatre, break-In

# Limitations of Manual Incident Response

- A lot of info - reliance on emails, Excel, Word, screen shots - complex to assemble – different versioning
- Blocked emails through filtering
- Generally reliant on one or two individuals for the information
- IT ticketing systems – issues with internal confidentiality
- Scramble to assimilate, analyze, communicate & act
- Key parts overlooked



**COMPANY**

**Security Incident Timeline - Internal**

*STRICTLY PRIVATE AND CONFIDENTIAL*

| | |
|---|---|
| Security Incident ID:sir_20180111_01 | Year:2018 |

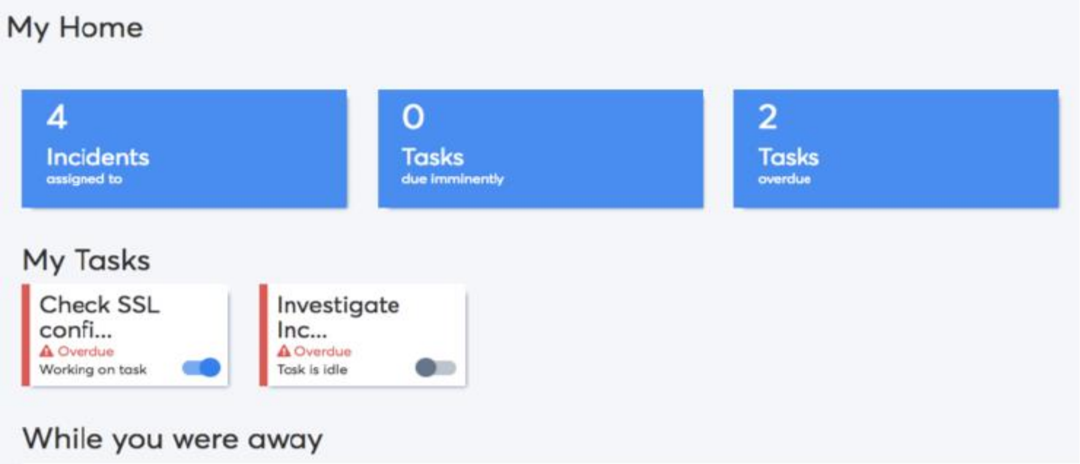
| Date | Time | Actions | Notes | Sender | Receiver | Communication method | Evidence reference |
|---|---|---|---|---|---|---|---|
| 11/01/18 | 16:30:00 | ME emails NAME [JG] with basic notification details and information. 16:33 | NAME [ME] receives phone call from Appco employee, notifying her that an amount ofCOMPANY's supporter personal data has been distributed by accident by a | NAME [KMcK] Appco Employee | NAME | Phone Call | n/a |
| 11/01/18 | 16:33:00 | DPO notification | [ME] emails notification to [JG] Data Protection Officer at COMPANY | [ME] | [JG] | Email | email id |
| 11/01/18 | 16:40:00 | Phone call to discuss incident | verbally | [JG] | [ME] | Phone Call | n/a |
| 11/01/18 | 17:36:00 | [JG] responds with an email | • Not sure what the 18 refers to. How many Australian supporters was this sent to? Also how many COMPANY supporters<br>• You quite rightly ask how they know - this should cover how they were made aware<br>• Confirmation of how happened<br>• Could there be a risk that any more Appco supporters or COMPANY supporters affected?<br>• What are they doing to prevent this recurring ?<br>• Description of details disclosed<br>• Confirmation they have removed all details from their | [JG] | [ME]<br>[PM]<br>[SJ] | Email | email id |
| 11/01/18 | 18:04:00 | [ME] receives email | Executive Incident summary from Appco | [KMcK] | [ME] | Email | email id |
| 12/01/18 | 09:31:00 | [ME] responds | Requests more information | [ME] | [KMcK] | Email | email id |
| 12/01/18 | 11:10:00 | [JG], [ME], [PM] & Ben Bradley [BB] meet | Internal discussion on incident response. Conclude that ICO should be notified and 18x affected donors should be notified, [BB] to confirm ICO notification advice with Protecture and Claire Horton [CH] should be made aware ICO notification. Fundraising team to start to notify affected donors of | | | Face to Face | n/a |
| 12/01/18 | 11:15:00 | Fundraising Team start to contact 18x affected donors | Phone call, followed up with email | Fundraising support team | 18x affected donors | Phone Call | n/a |
| 12/01/18 | 13:00:00 | [BB] calls Protecture | Speaks with Gary Shipsey [GS], who confirms best practise to notify ICO | [BB] | [GS] | Phone Call | n/a |
| | | | [ME], [BB], [KMcK] and NAME, Operations Director (Appco). Executive summary of incident, | | | | |

# Central Incident Response Management Platform

- Centralized ticketing system segregated from the network
- Incident Response - a discipline of Continual Improvement better Analysis to convert volumes of data into actionable intelligence and evidence
- Faster Response and recovery managing security incidents in real time
- Contained Communication - hierarchy of user permission levels - need to know basis. Emails containing IP address not blocked as suspicious
- Encrypted Data, immutably stored for analyst investigation & legal
- No PII issues – Personal Data is not distributed outside of the platform: CCPA GDPR
- Malware evidence stored hashed and encrypted

# Home Dash Board

- Information & Status
- Incident Snap Shot
  - with real time data with tasks, activity
- View Assets
- Add users, permissions
- Communication



My Home

4 Incidents assigned to

0 Tasks due imminently

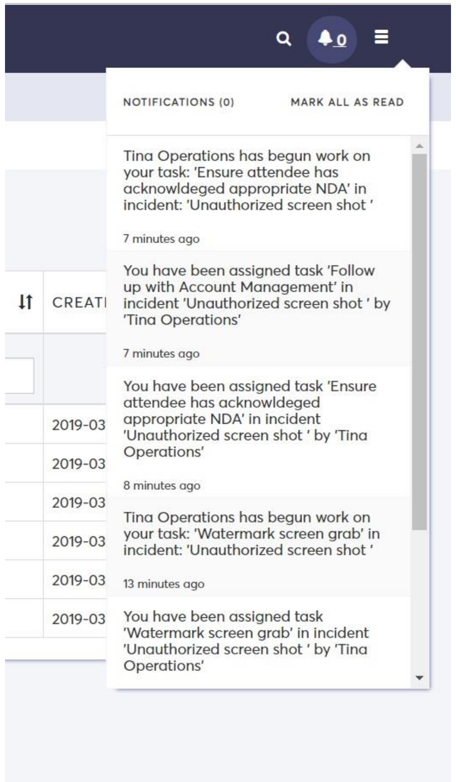
2 Tasks overdue

My Tasks

Check SSL confi... ⚠ Overdue Working on task

Investigate Inc... ⚠ Overdue Task is idle

While you were away



NOTIFICATIONS (0) MARK ALL AS READ

Tina Operations has begun work on your task: 'Ensure attendee has acknowldeged appropriate NDA' in incident: 'Unauthorized screen shot '

7 minutes ago

You have been assigned task 'Follow up with Account Management' in incident 'Unauthorized screen shot ' by 'Tina Operations'

7 minutes ago

You have been assigned task 'Ensure attendee has acknowldeged appropriate NDA' in incident 'Unauthorized screen shot ' by 'Tina Operations'

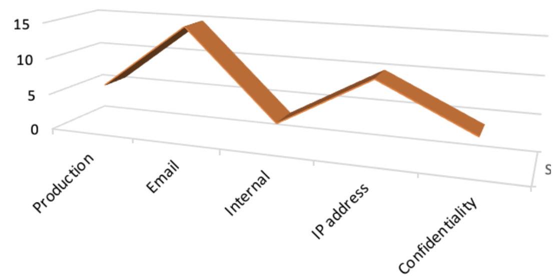
8 minutes ago

Tina Operations has begun work on your task: 'Watermark screen grab' in incident: 'Unauthorized screen shot '

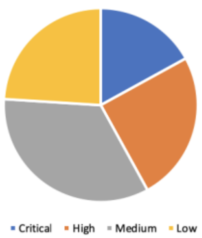
13 minutes ago

You have been assigned task 'Watermark screen grab' in incident 'Unauthorized screen shot ' by 'Tina Operations'

Incidents in last 7 days

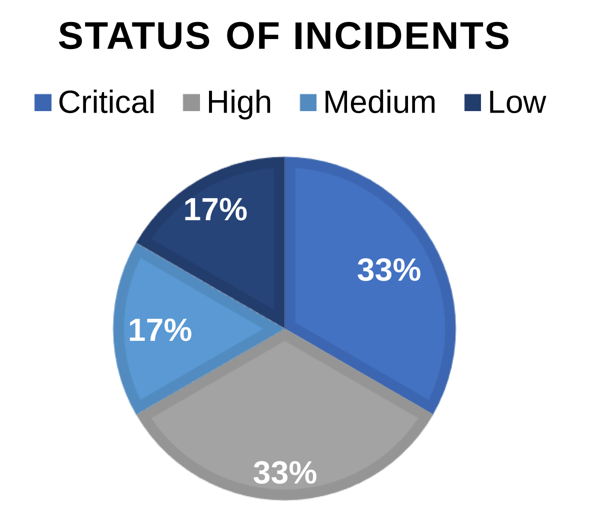


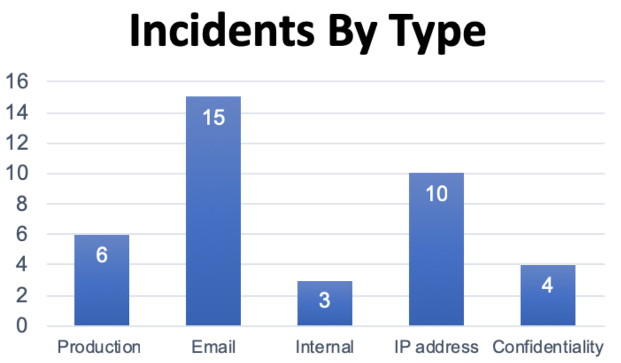
Threat Levels

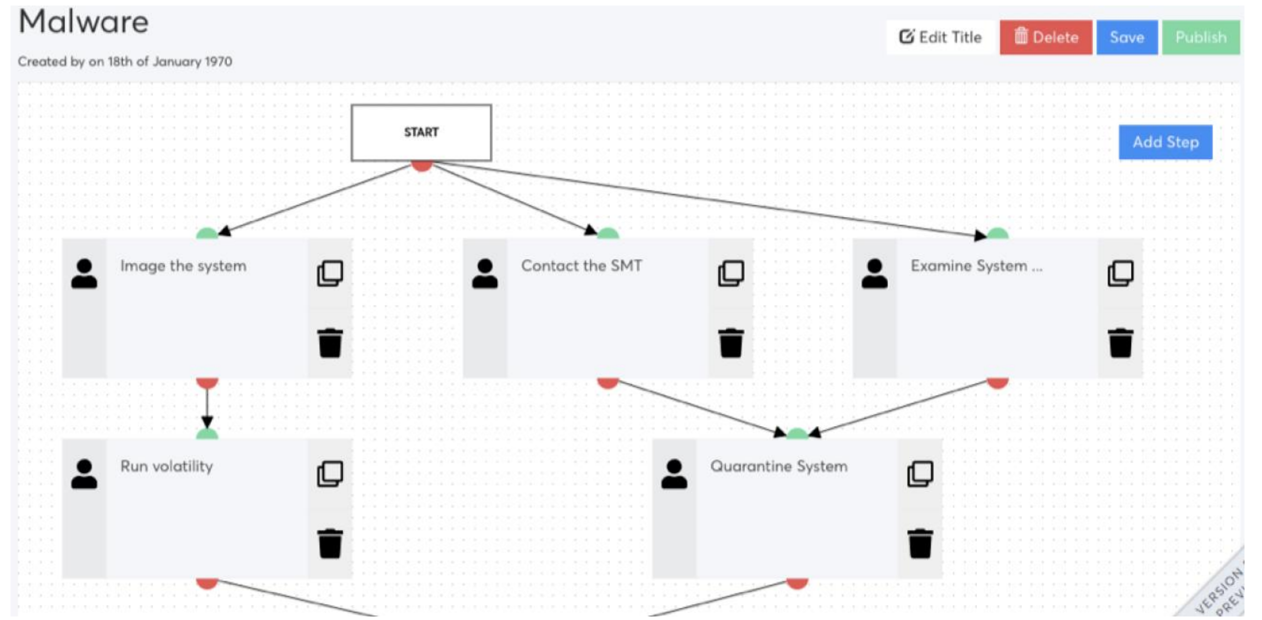


# Analysis of Activity

- Analysis
  - Graphs, charts, timelines
- A Playbook Feature
  - Visual representation for activity and remediation steps
  - Playbook Designer – drag & drop, add steps
  - Save to library & publish
  - Add playbook into an existing incident with Playbook Wizard





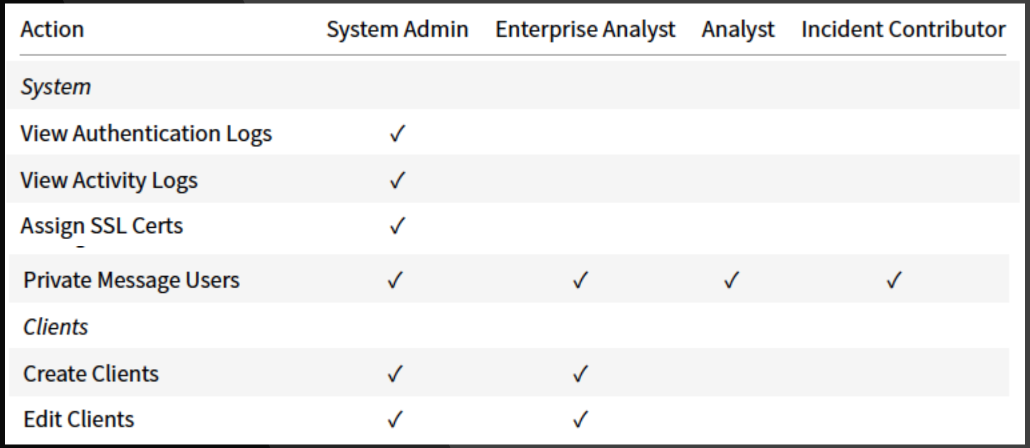


Malware

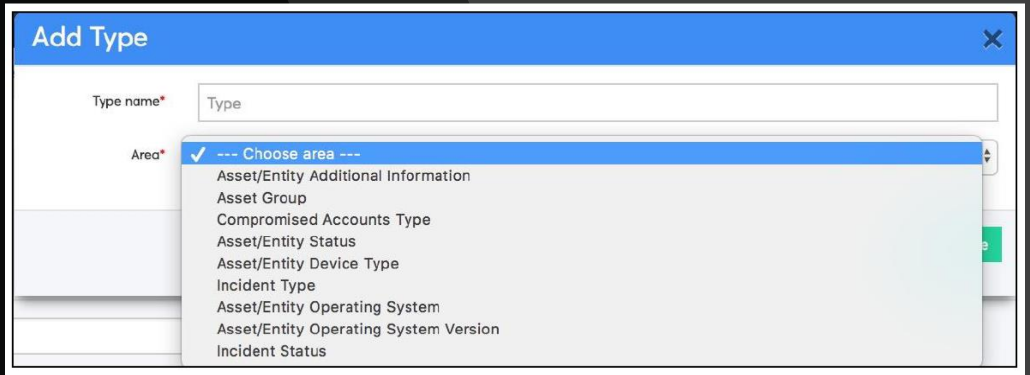
Created by on 18th of January 1970

# Clients, Users, Permissions

- User permissions
  - who is allowed to see what when
- Teams – set & edit permission levels
  - Enterprise Analysts: central control
  - Analysts: e.g. create tasks but not incidents, upload, examine, search evidence
  - Contributors (in the field) e.g. access to a single group, can upload evidence only



| Action | System Admin | Enterprise Analyst | Analyst | Incident Contributor |
|---|---|---|---|---|
| *System* | | | | |
| View Authentication Logs | ✓ | | | |
| View Activity Logs | ✓ | | | |
| Assign SSL Certs | ✓ | | | |
| Private Message Users | ✓ | ✓ | ✓ | ✓ |
| *Clients* | | | | |
| Create Clients | ✓ | ✓ | | |
| Edit Clients | ✓ | ✓ | | |



Add Type

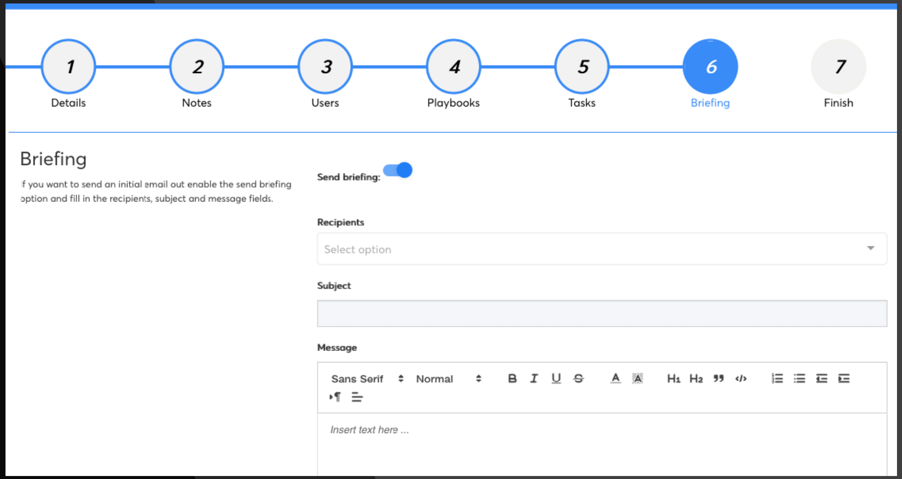
Type name* Type

Area* ✓ --- Choose area ---

Asset/Entity Additional Information
Asset Group
Compromised Accounts Type
Asset/Entity Status
Asset/Entity Device Type
Incident Type
Asset/Entity Operating System
Asset/Entity Operating System Version
Incident Status

# Adding Incidents & Evidence

- Import Incidents
  - Wizard to add, create, edit ensures all steps are competed
  - Event logs
  - Assets: laptops, servers, desktops, server rooms, buildings, IP addresses, malware sites
- Evidence
  - Uploading, downloading, analyzing
  - Encrypted in transit at rest
  - Ghost evidence (with hashing to original path & ASCII Strings)
  - Virus Total for file integrity



Briefing

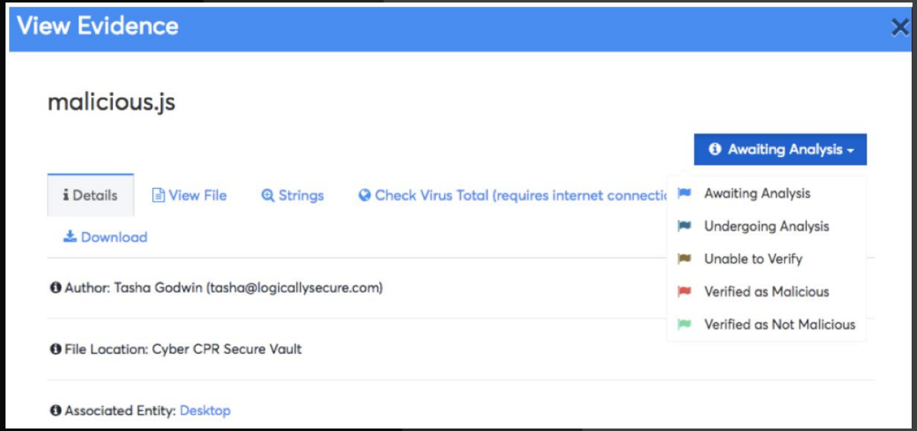
If you want to send an initial email out enable the send briefing option and fill in the recipients, subject and message fields.

Send briefing: ●

Recipients: Select option

Subject:

Message: Insert text here ...



malicious.js

Author: Tasha Godwin (tasha@logicallysecure.com)

File Location: Cyber CPR Secure Vault

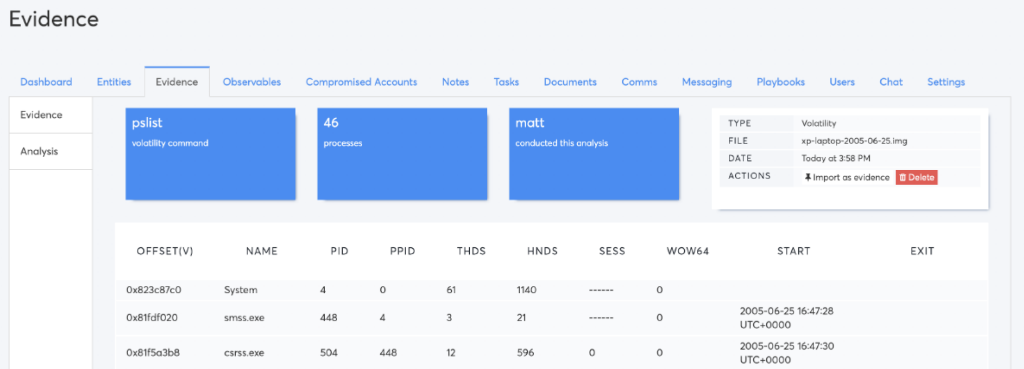
Associated Entity: Desktop

# Searches & Alerts

- Search tool for all incidents and clients
- By ASCII strings
- Alerts Icon – notify managers & users to priority events
- Save so much time with all assets logged in one repository

# Incident Processing

- Running Analysis
  - GREP to search strings
  - Volatility to analyze Windows memory images
- Observables
  - Non physical i.e. IP addresses, hashes to trace attacker activity & identify victim machines
- Indicators - Host & Network based to act on intelligence
- Compromised Accounts - record & monitor
- Convert Documents to Evidence



Evidence

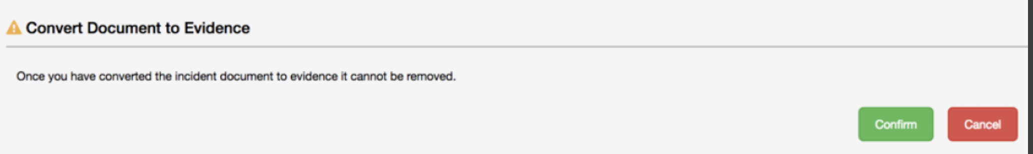
pslist
volatility command

46
processes

matt
conducted this analysis

| | |
|---|---|
| TYPE | Volatility |
| FILE | xp-laptop-2005-06-25.img |
| DATE | Today at 3:58 PM |
| ACTIONS | |

| OFFSET(V) | NAME | PID | PPID | THDS | HNDS | SESS | WOW64 | START | EXIT |
|---|---|---|---|---|---|---|---|---|---|
| 0x823c87c0 | System | 4 | 0 | 61 | 1140 | ------ | 0 | | |
| 0x81fdf020 | smss.exe | 448 | 4 | 3 | 21 | ------ | 0 | 2005-06-25 16:47:28 UTC+0000 | |
| 0x81f5a3b8 | csrss.exe | 504 | 448 | 12 | 596 | 0 | 0 | 2005-06-25 16:47:30 UTC+0000 | |

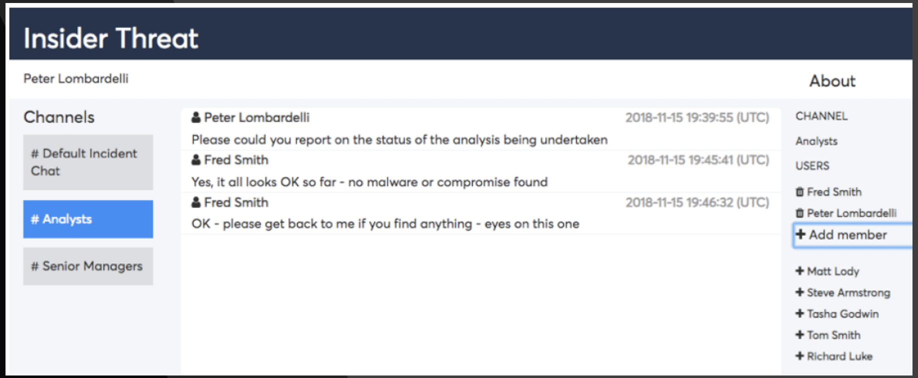


⚠ Convert Document to Evidence

Once you have converted the incident document to evidence it cannot be removed.

# Communication, Messaging & Chat

- Chat between assigned users to same incident is immutable
- Email Templates & configuration for messaging with specific layouts e.g. adding legal disclaimers
- Wizard for customized event briefings
- Accuracy & Proofing checks
- Briefing notices
- Communication logs
- Ideal for legal evidence



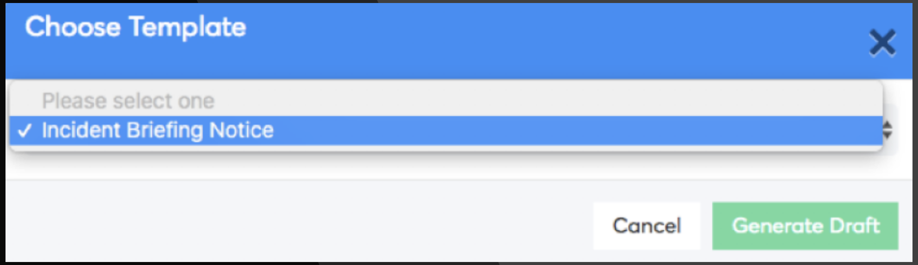
Insider Threat

Peter Lombardelli

Peter Lombardelli 2018-11-15 19:39:55 (UTC)
Please could you report on the status of the analysis being undertaken

Fred Smith 2018-11-15 19:45:41 (UTC)
Yes, it all looks OK so far - no malware or compromise found

Fred Smith 2018-11-15 19:46:32 (UTC)
OK - please get back to me if you find anything - eyes on this one



Choose Template

# Summary

- Company is better equipped to handle an incident emergency
- More information to analyze and more intelligence to act on
- Less reliant on a few individuals
- Faster response times
- Cost savings through prevented incidents

# Case Study

- Featured in the current SANS training course 504
- Used by corporate, government, military and law enforcement in the US, UK, EU, and Australasia including DOD
- Adopted by Convergent as a partnership offering

CPR

convergent

- Risk assessment & compliance services
- Principal provider of TPN assessments
- Penetration & vulnerability testing
- Pre-assessments & remediation advice
- Policy development, security training, breach investigations,
- CCPA & GDPR compliance testing

info@convergentrisks.com

# Q&A