EMC²
where information lives

Critical Incident Response Center – Reportable Metrics

The frequencies are based on actual reporting, but data is available and continuously reportable in Archer.

Continuously

1. Overall incident statuses
2. Threats by classification (VERIS model)
3. Top IoC
4. % Of valid threats (not false positive, this is the measure of whether the host was actually compromised by the threat)
5. Alert distribution by packet decoder

Quarterly

1. Total incidents triaged
2. Total actions taken (clean/reimage/drive captured)
3. Cost of remediation
4. Incident triage (how many incidents vs. actually assigned)
5. Incidents by host compliance
6. Number of malware samples analyzed
7. Number of drives forensically analyzed
8. Spam/phishing investigations
9. Incident closure rate (% closed in 'x' time)
10. Intelligence collection
    - Top sources
    - Top hits per source
    - IoC by Actor
    - IoC by category (kill chain stage)
11. Content Development
    - Rule creation broken out by technology (Packets/Logs)
    - Enhancements (requests for workflow/templates/apps)
    - Break fixes (workflow/apps/alerts)
12. Advanced analytics queries/functions added to production

Monthly

1. Heat map of incidents open/closed per hour

Weekly

1. Average time to closure by priority
2. Top 10 countries