



Digital Forensics Readiness

*PREPARE BEFORE AN INCIDENT
HAPPENS*

Digital Forensics Readiness



The idea that all networks can be compromised has been replaced by the reality that all networks likely will be compromised. Organizations now follow an ongoing course of deterrence, detection, response, and recovery. It is critical that your environment be configured to support effective response to and investigation of incidents as they occur.

If your network environment is not properly configured to track network activity, determination of what happened during an incident may be impossible. Forensic readiness is the ability of your organization to maximize use of digital evidence whilst minimizing the costs of an investigation.

Our Forensics Readiness Assessments will evaluate all aspects of your incident handling potential, including:

- Incident response process
- IT record keeping
- Logging facilities
- Mobile device readiness
- Detection capability
- Cloud forensics readiness

Incident Response Process



Here Forward Defense reviews the process and structure of your Incident Response program. When incidents are detected, swift and appropriate steps must be made to contain and remediate the incident. This is not the time to panic; however, without planned and practiced response processes in place the response time and effectiveness of the IT Forensic activity will suffer greatly.

We work with our Clients to put together appropriate response policies and procedures to address:

- Legal authorities
- Team organization
- Incident triggers
- Communication Protocols
- Business Continuity & Data Recovery (BCDR) plan
- System access
- Provider SLAs integration



IT record keeping review



When a network security incident occurs, it is important to have your house in order. When a network state is chaotic and undocumented, looking for anomalies and malicious deviations from normal states becomes increasingly challenging. To facilitate an effective IT forensic response, your IT, core telco or mobile network's known-good state should be clearly documented and managed. We can help identify and correct gaps in your IT management systems as they impact incident response requirements, including:

- Network diagrams
- Build/Deployment guides
- Equipment Inventories
- Baseline images
- Production system specifications
- Data categorization and location
- Change management

IT Logging facility auditing



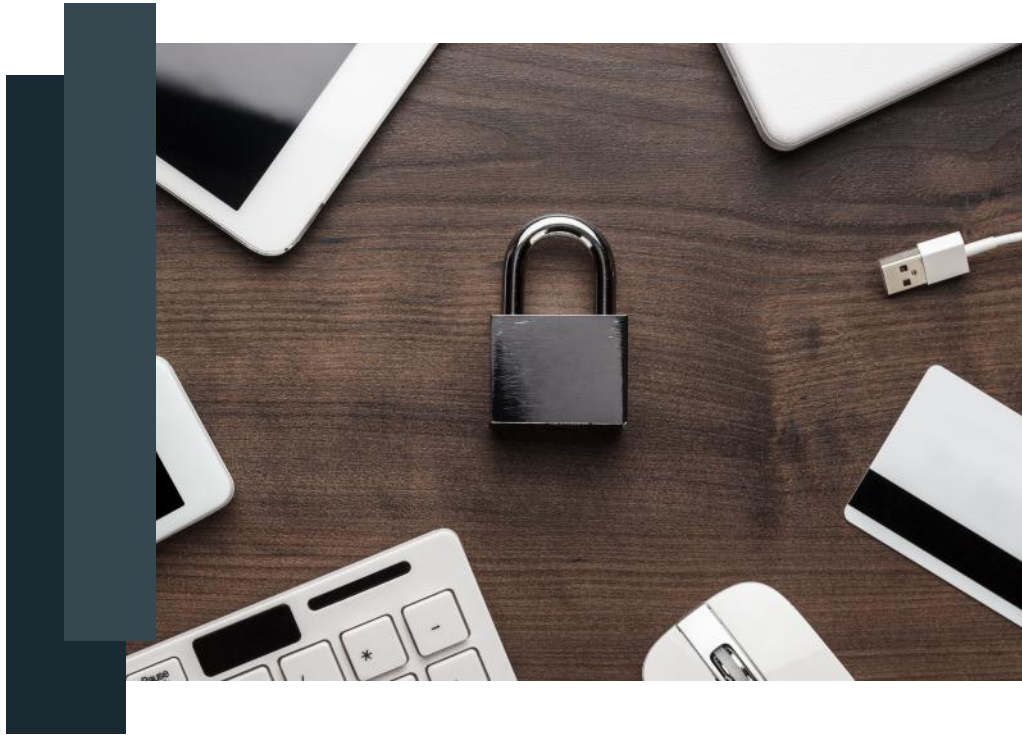
System logs can be powerful indicators of malicious network events, but only when they are effectively enabled, tuned and stored. Having a Security Information and Event Management (SIEM) is a great first step. However, incident response relies on the fact that a network's devices are correctly configured to record relevant events, that those events are effectively aggregated, and that those events can be efficiently collated and queried. It is critically important that these aspects are set up correctly and running to specification to be able to leverage this important IT security asset.

Forward Defense's team will audit your use of log data including:

- Firewall
- User logon
- Remote access
- Printer usage
- Object access for critical assets
- Application user input variables
- Full packet capture
- Database access
- Log retention and backup
- DLP systems (USB drive use)
- Host (end point) event detection
- IDS / IPS / Anti-APT / Anti-Malware



Mobile Device Readiness



Mobile devices are increasingly entering the workplace, and bringing with them a host of new vulnerabilities and attack vectors. Our team can help develop appropriate strategies for allowing these devices to increase employee productivity while controlling the risk they represent. Forward Defense's will examine your organization's incorporation of mobile devices for potential incident response challenges. Items examined include:


- Mobile Device Management (MDM)/ Enterprise Mobility Management (EMM)
- Network isolation and threat hunting capability
- Update management and enforcement controls
- Bring Your Own Device (BYOD)/Corporate-owned, personally enabled (COPE) procedures and authorities
- Forensic access to mobile devices

Detection capability review



The best way to remediate an incident is early detection and response, but most attackers go for months before their presence is detected. Our team can provide a review of your active IT forensic readiness in relation to your defense systems, detection systems, and associated configurations. We can identify gaps in technology, process, and employee capability and put together a comprehensive detection plan to address any issues identified.


We can also conduct simulated attack drills to provide your team with ongoing IT forensic readiness training based on real-world scenarios in their production environment to help them achieve proficiency in detecting incidents.





Cloud forensics readiness

As more services are shifted to third-party cloud providers, organizations must consider the cloud an integral part of their incident and forensics readiness plans. We will help you evaluate the capabilities of your organization and your cloud service provider to address many critical elements of incident response including:

- Contract IR and forensics services
 - Response times
 - Data transfer mechanism
 - Remote forensics deployment
 - Detection and alerting
 - Affidavits or expert testimony arrangements
 - Log aggregation/availability
- 
- A solid black rectangular redaction box covering a portion of the page.