



**Forensics Readiness** : Maximize use of digital evidence whilst minimizing the costs of an investigation

## Forensics Readiness

Organizations need to follow a course of deterrence, detection, response, and recovery. It is critical that you are able 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.



The Forward Defense Forensics Readiness Assessments 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

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





**Forensics Readiness** : Maximize use of digital evidence whilst minimizing the costs of an investigation



### **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. But it is critically important that far more aspects of your systems are set up correctly and running to specification to be able to leverage this important IT security asset.

### **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

### **Detection capability review**

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.

### **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.

## **Contact Us**

Each of our solutions is as unique as our customers. Please contact us to discuss the best way to meet all of your digital forensics requirements

[www.forwarddefense.com](http://www.forwarddefense.com)  
[info@forwarddefense.com](mailto:info@forwarddefense.com)

Forward Defense Equipment and Services  
51st Floor, Addax Tower City of Lights  
Al Reem Island PO Box 47019 Abu Dhabi, UAE  
+971 2 627 8921