# Mickey Lasky

(GCFA GWAPT GCFE GREM GNFA RHCE CEH)

Principal Security Analyst, INFOSEC Engineer, Forensics Analyst, Incident Response

**703-942-9156**
mickey@ita.org
http://www.ita.org
linkedin.com/in/mickeylasky

## EXPERIENCE

### Sr. Manager, Service Management, Global Security Incident Response Team (GSIRT)

*Sony Corporation of America*, Remote

OCT 2015 - PRESENT

• Lead a team of 4 analysts in security relevant data source onboarding, tuning, and management activities for Sony's APAC and European regions.
• Developed advanced use case/alerts/correlation cases in McAfee Nitro & Splunk Enterprise for SOC Analysts & Corporate Clients.
• Performed deep-dive data analysis of new & existing corporate data sources to support SOC with up-to-date security data & identifying potential incidents.
• Maintained expert level awareness of APAC & European security environments
• Supported auditing/reporting requests of Sony's operating companies & assisted them in establishing GSIRT security environments.

### Tier 3 Incident Response Analyst, GSIRT Team

*Sony Corporation of America*, Herndon, VA

APR 2013 - OCT 2015

• Acted as Tier 3 escalation in a 24x7 SOC environment covering Sony's worldwide presence & involving over 170 separate operating companies and organizations.
• Analyzed data from over 4000 sources in a globally deployed McAfee Nitro SIEM solution to support incident response activities.
• Created custom content such as signatures, parsers, views, & channels for deployed security solutions such as McAfee Nitro, Sourcefire, HP TippingPoint, & FireEye utilizing open source intelligence (OSINT), proprietary intelligence sources, & analyst input.
• Mentored Tier 1 & Tier 2 analysts with training opportunities
• Validated & reviewed incident ticketing activities for other analysts in JIRA & performed forensics & malware analysis on enterprise source samples to support incident response activities.
• Worked with operating companies to transition them from outsourced security services to in-house services.

***Key Accomplishments***

• Helped establish SOC services for global Sony & transitioned 20 different operating companies from 3rd-party to in-house services.
• Responsible for management/development of entire Global Security Incident Response Team JIRA instance & produced custom content/maintenance globally
• Developed 5-day McAfee Nitro intro course for Sony's European operating companies.
• Developed content for McAfee Nitro that reduced unknown events from 150M+

## SKILLS

***Operating Systems***
Linux/Unix
Solaris
OSX
Microsoft Windows (All Versions)

***SOC Operations***
McAfee Nitro
Splunk Enterprise
SIEM

***Information Security***
Sourcefire
HP TippingPoint
FireEye HX/NX/EX
NMAP
Wireshark
Metasploit
Kali Linux
Tenable Nessus
Snort
Tcpdump
Netflow
Iptables
Paros
HP WebInspect
Rapid7 NeXpose
Honeypots
AIDE
Tripwire
RSA SecurID
Check Point
Palo Alto
Cisco PIX/ASA
DLP
Blue Coat
Infoblox
Dynamic Malware Reverse Engineering
REMnux
Event analysis

***Forensics***
AccessData Forensic Toolkit

events to under 4M events.
• Developed and implement Customer Account Manager program.

## Incident Response Manager

*Verisign*, Reston, VA

JAN 2012 - APR 2013

• Managed incident response & investigative duties. Coordinate multi-department Responses to information security events within the corporate infrastructure, Verisign product offerings, .COM, .NET, .GOV, .TV, .CC, & .NAME resolution system.
• Managed, operated, and analyzed data from corporate security systems including Sourcefire IDS, Solera Network Forensics, Mandiant Intelligent Response, and EnCase.
• Analyzed incident event data from FireEye and Damballa Failsafe appliances, as well as other data sources.
• Acted as Tier 3 support for Global Service Desk for security incidents.
• Managed department database for investigations & security incidents.
• Held Public Trust clearance with MBI for working with sensitive .GOV resolution data.

***Key Accomplishments***

• Designed, published, & maintained company Incident Response Program Guide.
• Upgraded & modernized existing forensics environment by upgrading to EnCase Enterprise 7 and installing AccessData Forensic Toolkit v4.1 for greater coverage.

## Manager, Systems & Platform Security

*Network Solutions*, Herndon, VA

AUG 2009 - DEC 2011

• Managed day-to-day technical security operations for global web hosting provider & domain registrar as part of leadership for Corporate Security Team.
• Operated & analyzed results from enterprise detection systems including Sourcefire & Tripwire.
• Performed incident response for in-network companies both in production and back-end servers; acted as Tier 3 escalation point & on-call responder.
• Maintained corporate SSL certificates.
• Performed regular vulnerability assessments & internal penetration tests against corporate assets.

***Key Accomplishments***

• Designed and deployed multi-sensor Sourcefire Intrusion Prevention System covering public shared web hosting, corporate web storefront, three remote offices, and public E-Commerce environments directly leading to a reduction in attack volume to near zero percentage within the first 3 months of implementation.
• Researched and developed over 900 customized Snort signatures to assist in detection & prevention of attacks.
• Designed and deployed enterprise-wide vulnerability management & remediation system utilizing Rapid7 NeXpose and multiple scanning engines for continuous scanning per environment and comprehensive remediation reporting.

X-Ways Forensics
Guidance EnCase 7.x
Autopsy Forensic Browser
The Sleuth Kit (TSK)
Windows Forensic Toolkit
RegRipper
Volatility
SANS SIFT Workstation
Foremost
Scalpel
Sysinternals Suite
IEF
Mandiant Intelligent Response
McAfee Tanium

***Software***

Microsoft Office
Atlassian JIRA
Atlassian Confluence
Regex
Python
VMWare

## CERTIFICATIONS & CLASSES

***(2016)*** Using Splunk 6.4
***(2016)*** Searching/Reporting with Splunk 6.4
***(2016)*** Splunk Infrastructure Overview 6.4
***(2015)*** SANS GIAC Network Forensics Analyst (GNFA) #161
***(2015)*** SANS SEC560: Network Penetration Testing and Ethical Hacking (GPEN)
***(2014)*** Volatility - Malware and Memory Forensics Training
***(2012)*** SANS GIAC Reverse Engineering Malware (GREM) #3610
***(2012)*** SANS GIAC Certified Forensic Examiner (GCFE) #666

***(2010)*** Pentesting with BackTrack Live, Offensive Security
***(2010)*** SANS GIAC Web Application Penetration Tester (GWAPT) #799
***(2009)*** Red Hat Certified Engineer (RHCE)

## Sr. Security Analyst

*Georgetown University*, Washington, DC

MAY 2005 - AUG 2009

• Established the Information Security Office and program for the University leading d day security operations.
• Performed security architecture reviews, vulnerability analyses, penetration tests, assessments for University organizations and IT projects. Served as a tier 3 escalation contact for University help desk services.
• Led incident response and forensics analysis for security breaches and litigation support.

***Key Accomplishments***
• Managed, designed, & led the implementation of border HA VPN Nokia firewall cluster for main campus data center, School of Foreign Service in Qatar, & disaster recovery sites.
• Supported University network migration in reviewing & securing of over 500 servers to a default deny security stance.
• Performed forensics on a 2006 data breach that directly led to arrests and prosecution by Federal authorities.
• Guest-lectured for computer science classes on the topic of Information Security.

## Security Specialist

*Computer Associates*, Herndon, VA

MAY 2004 - MAY 2005

• Deployed and operated the Managed Vulnerability Service (MVS) & Vulnerability Operations Center (VOC).
• Worked with clients to integrate the CA Unicenter suite into their existing environments to mitigate security threats.

***Key Accomplishments***
• Built the MVS Vulnerability Operations Center from scratch to support the newly launched MVS service.
• Successfully deployed CA Unicenter to act as a patch management infrastructure for a large government agency supporting thousands of workstations simultaneously.

## SOC Engineer

*Counterpane Internet Security*, Chantilly, VA

JAN 2003 - MAY 2004
• Performed technical operations in a 24x7x365 Security Operations Center Environment & incident response for clients, while managing client security monitoring devices.

## Manager, Network Security Consulting, Business Services

*WorldCom (UUNET)*, Ashburn, VA

DEC 1993 - DEC 2002

#805009840838122
***(2008)*** SANS GIAC Certified Forensic Analyst (GCFA) #4598
***(2006)*** EC Council Certified Ethical Hacker ECC915516
***(2003)*** Registered Virginia Private Investigator DCJS #99143477