Incident Management & Response
Fact Sheet v2.4

EVERY MINUTE COUNTS

Privasec helps organisations prevent, prepare and manage security incidents to protect their businesses. Whether you have just experienced an incident, or are planning your resilience strategy, our expert cybersecurity team can help you plan your resilience, manage your incident and recover to avoid recurrence.

The Incident Management Lifecycle

We cover the full incident management lifecycle to provide an end-to-end response capability.

OUR SERVICES

Emergency Incident Response

Get immediate support and guidance at the drop of a hat when you need it most. Just like calling 911 or 000 for help, our Emergency Response line is available 24/7.

Incident Response Retainer

Get guaranteed immediate access to our most senior responders 24/7. Save time and money by establishing a defined and agreed engagement plan to ensure no time is wasted.

Digital Forensics

Our skilled forensic investigators collect preserved evidence to investigate the causes and consequences of incidents. We maintain chain of custody and can testify in court.

Recovery guidance & Recurrence Prevention

We provide security expertise through the recovery of business services to ensure that new systems do not introduce further vulnerabilities.

Post Incident Assessment

We assess a particular incident and response to provide an accurate statement of events, identify similar risks and ensure that recurrences are prevented.

We also provide the following specialised incident response services

SCADA & ICS Incident Response

As SCADA and ICS ethical hackers, we know the criticality, sensitivity and cost of ICS incidents. We leverage years of experience as ICS engineers and testers to lead ICS operators through prompt containment and recurrence prevention.

Drone Incident Response

Privasec partners with DroneSec to provide policies, incident response, and operating procedures and frameworks. In addition, DroneSec can assist with responding to drone intrusion, payload delivery, and forensic analysis.

OUR PROCESS

While environments and incidents are unique, we follow proven best practices, refined by experience, to enable controlled execution when managing incidents.

1. Preparation (Pre-Incident)
- ☐ Incident Management Framework design & build
- ☐ Incident Response checklists and procedures
- ☐ Incident tresting & War Room simulations
- ☐ Security Assurance & Risk Management
- ☐ Cyber Security Insurance & Incident Response Retainer

2. Identify
- ☐ Initial incident assessment
- ☐ Confirm incident severity
- ☐ Liaise with/engage PR, Legal functions as required
- ☐ Assemble Crisis Management Team (CMT)
- ☐ Identify key internal and external stakeholders &
- ☐ Confirm communication frequency & medium
- ☐ Regular communications & updates*

3. Contain
- ☐ Containment options to mitigate business impacts
- ☐ Targeted intervention to affected systems
- ☐ Removal & replacement of systems if required
- ☐ Confirm containment & increased monitoring
- ☐ Regular communications & updates*

4. Investigate
- ☐ Collection of evidence
- ☐ Forensic investigation to determine root cause(s)
- ☐ Regular communications & updates*

5. Eradicate
- ☐ Planned removal and mitigation of attack vectors
- ☐ Regular communications & updates**

6. Recover
- ☐ Confirm eradication
- ☐ Security guidance through client restoration of services to operational state.
- ☐ Regular communications & updates*

*(*hourly & **daily, unless agreed otherwise)*

7. Improve
- ☐ Detailed post-incident report & presentation tailored to specific executive, business and technical audiences
- ☐ Risk assessment to identify similar exposures
- ☐ Mitigation to prevent recurrence
- ☐ Training to client SMEs

Communication and coordination are paramount to prompt and efficient incident response.

We can provide all internal stakeholders with regular* ** updates via emails, WhatsApp, etc. We can accommodate different periodicity and communication medium (i.e. Slack, Yammer, Signal, Skype) as agreed with you.

CHAIN OF CUSTODY

Our playbooks and procedures ensure we maintain the chain of custody at all times. All our incidents are managed within a secure purpose-built crisis and incident management platform. We can, as required, provide expert opinion and testimony in a Court of Law.

REMOTE AND ONSITE ASSISTANCE

There is no time to waste when an incident occurs. Every minute counts. Just like a 911 call, our Responders start providing immediate remote support upon notification to assess the gravity of the incident and work to contain it. We can reach most sites in Singapore, NSW, VIC and QLD within minutes and fly to anywhere in ASIA and EMEA within hours.

CAPABILITIES AND COMPETENCIES

Our team of experts are proficient in most technologies, including but not limited to; all commercial and open source operating systems, most commercial and open source business applications, major databases, common non-proprietary programming languages, all current log correlation tools, common PaaS and IaaS such as AWS, Azure, and Salesforce, etc.

In addition to these tools, Privasec and its partners also specialise in Unmanned Aerial Systems (drones) and Industrial Control System (SCADA/ICS) for government, critical infrastructure providers, processing plants, correctional facilities, and event organisers.

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia