Escalation chart - severity escalation

Escalation Chart with Examples (This table is not inexhaustible)

severity	event	action	Capacity	Report to authorities	Preparation
level 1 (Low)	• potentially unwanted programs (PUP) • warning banners • clean alerts from antimalware solution • Adware	• Delete the files • Remove the software / service	• Normal operations • Register the event	no	• Normal service and follow up of Antimalware services.
level 2 (mid)	• Phishing • malware detected and deleted • Macro viruses	• Delete the files • Remove the software / service • Maybe look for online information.	• As level 1 • Escalate if more occurrences are detected	• As information only. Report, don't expect any investigation	• Normal service and follow up of Antimalware services. • validated and tested, response plan
level 3 (High severity and low spread)	• Copyright infringement • malware partially detected • Passwords leaks with e-mail • Spear phishing and data not delivered • Attempts to escalate privileges • Attempts of lateral movement • Usage of CVE 7+ vulnerabilities	• Escalate the Incident Response plan accordingly • Analyze the event to see what is the intention. • Set up monitoring for the events • Prepare for further events and inform management • Monitor closely for activity	• As level 2 • • Collection of data with integrity and timestamps (maybe Forensic less sound) • Carefully describe your process of evidence collection.	• Yes, share data and the identification findings. • Get case/report ID. • Get contact at the police and get JNR number (IT-engineer at NSK/NC3)	• The above, including below • Have updated and tested Incident Response plan • Forensic capability, and les forensic ways of data collection
level 4 (Critical, high impact - high spread - business critical)	• Zero days • APT • Malware not detected and activated • Spear phishing and data delivered • Services have been breached • Accounts have been escalated • Usage of CVE 7+ vulnerabilities	• Escalate the Incident Response plan accordingly • Create a communication plan if needed. (specially of company deliveries to the community) • Analyze the events for the intention. • Prepare 3´rd party	• As level 4 • Designate responsibility to file responsable. • Report to authorities (Get contact to appropriate level (NSK/NC3)) • Physical collect data from media if possible	• Yes, share data and the identification findings. • Get case/report ID • Get contact at the police and get JNR number (IT-engineer at NSK/NC3) • Prepare court case (if needed and	• Major incident plan. • Secondary communications channels

Escalation chart - severity escalation

	• Lateral movement • Targeted attacks • Insider threats or paid actors.	trusted partner • Set up intensified monitoring for the breach inform authorities • Determine if data is lost or stolen.	• Collect Physical evidence • Have secure room for Evidence and have Chain of Custody • Integrity check of SHA256 or above HASH and look for OSINT. • Carefully describe your process of evidence collection.	appropriate) • if possible arrange share of forensic data vis encryption)	