

CLAIMS

1. A computing system comprising:
- 5 one or more processors, the one or more processors configured to execute one or more computing environments (CEs), the one or more CEs being configured to access shared resources;
- a processor-based computing environment inspector unit (CEIU) operably connected to the one or more CEs and configured to inspect
- 10 CE data of the one or more CEs,
- a processor-based mitigator unit (MU);
- wherein the CEIU is further configured, responsive to detecting CE data that is indicative of a compromise of a first CE, to notify the MU of the compromise of the first CE,
- 15 and wherein the MU is configured, responsive to receiving notification of a compromise of the first CE, to perform at least one of a group comprising:
- a) disabling access to the shared resources by the first CE,
- 20 b) storing data derivative of an executing state of the first CE, thereby giving rise to a CE image usable for threat analysis, and
- c) terminating the first CE and restoring CE operation from a first boot image of the first CE.
- 25
2. The system of claim 1, wherein at least one of the one or more CEs is a guest CE, and wherein the MU has hypervisor capabilities.
3. The system of claim 1, wherein at least one of the one or more CEs is a
- 30 base CE, and wherein the MU has boot loader capabilities.

4. The system of claim 1, wherein at least one of the one or more CEs is an operating system process.
5. The system of claim 1, wherein at least one of the one or more CEs is a container.
6. The system of claim 1, wherein
at least one of the one or more processors is in a remote device comprising a wireless link,
a remote CE executes on the at least one processor, and
the operable connection of the remote CE to the CEIU utilizes the wireless link.
7. The system of claim 1, wherein the MU is configured to disable access to shared resources by directing CE data of the first CE to decoy resources, thereby isolating the first CE.
8. The system of claim 7, wherein the decoy resources are configured to store data derivative of CE data of the first CE to a storage medium.
9. The system of claim 7, wherein the decoy resources are configured to provide decoy data to the first CE.
10. The system of claim 1, wherein the CEIU is collocated in a network interface controller, and wherein the CEIU is configured to inspect network data from the one or more CEs.

11. The system of claim 1, wherein the CEIU is a guest CE operably connected to a virtual network, and wherein the CEIU is configured to inspect at least one of:

5 network data generated by one or more of the CEs, and
 network data transmitted to one or more of the CEs.

12. A method of mitigating compromise of computing environments (CEs), the method comprising:

10 inspecting, by a processor-based computing environment inspector unit (CEIU), CE data of one or more CEs that are configured to access shared resources;

 detecting, by the processor-based CEIU, CE data that is indicative of a
15 compromise of a first CE;

 responsive to detecting the data indicative of compromise, notifying,
 by the processor-based CEIU, a processor-based mitigation unit (MU)
 of the compromise of the first CE; and

 responsive to receiving notification of a compromise of the first CE,
20 performing, by the MU, at least one of a group comprising:

 g) disabling access to the shared resources by the first CE,
 h) storing data derivative of an executing state of the first CE, thereby
 giving rise to a CE image usable for threat analysis, and
 i) terminating the first CE and restoring CE operation from a first boot
25 image of the first CE.

13. The method of claim 12, wherein the disabling access to shared resources comprises directing CE data of the first CE to a decoy resources unit, thereby isolating
30 the first CE.

14. The method of claim 12, further comprising, subsequent to the disabling access to shared resources: restoring, by the processor-based MU, CE operation from a first CE boot image stored on a storage medium.

5 15. The method of claim 13, wherein the decoy resources provide decoy data to the first CE.

16. A computer program product comprising a computer readable storage medium containing program instructions, which program instructions when read by a processor,
10 cause the processor to perform a method of mitigating compromise of computing environments (CEs), the method comprising:

inspecting, by a processor-based computing environment inspector unit (CEIU), CE data of one or more CEs that are configured to access shared resources;

15 detecting, by the processor-based CEIU, CE data that is indicative of a compromise of a first CE;

responsive to detecting the data indicative of compromise, notifying, by the processor-based CEIU, a processor-based mitigation unit (MU) of the compromise of the first CE; and

20 responsive to receiving notification of a compromise of the first CE, performing, by the MU, at least one of a group comprising:

j) disabling access to the shared resources by the first CE,

k) storing data derivative of an executing state of the first CE, thereby giving rise to a CE image usable for threat analysis, and

25 l) terminating the first CE and restoring CE operation from a first boot image of the first CE.

17. The computer program product of claim 16, wherein disabling access to shared resources comprises terminating the first CE.

30

18. The computer program product of claim 16, wherein disabling access to shared resources directing CE data of the first CE to a decoy resources unit, thereby isolating the first CE.

- 5 19. The computer program product of claim 16, wherein the method further comprises, subsequent to the disabling access to shared resources: restoring, by the processor-based MU, CE operation from a first CE boot image stored on a storage medium.