CSC 431: Cyber Security Operations

Frank M. Olmstead

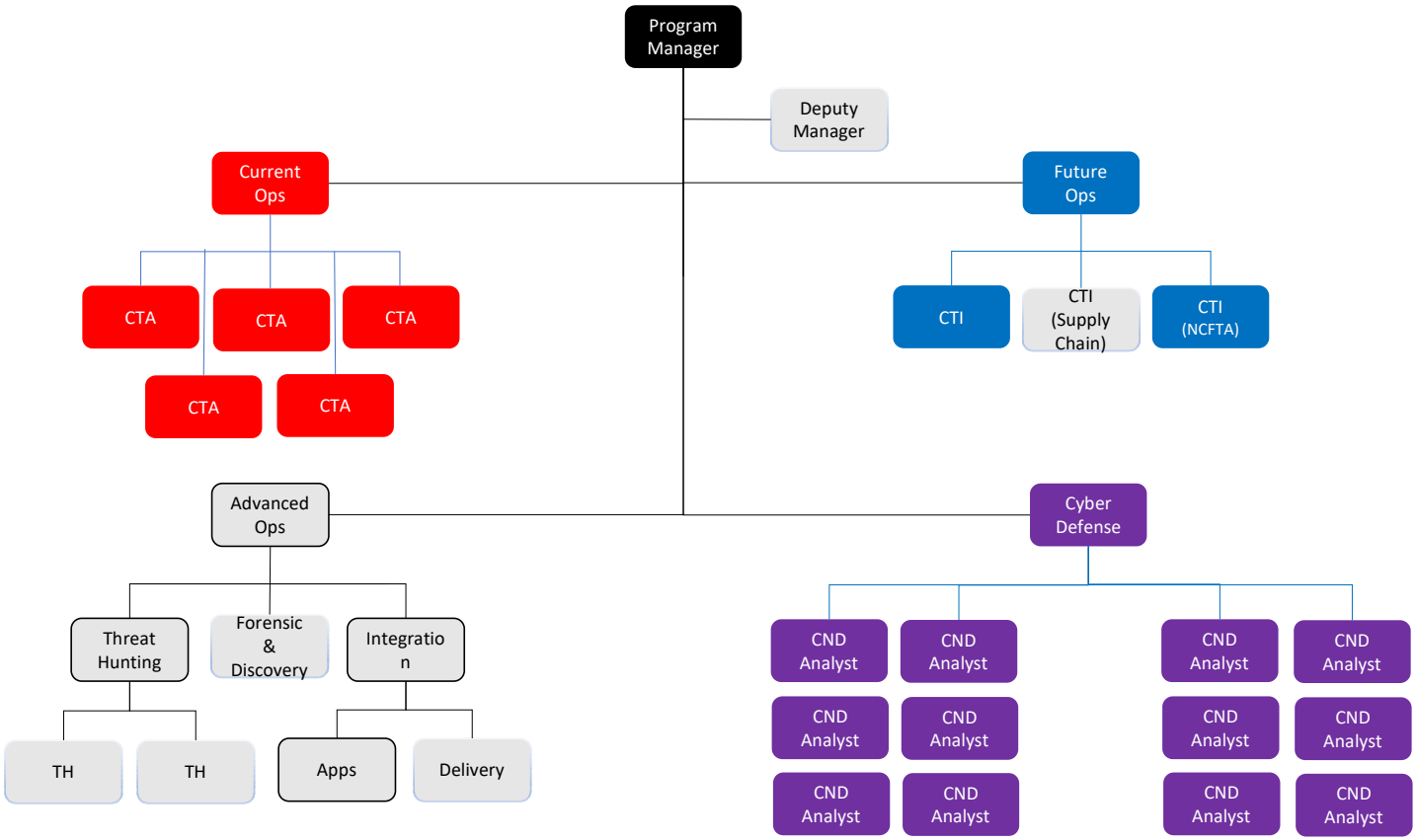
Frank.Olmstead@lsus.edu

Agenda – 1st Meeting

- Introductions
- Security Operations
  - Organization & Roles
  - Security Operations Center (SOC) Process
- A day in the life
- Real-life example

Frank Olmstead

What does it (SOC) look like ?



Frank Olmstead

SOC Monitoring – The Process

1. TUNING
2. SYNTHESIZE
3. TIER I
4. TIER II
5. TIER III

Onboarding new technologies

Reducing false positives

Detect Strategy

ThreatConnect

Intelligence

Enhancing signals

Correlation of adjacent / related events

McAfee

Collect, process & verify

Determine events of interest

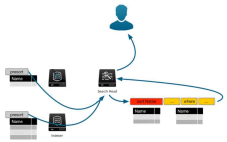
Tuning / Filtering

splunk>

Data enrichment, intelligence, analysis

Priority determination (Impact + Severity)

SIEM Correlation Development

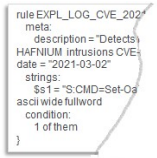


yara zeek SURICATA

Internal resolution (Tuning)

Signature Development

Follow-through to resolution

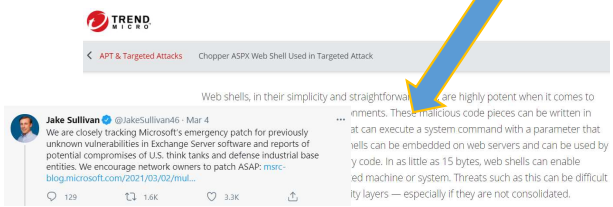


Customer Detect !

A Day in the Life

Tier I

- Collect and process events
- Determine events of interest
- Verification of event
- Tune and filter as needed
- Forward on for additional analysis



Tier II

- Verification of Tier I data
- Data enrichment, intelligence, analysis
- Correlation of adjacent/related events
- Priority determination (Impact & Severity)
- Provide recommendations and RFI
- SIEM Correlation Development
- Closure or Escalation for resolution

Tier III

- Verification (accuracy and completeness)
- Internal resolution (e.g. Tuning)
- External escalation (e.g. SOC Ticket)
- Signature Development
- Follow-through to resolution
- Feedback to lower tiers
- Signature Development

Splunk
(((c-uri="*/owa/auth/Current*" OR c-uri="*/ecp/default.flt*" OR c-uri="*/ecp/main.css*" OR …

QRadar
SELECT UTF8(payload) as search_payload from events where ((("URL" ilike '%/owa/auth/Current%' or "URL" ilike…

```
rule
EXPL_LOG_CVE_2021_27065_Exchange_Forensic_Artefacts_Mar21
_1 {
  meta:
    description = "Detects forensic artefacts found in HAFNIUM
intrusions exploiting CVE-2021-27065"
    author = ""
    reference =Florian Roth
"https://www.volexity.com/blog/2021/03/02/active-exploitation-
of-microsoft-exchange-zero-day-vulnerabilities/"
    date = "2021-03-02"
  strings:
    $s1 = "S:CMD=Set-OabVirtualDirectory.ExternalUrl='" ascii wide
fullword
  condition:
    1 of them
}
```

Customer Detect !

Frank Olmstead

Team in Action (APT 38 - Lazarus Group)

Offense 107150	
Magnitude	[redacted]
Description	Outbound DNS Query for ThreatConnect IOC Domain
Source IP(s)	[redacted]
Destination IP(s)	Local (3)
Network(s)	Multiple (2)

TIP IOCs alert within Customers SIEM on DNS Query

05-19-2020

Employee contacted on LinkedIn

05-26-2020

Operation 'Dream Job' Widespread North Korean Espionage Campaign

Posted on August 13, 2020 by ClearSky Research Team

Clear Sky Research Team Published first public Lazarus Report

06-03-2020

Lazarus report published

10-13-2020